

# Symantec Backup Exec 2012

Administrator's Guide



The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: March 2012 (Revision 1A)

## Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043  
<http://www.symantec.com>

# Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

## Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://www.symantec.com/business/support/)

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan [customercare\\_apac@symantec.com](mailto:customercare_apac@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# Contents

Technical Support .....	4	
Chapter 1	Introducing Backup Exec 2012 .....	43
	About Backup Exec .....	43
	How Backup Exec works .....	44
	What's new in Backup Exec 2012 .....	46
	What's new in Backup Exec 2012 agents and options .....	51
Chapter 2	Installation .....	57
	About installing Backup Exec .....	58
	Backup Exec pre-installation checklist .....	60
	About the Environment Check .....	61
	Checking your environment before installing .....	62
	About Microsoft SQL Server 2005 Express Edition components installed with Backup Exec .....	63
	About Backup Exec's standard features .....	64
	System requirements .....	65
	About the differences between a typical installation and a custom installation .....	67
	Installing a typical installation of Backup Exec .....	68
	Installing a custom installation of Backup Exec .....	70
	Installing additional Backup Exec options to the local Backup Exec server .....	75
	Special considerations for installing Backup Exec to remote computers .....	76
	Push-installing Backup Exec to remote computers .....	77
	About installing the Agent for Windows .....	83
	About push-installing the Agent for Windows to remote computers .....	83
	Installing updates to the Agent for Windows on remote computers .....	89
	How to install the Agent for Windows in an Active Directory network .....	90
	Using a command prompt to install the Agent for Windows on a remote computer .....	94

Using a command script to install the Agent for Windows .....	98
Installing the Remote Administrator .....	99
Installing the Remote Administrator using the command line .....	100
Running the Remote Administrator .....	102
Installing Backup Exec using the command line (silent mode) .....	104
Command line switches for silent mode installation of Backup Exec .....	105
Creating installation parameter files .....	112
Installing a trial version of Backup Exec agents and options .....	114
About the installation log .....	114
Repairing Backup Exec .....	115
About updating Backup Exec with LiveUpdate .....	116
About scheduling automatic updates using LiveUpdate .....	117
Scheduling automatic updates using LiveUpdate .....	117
Application settings for LiveUpdate .....	118
Running LiveUpdate manually .....	119
Viewing installed updates .....	119
Viewing license information .....	120
Finding installed licenses in your environment .....	120
About Backup Exec maintenance contract information .....	121
Viewing Backup Exec maintenance contract information .....	122
Updating expired maintenance contracts .....	123
Managing maintenance contract customer numbers .....	124
About upgrading from previous versions of Backup Exec .....	124
Backup Exec pre-upgrade checklist .....	126
About the Data Migration report .....	127
Viewing the Data Migration report .....	127
Post-installation tasks .....	127
Uninstalling Backup Exec .....	128
Uninstalling Backup Exec using the command line .....	129
Uninstalling Backup Exec options from the local Backup Exec server .....	129
 Chapter 3	
Getting Started .....	131
About the administration console .....	131
Displaying the Backup Exec version .....	134
About sorting and filtering information .....	134
Sorting and filtering information .....	134
Deleting a configured view .....	135
Editing a configured view .....	136
About the Home tab .....	136

	Layout group .....	137
	System Health group .....	137
	Support group .....	139
	Configuring the Home tab .....	140
	Restoring the Home tab's default layout .....	140
	About the Symantec RSS Reader .....	140
	Viewing an article in the Symantec RSS Reader .....	141
	Customizing the Symantec RSS Reader .....	141
	Removing a default RSS feed from the Symantec RSS reader .....	142
	Getting ready to back up your computer .....	142
Chapter 4	Storage configuration .....	145
	About the Configure Storage wizard .....	145
	About the All Storage view in Backup Exec .....	149
Chapter 5	Backups .....	153
	About preparing for your first backup .....	154
	About backing up data .....	155
	Required user rights for backup jobs .....	157
	About the list of servers .....	157
	Adding servers to the list of servers .....	158
	Removing servers from the list of servers .....	159
	About server groups .....	159
	Viewing server groups .....	160
	Creating a server group .....	160
	Editing a server group .....	161
	Deleting a server group .....	162
	Backing up data .....	163
	Creating a one-time backup .....	164
	Creating a new backup from an existing backup .....	165
	Backup Job Selection options .....	167
	Backing up server groups .....	168
	Running the next scheduled backup job .....	169
	Editing backups .....	170
	Backup menu options .....	171
	About testing or editing credentials for jobs .....	175
	Test/edit credentials options .....	175
	Viewing or editing credentials for a computer or a computer's contents .....	176
	Credentials properties .....	176
	About selecting data to back up .....	177

About including or excluding files for backup jobs .....	180
Include/Exclude options .....	181
About stages .....	183
Editing a stage .....	184
About backup job settings .....	185
Schedule options .....	188
Storage options .....	190
Network options .....	195
Test Run options .....	196
Verify options .....	197
Advanced Open File options .....	199
Security options .....	201
Pre/post commands options .....	202
Files and Folders options .....	204
Exclusions options .....	209
About backup sets .....	212
About keeping backup sets .....	213
Deleting backup sets .....	214
Retaining backup sets .....	215
Releasing retained backup sets .....	216
Cataloging backup sets .....	217
Viewing the contents of backup sets .....	217
Viewing backup sets properties .....	218
About duplicating backed up data .....	218
Duplicating backup sets .....	219
Duplicating job history .....	220
About test run jobs .....	222
About verifying backed up data .....	222
Verifying backup sets .....	223
Verifying job history .....	223
How to copy data directly from a virtual tape library to a physical tape device .....	225
Copying data from a virtual tape library to a physical tape device .....	225
Viewing all scheduled backup jobs on a calendar .....	226
Excluding dates from the schedule using the backup calendar .....	226
Backup calendar options .....	227
<b>Chapter 6 Restores .....</b>	<b>229</b>
About searching for and restoring data .....	229
Setting defaults for restore jobs .....	231
Restore job defaults .....	231

About restoring encrypted data .....	233
About performing a complete online restore of a Microsoft Windows computer .....	234
About restoring System State .....	234
Restoring System State to a domain controller .....	235
About restoring Backup Exec Shadow Copy Components .....	236
About restoring utility partitions and UEFI system partitions .....	237
Installing a new Windows Server domain controller into an existing domain by using a redirected restore .....	237
About restoring media created with other backup software .....	239
About restoring data from ARCserve tapes .....	240
Restoring data from ARCserve tapes .....	240
About canceling a restore job .....	241
About catalogs .....	242
Editing global options for catalogs .....	242
Global options for catalogs .....	243
Chapter 7      Job management and monitoring .....	247
About managing and monitoring active and scheduled jobs .....	247
Viewing job activity details for active jobs .....	248
Editing a single scheduled job .....	251
Editing multiple scheduled jobs .....	252
Canceling an active job .....	252
Placing a job on hold .....	253
Removing the hold on a job .....	253
Placing the job queue on hold .....	253
Removing the hold on the job queue .....	254
Active job statuses .....	254
Scheduled job statuses .....	256
Running a scheduled job immediately .....	258
Changing the priority for a scheduled job .....	258
Deleting scheduled jobs .....	259
Running a test job from the Jobs list .....	259
About the Job History .....	260
Viewing the history of a job .....	260
Deleting a job from the Job History .....	262
Running a job from the Job History .....	263
Completed job statuses .....	263
Viewing the job log .....	264
Finding text in the job log .....	267
Configuring default job log options .....	268
About error-handling rules for failed or canceled jobs .....	270

Creating a custom error-handling rule .....	270
Enabling or disabling error-handling rules .....	274
Deleting a custom error-handling rule .....	274
Enabling an error-handling rule for a failed job .....	274
Custom error-handling rule for recovered jobs .....	275
About the cluster failover error-handling rule .....	276
About job status and recovery .....	276
Setting job status and recovery options .....	277

Chapter 8	Alerts and notifications .....	279
	About alerts .....	279
	Viewing active alerts and alert history on the Home tab .....	281
	Active alerts properties .....	281
	Viewing the alert history for a server or a storage device .....	282
	Alert History options .....	282
	Filtering alerts .....	284
	Viewing the job log from an alert .....	284
	Responding to active alerts .....	285
	Alert response options .....	285
	Clearing all informational alerts manually .....	286
	Configuring alert categories .....	286
	Configure Alert Categories options .....	287
	About notifications for alerts .....	288
	Setting up notification for alerts .....	289
	Configuring email notification for alerts .....	290
	Configuring text message notification for alerts .....	291
	Configure Email and Text Messages options .....	291
	About managing recipients for alert notifications .....	292
	.....	293
	Configuring an individual recipient for alert notifications .....	293
	Configuring a group recipient for alert notifications .....	295
	Editing recipient notification properties .....	297
	Deleting recipients .....	298
	Stopping alert notification for a recipient .....	298
	Sending a notification when a job completes .....	299
	Notification options for jobs .....	299
	About SNMP notification .....	300
	Installing and configuring the SNMP system service .....	303
	Installing the Windows Management Instrumentation performance counter provider .....	303
	Installing the Windows Management Instrumentation provider for SNMP .....	304

	Uninstalling the Windows Management Instrumentation performance counter provider .....	304
	Uninstalling the Windows Management Instrumentation provider for SNMP .....	304
Chapter 9	Disk-based storage .....	305
	About disk-based storage .....	305
	About storage trending for disk storage and virtual disks .....	306
	About disk storage .....	307
	About restoring data from a reattached disk-based storage device .....	308
	Changing the location of a disk storage device .....	309
	Editing disk storage properties .....	309
	Disk storage properties .....	310
	About disk cartridge storage .....	317
	Editing disk cartridge properties .....	317
	Disk cartridge properties .....	317
Chapter 10	Network-based storage .....	323
	About network-based storage .....	323
	About cloud storage devices .....	323
	Editing the properties of a cloud storage device .....	324
	Cloud storage device properties .....	324
Chapter 11	Legacy backup-to-disk folders .....	327
	About legacy backup-to-disk folders .....	327
	Importing a legacy backup-to-disk folder .....	328
	Editing backup-to-disk folder properties .....	328
	Backup-to-disk folder properties .....	329
	Changing the location of a legacy backup-to-disk folder .....	330
	Recreating a legacy backup-to-disk folder and its contents .....	331
Chapter 12	Tape drives and robotic libraries .....	333
	About tape drives and robotic libraries .....	334
	About the Virtual Tape Library Unlimited Drive Option .....	334
	About the Library Expansion Option .....	335
	About using the Hot-swappable Device Wizard to add or replace devices .....	335
	Using the Hot-swappable Device Wizard to add or replace devices .....	336
	About installing Symantec tape device drivers .....	336

Installing Symantec tape device drivers by running tapeinst.exe .....	337
Using the Symantec Device Driver Installation Wizard to install tape device drivers .....	337
Editing tape drive properties .....	338
Tape drive properties .....	338
Enabling or disabling hardware compression for tape drives .....	343
Changing the block size, buffer size, buffer count, and high water count for tape drives .....	343
Changing the settings to read and write in single block mode for tape drives .....	344
Changing the settings to read and write in SCSI pass-through mode for tape drives .....	344
Viewing tape drive statistics .....	344
Tape drive statistics .....	345
About robotic libraries in Backup Exec .....	349
Requirements for setting up robotic library hardware .....	349
Inventorying robotic libraries when Backup Exec services start .....	350
Initializing a robotic library when the Backup Exec service starts .....	351
Defining a cleaning slot .....	351
Viewing robotic library properties .....	352
Viewing jobs, job histories, and active alerts for a robotic library .....	354
About robotic library partitions .....	355
Editing the properties of a robotic library partition .....	356
Configuring robotic library partitions .....	356
Removing robotic library partitions .....	357
Reassigning a slot base number for robotic libraries .....	357
Viewing robotic library slot properties or backup sets .....	357
 Chapter 13	
Tape and disk cartridge media .....	365
About tape and disk cartridge media .....	365
About media sets .....	366
About media overwrite protection and append periods .....	369
About the default media set Keep Data for 4 Weeks .....	373
Creating media sets for tape and disk cartridge media .....	373
About media overwrite protection levels for tape and disk cartridge media .....	377
About overwriting allocated or imported media for tape and disk cartridge media .....	377

How Backup Exec searches for overwritable media in tape drives and disk cartridges .....	378
Viewing audit log entries for tape and disk cartridge media operations .....	380
Configuring tape and disk cartridge media operations to appear in the audit log .....	380
About labeling tape and disk cartridge media .....	381
About labeling imported media .....	382
About barcode labeling .....	382
Renaming a media label .....	383
About WORM media .....	383
About media vaults .....	384
Editing media vault properties .....	385
Creating media vault rules to move media to and from media vaults .....	386
Updating the media location in media vaults .....	387
Moving media to a vault .....	387
Deleting a media vault .....	388
About retiring damaged media .....	388
Retiring damaged media .....	388
About deleting media .....	389
Deleting media .....	389
About erasing media .....	389
Erasing media .....	390
About cataloging media that contains encrypted backup sets .....	391
Associating media with a media set .....	391
Editing media properties .....	391
Media properties .....	392
Media rotation strategies .....	398
Son media rotation strategy .....	398
Father/son media rotation strategy .....	399
Grandfather media rotation strategy .....	400
 Chapter 14	
Storage device pools .....	403
About storage device pools .....	403
Creating a storage device pool .....	405
Viewing jobs, job histories, and active alerts for a storage device pool .....	405
Editing storage device pool properties .....	406
Storage device pool properties .....	406

Chapter 15	Storage operations .....	409
	About storage operation jobs .....	410
	Storage operations for virtual tape libraries and simulated tape libraries .....	412
	Sending a notification when a scheduled storage operation job completes .....	413
	Notification options for scheduled storage operation jobs .....	413
	Schedule options for storage operation jobs .....	414
	Editing global settings for storage .....	415
	Global settings for storage .....	415
	About sharing storage devices .....	418
	Sharing a storage device .....	419
	Shared Storage options .....	420
	About deleting a storage device .....	420
	Deleting a storage device .....	421
	Renaming a storage device .....	421
	Viewing jobs, job histories, backup sets, and active alerts for storage devices .....	422
	About inventorying a storage device .....	422
	Inventorying a storage device .....	423
	Inventorying and cataloging a storage device .....	423
	Cataloging a storage device .....	424
	Scanning a storage device .....	424
	Changing the state of a storage device to online .....	425
	Pausing and unpausing a storage device .....	425
	Disabling and enabling a storage device .....	425
	Initializing a robotic library .....	426
	Retensioning a tape .....	426
	Formatting media in a drive .....	427
	Labeling media .....	427
	Ejecting media from a disk cartridge or tape drive .....	428
	Cleaning a robotic library drive .....	429
	About importing media .....	430
	Importing media .....	431
	About exporting expired media .....	431
	Exporting media .....	432
	About locking the robotic library's front portal .....	433
	Unlocking the robotic library's front portal .....	433
	Backup Exec server and storage device states .....	434

Chapter 16	Virtualization .....	437
	About conversion to virtual machines .....	437
	Requirements for conversion to virtual machines .....	439
	Creating a backup job with a simultaneous conversion to a virtual machine .....	440
	Creating a backup job with a conversion to a virtual machine after the backup .....	441
	Schedule options for a conversion to virtual machine job .....	442
	Notification options for a conversion to virtual machine job .....	443
	Adding a stage to convert to a virtual machine .....	444
	Converting to a virtual machine from a point in time .....	444
	Conversion from point in time options .....	445
	Schedule options for a conversion from a point in time .....	446
	Virtual machine conversion options .....	446
	Disk configuration details .....	450
	About editing a conversion to virtual machine job .....	451
	Setting default options for conversion to virtual machines .....	451
	Default conversion settings for conversion to virtual machines .....	452
Chapter 17	Configuration and settings .....	455
	About configuring Backup Exec .....	455
	About job defaults .....	456
	Setting default backup job settings .....	456
	Setting global schedule options .....	457
	About excluding dates from the backup schedule .....	458
	Selecting dates to exclude from the backup schedule .....	459
	Importing a list of dates to exclude from the backup schedule .....	459
	Exporting excluded backup dates to another server .....	460
	Deleting dates from the exclude dates list .....	460
	Excluding selections from all backups .....	462
	About global Backup Exec settings .....	463
	Changing the default preferences .....	465
	About database maintenance .....	466
	Changing database maintenance options .....	467
	Configuring Backup Exec to discover data to back up .....	469
	Changing network and security options .....	470
	Setting default Granular Recovery Technology (GRT) options .....	482
	About configuring DBA-initiated job templates .....	483
	About logon accounts .....	498

About the default Backup Exec logon account .....	499
About Backup Exec restricted logon accounts .....	500
Creating a Backup Exec logon account .....	500
About the Backup Exec System Logon Account .....	501
Editing a Backup Exec logon account .....	502
Changing the password for a Backup Exec logon account .....	503
Replacing a Backup Exec logon account .....	503
Deleting a Backup Exec logon account .....	504
Changing your default Backup Exec logon account .....	505
Creating a new Backup Exec System Logon Account .....	505
Copying logon account information to another Backup Exec server .....	505
About the Backup Exec Services Manager .....	511
Starting and stopping Backup Exec services .....	511
About the Backup Exec service account .....	512
Changing service account information .....	513
Changing service startup options .....	514
About audit logs .....	516
Configuring the audit log .....	516
Viewing the audit log .....	517
Removing entries from the audit log .....	517
Saving the audit log to a file .....	518
Copying configuration settings to another Backup Exec server .....	519
Copy Settings options .....	520
Importing a list of destination Backup Exec servers to the Copy Settings dialog .....	521
Adding a destination Backup Exec server to the Copy Settings dialog .....	521
About viewing server properties .....	523
Viewing local Backup Exec server properties .....	524
Viewing server properties .....	524
Chapter 18	
Backup strategies .....	525
About backup strategies .....	526
How to choose a backup strategy .....	526
How to determine your backup schedule .....	526
How to determine the amount of data to back up .....	527
How to determine a schedule for data storage .....	527
How to determine what data to back up .....	528
About backup methods .....	528
About the full backup method .....	528
About the differential backup method .....	529

About the incremental backup method .....	530
About backup method advantages and disadvantages .....	530
About configuring Backup Exec to determine if a file has been backed up .....	532
About backing up and deleting files .....	535
About using fully qualified domain names in backup selections .....	536
About discovering data to back up .....	537
About using checkpoint restart .....	538
About backing up critical system components .....	539
About the Backup Exec Shadow Copy Components file system .....	540
About managing Microsoft Virtual Hard Disk (VHD) files in Backup Exec .....	542
About pre/post commands .....	542
How to restore individual items by using Granular Recovery Technology .....	543
Recommended devices for backups that use Granular Recovery Technology .....	545
About requirements for jobs that use Granular Recovery Technology .....	547
About specifying backup networks .....	548
About using IPv4 and IPv6 in Backup Exec .....	550
About using Backup Exec with Symantec Endpoint Protection .....	550
About encryption .....	551
About software encryption .....	551
About hardware encryption .....	552
Encryption keys .....	552
About pass phrases in encryption .....	553
Chapter 19	Reports .....
	555
About reports in Backup Exec .....	556
About report groups .....	557
Viewing the list of available reports in a report group .....	558
Running a report .....	558
Saving a report .....	559
Saving a scheduled report to a new location upon completion .....	559
Printing a report from the Backup Exec Report Viewer .....	560
Printing a report that is saved in PDF format .....	560
Printing a report that is saved in HTML format .....	561
Additional settings for standard reports .....	561
Viewing a scheduled report .....	563
Editing a scheduled report .....	564

Copying a custom report .....	564
Re-running a completed report .....	565
Deleting a custom or scheduled report .....	565
About scheduling report jobs and setting notification recipients .....	566
About custom reports in Backup Exec .....	566
Creating a custom report .....	567
Custom report name and description options .....	568
Field selection options for custom reports .....	569
About filter criteria and filter expressions for custom reports .....	570
About grouping fields in custom reports .....	577
Available groups from which to select fields for custom reports .....	579
About sorting fields in custom reports .....	579
Setting graph options in custom reports .....	581
Previewing custom reports .....	585
Copying custom reports .....	585
Editing custom reports .....	586
Deleting custom reports .....	586
Editing application settings for reports .....	586
Application settings for reports .....	587
Viewing report properties .....	588
Report properties .....	588
Available reports .....	589
Alert History report .....	595
Alert History By Backup Exec Server report .....	595
Audit Log report .....	596
Backup Job Success Rate report .....	597
Backup Recommendations report .....	597
Backup Resource Success Rate report .....	598
Backup Sets by Media Set report .....	598
Backup Size By Resource report .....	599
Daily Device Utilization report .....	600
Device Summary report .....	601
Deduplication Device Summary report .....	602
Deduplication Summary report .....	603
Disk Storage Summary report .....	603
Error-Handling Rules report .....	604
Event Recipients report .....	605
Failed Backup Jobs report .....	606
Jobs Summary report .....	607
Managed Backup Exec Servers report .....	608
Media Audit report .....	609

Media Errors report .....	610
Media Required for Recovery report .....	610
Media Summary report .....	611
Media Vault Contents report .....	612
Move Media to Vault report .....	613
Operations Overview report .....	614
Overnight Summary report .....	616
Problem Files report .....	617
Recently Written Media report .....	617
Resource Risk Assessment report .....	618
Restore Set Details by Resource report .....	619
Resource Protected Recently report .....	619
Retrieve Media from Vault report .....	620
Robotic Library Inventory report .....	621
Scheduled Server Workload report .....	622
Scratch Media Availability report .....	623
Test Run Results report .....	624
Archive Job Success Rate report .....	625
Archive Selections by Archive Rules and Retention Categories report .....	625
Exchange Mailbox Group Archive Settings report .....	626
Failed Archive Jobs report .....	627
File System Archive Settings report .....	628
Overnight Archive Summary report .....	628
Vault Store Usage Details report .....	629
Vault Store Usage Summary report .....	630
 Chapter 20	
Disaster preparation and recovery .....	633
About disaster preparation .....	634
About key elements of a disaster preparation plan (DPP) .....	634
Returning to the last known good configuration .....	636
Creating a hardware profile copy .....	636
About using Windows' Automated System Recovery and System Restore to recover a Windows XP or Windows Server 2003 system .....	637
About manual disaster recovery of Windows computers .....	637
About a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller) .....	638
Running a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller) .....	639

	About a disaster recovery operation of a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller) .....	643
	Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller) .....	644
Chapter 21	Troubleshooting Backup Exec .....	649
	Troubleshooting hardware-related issues .....	650
	How to get more information about alerts and error messages .....	654
	Troubleshooting backup issues .....	655
	Troubleshooting failed components in the SAN .....	656
	Troubleshooting offline storage devices in a SAN .....	657
	Finding hardware errors in a SAN .....	659
	Resetting the SAN .....	660
	Bringing storage devices online after an unsafe device removal event in a SAN .....	660
	How to improve Backup Exec's performance .....	661
	Accessing Symantec Online .....	661
	About the Symantec Knowledge Base .....	662
	Searching the Symantec Knowledge Base .....	663
	About contacting Technical Support .....	663
	About Backup Exec diagnostic tools .....	664
	About the Symantec Backup Exec Support Tool .....	664
	Running the Backup Exec Support Tool .....	665
	About the Backup Exec diagnostic application .....	665
	Generating a diagnostic file for troubleshooting .....	666
	Backup Exec Diagnostics .....	666
	Using the command line to generate a diagnostic file for troubleshooting .....	667
	Command line switches for a diagnostic file .....	668
	Generating a diagnostic file on a remote Backup Exec server .....	669
	Running the begather utility to troubleshoot Backup Exec components on Linux servers .....	670
	Using the Backup Exec Debug Monitor for troubleshooting .....	670
	About the Backup Exec debug tool .....	671
Chapter 22	Using Backup Exec in cluster environments .....	673
	About Backup Exec and clusters .....	674
	Requirements for clustering Backup Exec in a Microsoft Cluster Server environment .....	675

How Backup Exec works in a Microsoft Cluster Server environment .....	675
Requirements for installing Backup Exec on a Microsoft Cluster Server .....	676
Installing Backup Exec on a Microsoft Cluster Server .....	677
Upgrading Backup Exec on a Microsoft cluster .....	678
Installing additional Backup Exec options on a Microsoft cluster .....	679
Uninstalling Backup Exec from a Microsoft cluster .....	680
Creating storage device pools for Microsoft Cluster Servers .....	680
Using checkpoint restart on Microsoft Cluster Server failover .....	681
About enabling or disabling checkpoint restart .....	683
Specifying a different failover node .....	683
Designating a new central administration server in a Microsoft Cluster Server .....	684
Configurations for Backup Exec and Microsoft Cluster Servers .....	686
Two-node cluster with locally attached storage devices .....	687
Two-node cluster with tape devices on a shared SCSI bus .....	688
Configuring a shared SCSI bus for tape devices .....	689
Multi-node clusters on a fibre channel SAN with the Central Admin Server Option .....	691
Using the Central Admin Server Option with Microsoft clusters and a storage area network .....	692
About backing up Microsoft Cluster Servers .....	693
About restoring data to a Microsoft cluster .....	694
Disaster recovery of a cluster .....	694
Using Simplified Disaster Recovery to prepare for disaster recovery of a cluster .....	696
Recovering nodes on the cluster using Simplified Disaster Recovery .....	696
Recovering Backup Exec on a Microsoft cluster using Simplified Disaster Recovery .....	697
Recovering the entire cluster using a manual disaster recovery procedure .....	697
Restoring the Microsoft Cluster Server data files .....	699
Recovering all shared disks in a Microsoft cluster .....	699
Recovering Backup Exec in a Microsoft cluster .....	700
Changing the Quorum disk signature .....	700
Manually joining two cluster disk groups and resynchronizing volumes .....	701
Troubleshooting clusters .....	701

Chapter 23	Simplified Disaster Recovery .....	703
	About Simplified Disaster Recovery .....	704
	About disaster recovery information files .....	704
	About the Simplified Disaster Recovery Disk .....	705
	Requirements for using Simplified Disaster Recovery .....	706
	About installing Simplified Disaster Recovery .....	707
	About preparing computers for use with Simplified Disaster Recovery .....	707
	Notes about using deduplication storage devices with Simplified Disaster Recovery (SDR) .....	708
	About setting an alternate location for a disaster recovery information file .....	709
	Setting or changing the alternate location for the disaster recovery information file .....	710
	Requirements and recommendations for running the Create Simplified Disaster Recovery Disk Wizard .....	714
	About the Create Simplified Disaster Recovery Disk Wizard .....	714
	Running the Create Simplified Disaster Recovery Disk Wizard .....	715
	About copying the disaster recovery files .....	715
	Preparing a custom Simplified Disaster Recovery disk locally for remote Backup Exec servers .....	716
	Backup Exec server logon credential options .....	716
	About preparing to recover from a disaster by using Simplified Disaster Recovery .....	717
	About changing hardware in the computer to be recovered .....	718
	About using Simplified Disaster Recovery to recover IBM computers .....	719
	About the Recover This Computer Wizard .....	720
	About encrypted backup sets and the Recover This Computer Wizard .....	720
	Recovering a computer by using the Recover This Computer Wizard .....	721
	Performing a local recovery by using the Recover This Computer Wizard .....	721
	Performing a remote recovery by using the Recover This Computer Wizard .....	722
	Installing network controller drivers .....	722
	Configuring network adapter settings .....	723
	About the simplified volume layout view .....	723
	About Advanced Disk Configuration .....	724
	Microsoft SQL Server recovery notes .....	727

	Microsoft Exchange recovery notes .....	728
	SharePoint Portal Server recovery notes .....	728
	About using Simplified Disaster Recovery with the Central Admin Server Option .....	728
	Best practices for Simplified Disaster Recovery .....	729
Appendix A	Symantec Backup Exec Agent for Windows .....	731
	About the Agent for Windows .....	731
	Requirements for the Agent for Windows .....	732
	Stopping and starting the Agent for Windows .....	733
	About establishing a trust between the Backup Exec server and a remote computer .....	734
	Establishing a trust for a remote computer .....	735
	About the Backup Exec Agent Utility for Windows .....	735
	Starting the Backup Exec Agent Utility .....	736
	Viewing the activity status of the remote computer in the Backup Exec Agent Utility .....	736
	Status options for the Backup Exec Agent Utility .....	736
	Viewing the activity status of the remote computer from the system tray .....	737
	Starting the Backup Exec Agent Utility automatically on the remote computer .....	737
	Setting the refresh interval on the remote computer .....	738
	About publishing the Agent for Windows to Backup Exec servers .....	738
	Configuring database access .....	742
	Removing a security certificate for a Backup Exec server that has a trust with the Agent for Windows .....	745
	About the Backup Exec Agent Utility Command Line Applet .....	746
	Using the Backup Exec Agent Utility Command Line Applet .....	747
	Backup Exec Agent Utility Command Line Applet switches .....	747
Appendix B	Symantec Backup Exec Deduplication Option .....	751
	About the Deduplication Option .....	752
	Deduplication methods for Backup Exec agents .....	754
	Requirements for the Deduplication Option .....	755
	About installing the Deduplication Option .....	757
	About OpenStorage devices .....	757
	Editing the properties of an OpenStorage device .....	758
	About deduplication disk storage .....	760
	Editing the properties of a deduplication disk storage device .....	761

Changing the password for the logon account for deduplication disk storage .....	769
About sharing a deduplication device between multiple Backup Exec servers .....	770
About direct access sharing of storage devices .....	771
Selecting storage devices for direct access sharing .....	771
Editing the properties for direct access .....	772
About client-side deduplication .....	773
About backup jobs for deduplication .....	774
About copying deduplicated data between OpenStorage devices or deduplication disk storage devices by using optimized duplication .....	775
Copying deduplicated data between deduplication disk storage devices or OpenStorage devices by using optimized duplication .....	776
About copying deduplicated data to tapes .....	778
About using deduplication with encryption .....	778
About restoring deduplicated data .....	778
About disaster recovery of a deduplication disk storage device .....	778
Preparing for disaster recovery of a deduplication disk storage device .....	779
About disaster recovery of OpenStorage devices .....	780
Appendix C	
Symantec Backup Exec Agent for VMware .....	781
About the Agent for VMware .....	781
Requirements for using the Agent for VMware .....	782
About installing the Agent for VMware .....	783
About adding VMware vCenter and ESX servers .....	783
About backing up VMware data .....	783
Setting default backup options for virtual machines .....	784
Virtual machine backup options .....	785
How Backup Exec automatically backs up new virtual machines during a backup job .....	788
How Backup Exec backs up Microsoft application data on virtual machines .....	788
Requirements for backing up Microsoft application data on virtual machines .....	789
About protecting databases and applications with the Symantec VSS Provider .....	790
Changing the log truncation setting of the Symantec VSS Provider .....	791
About restoring VMware resources .....	791

	VMware restore options .....	792
	VMware restore redirection options .....	794
Appendix D	Symantec Backup Exec Agent for Microsoft Hyper-V .....	797
	About the Agent for Microsoft Hyper-V .....	797
	Requirements for using the Agent for Microsoft Hyper-V .....	798
	About installing the Agent for Microsoft Hyper-V .....	800
	About upgrading from the Agent for Microsoft Virtual Servers .....	800
	About backing up Microsoft Hyper-V virtual machines .....	800
	Microsoft Hyper-V backup options .....	802
	How Granular Recovery Technology works with the Agent for Microsoft Hyper-V .....	804
	How Backup Exec automatically protects new virtual machines during a backup job .....	804
	About restoring Microsoft Hyper-V virtual machines .....	805
	About backing up and restoring highly available Hyper-V virtual machines .....	805
	How Backup Exec protects Microsoft application data on virtual machines .....	806
	Requirements for protecting Microsoft application data on virtual machines .....	807
Appendix E	Symantec Backup Exec Agent for Microsoft SQL Server .....	809
	About the Agent for Microsoft SQL Server .....	809
	Requirements for using the SQL Agent .....	811
	About installing the SQL Agent .....	811
	How to use Backup Exec logon accounts for SQL databases .....	812
	About backup strategies for SQL .....	812
	SQL backup strategy recommendations .....	813
	About consistency checks for SQL .....	814
	How to use snapshot technology with the SQL Agent .....	814
	About backing up SQL databases .....	815
	SQL backup options .....	817
	About automatic exclusion of SQL data during volume level backup .....	823
	How to back up SQL transaction logs .....	823
	About SQL 2005 or later database snapshots .....	824
	About reverting SQL 2005 or later databases using database snapshots .....	825
	About restoring SQL databases .....	825

About restoring encrypted SQL databases .....	826
How to restore from SQL transaction logs up to a point in time .....	826
How to restore from SQL transaction logs up to a named transaction .....	826
About restoring the SQL master database .....	827
Restarting SQL using database copies .....	827
Restoring the master database .....	829
About redirecting restores for SQL .....	830
About disaster recovery of a SQL Server .....	830
How to prepare for disaster recovery of SQL .....	830
Requirements for SQL disaster recovery .....	831
Disaster recovery of SQL .....	831
About recovering SQL manually .....	832

Appendix F	Symantec Backup Exec Agent for Microsoft Exchange Server .....	833
	About the Backup Exec Exchange Agent .....	834
	Requirements for using the Exchange Agent .....	834
	About installing the Exchange Agent .....	838
	About adding Exchange Servers and database availability groups .....	839
	About preferred server configurations .....	839
	Creating preferred server configurations .....	840
	Deleting preferred server configurations .....	840
	Editing settings for preferred server configurations .....	840
	Designating a default preferred server configuration .....	841
	Removing the default status for a preferred server configuration .....	841
	Manage Preferred Servers options .....	842
	Preferred Servers options .....	843
	Recommended configurations for Exchange .....	844
	Requirements for accessing Exchange mailboxes .....	845
	Backup strategies for Exchange .....	846
	Automatic exclusion of Exchange data during volume-level backups .....	848
	About the circular logging setting for Exchange .....	848
	How Granular Recovery Technology works with the Exchange Information Store .....	849
	About Backup Exec and Microsoft Exchange Web Services .....	849
	Snapshot and offhost backups with the Exchange Agent .....	850
	Configuring a snapshot backup for Exchange data .....	851

Troubleshooting Exchange Agent snapshot and offhost jobs .....	852
About backing up Exchange data .....	852
Microsoft Exchange backup options .....	854
About restoring Exchange data .....	857
Requirements for restoring Exchange .....	857
Configuring a database in Exchange .....	858
About restoring data using the Exchange 2003/2007 recovery storage group or Exchange Server 2010 recovery database .....	858
About restoring Exchange data from snapshot backups .....	860
About redirecting Exchange restore data .....	860
About redirecting Exchange mailbox items .....	861
How to prepare for disaster recovery of Exchange Server .....	862
Recovering from a disaster for Exchange .....	862

Appendix G	Symantec Backup Exec Agent for Microsoft SharePoint .....	865
	About the Agent for Microsoft SharePoint .....	866
	About installing the Agent for Microsoft SharePoint .....	866
	Requirements for the Agent for Microsoft SharePoint .....	867
	About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010 .....	868
	About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0 .....	869
	About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0 .....	869
	About adding a Microsoft SharePoint server farm to the list of servers .....	870
	About deleting a Microsoft SharePoint server farm from the list of servers .....	871
	About backing up Microsoft SharePoint data .....	871
	Microsoft SharePoint backup options .....	872
	About restoring Microsoft SharePoint data .....	872
	Microsoft SharePoint restore options .....	874
	Disabling or enabling communication between a Microsoft SharePoint Web server and Backup Exec .....	876
	Viewing SharePoint farm properties .....	876
	SharePoint farm properties .....	876
	Recovering Microsoft SharePoint 2010 data after a disaster .....	877
	Recovering Microsoft SharePoint 2007 data after a disaster .....	881

Appendix H	Symantec Backup Exec Agent for Oracle on Windows or Linux Servers .....	885
	About the Backup Exec Oracle Agent .....	885
	About installing the Oracle Agent .....	886
	Configuring the Oracle Agent on Windows computers and Linux servers .....	887
	Configuring an Oracle instance on Windows computers .....	888
	Viewing an Oracle instance on Windows computers .....	890
	Editing an Oracle instance on Windows computers .....	891
	Deleting an Oracle instance on Windows computers .....	892
	Enabling database access for Oracle operations on Windows computers .....	892
	Configuring an Oracle instance on Linux servers .....	893
	Viewing an Oracle instance on Linux servers .....	894
	Editing an Oracle instance on Linux servers .....	895
	Deleting an Oracle instance on Linux servers .....	895
	Enabling database access for Oracle operations on Linux servers .....	896
	About authentication credentials on the Backup Exec server .....	897
	Setting authentication credentials on the Backup Exec server for Oracle operations .....	898
	Deleting an Oracle server from the Backup Exec server's list of authentication credentials .....	899
	About Oracle instance information changes .....	900
	About backing up Oracle databases .....	900
	About backing up Oracle RAC databases .....	901
	About performing a DBA-initiated backup job for Oracle .....	902
	Oracle backup options .....	903
	About restoring Oracle resources .....	904
	About DBA-initiated restore for Oracle .....	906
	About redirecting a restore of Oracle data .....	906
	Requirements for recovering the complete Oracle instance and database using the original Oracle server .....	907
	Recovering the complete Oracle instance and database using the original Oracle server .....	907
	Requirements for recovering the complete Oracle instance or database to a computer other than the original Oracle server .....	908
	Recovering the complete Oracle instance or database to a computer other than the original Oracle server .....	909
	Troubleshooting the Oracle Agent .....	910

Changing the SqlplusTimeout for Oracle instances on Windows computers .....	913
Changing the SqlplusTimeout for Oracle instances on Linux computers .....	914
Changing the time-out for an automatic RMAN channel for Oracle instances on Windows computers .....	914
Changing the time-out for an automatic RMAN channel for Oracle instances on Linux computers .....	915
Updating the online redo log file path .....	915
Appendix I	
Symantec Backup Exec Agent for Enterprise Vault .....	917
About the Agent for Enterprise Vault .....	917
Requirements for the Enterprise Vault Agent .....	922
About installing the Enterprise Vault Agent .....	922
About backup methods for Enterprise Vault backup jobs .....	923
Enterprise Vault backup options .....	926
About backing up Enterprise Vault components .....	926
About consistency checks for Enterprise Vault databases and Compliance and Discovery Accelerator databases .....	929
About restoring Enterprise Vault .....	929
Enterprise Vault restore options .....	931
About restoring individual files and folders with the Enterprise Vault Agent .....	935
About automatic redirection of Enterprise Vault components under an Enterprise Vault server .....	935
About redirecting a restore for an Enterprise Vault component .....	936
Configuring Enterprise Vault to use the name of the new SQL Server that holds the Directory database .....	938
Best practices for the Enterprise Vault Agent .....	940
About the Backup Exec Migrator for Enterprise Vault .....	940
Backup Exec Migrator for Enterprise Vault requirements .....	941
How the Backup Exec Migrator works .....	941
About using staged migrations with Backup Exec and the Backup Exec Migrator .....	945
About Backup Exec Migrator events .....	946
About Backup Exec Migrator logs .....	946
About deleting files migrated by Backup Exec Migrator .....	947
Configuring the Backup Exec Migrator .....	948
About viewing migrated Enterprise Vault data .....	956
About retrieving migrated Enterprise Vault data .....	957

	About the Partition Recovery Utility .....	958
Appendix J	Symantec Backup Exec Agent for Lotus Domino .....	963
	About the Agent for Lotus Domino Server .....	964
	Lotus Domino Agent requirements .....	964
	About installing the Lotus Domino Agent on the Backup Exec server .....	966
	About the Lotus Domino Agent and the Domino Attachment and Object Service (DAOS) .....	966
	Best practices for restoring the missing .nlo files .....	967
	Viewing Lotus Domino databases .....	968
	About backing up Lotus Domino databases .....	968
	About selecting backup options for Lotus Domino databases .....	970
	Lotus Domino Agent backup options .....	970
	About automatic exclusion of Lotus Domino files during volume-level backups .....	971
	About supported Lotus Domino database configurations .....	971
	About Lotus Domino transaction logs .....	972
	About restoring Lotus Domino databases .....	973
	Restoring Lotus Domino databases .....	974
	Lotus Domino Agent restore options .....	975
	About redirecting restore jobs for Lotus Domino databases .....	977
	About redirecting the restore of DAOS NLO files .....	977
	How to prepare for disaster recovery on a Lotus Domino server .....	977
	Recovering a Lotus Domino server from a disaster .....	978
	About disaster recovery of a Lotus Domino server using archive logging .....	979
	Disabling the monitor change journal .....	980
	Recovering the Lotus Domino server, databases, and transaction logs when archive logging is enabled .....	980
	Re-enabling the monitor change journal .....	981
	Recovering of a Lotus Domino server that uses circular logging .....	982
Appendix K	Symantec Backup Exec Agent for Microsoft Active Directory .....	985
	About the Agent for Microsoft Active Directory .....	985
	Requirements for the Agent for Microsoft Active Directory .....	986
	About installing the Agent for Microsoft Active Directory .....	987
	How the Agent for Microsoft Active Directory works .....	987

How Granular Recovery Technology works with Active Directory and ADAM/AD LDS backups .....	988
Editing defaults for Active Directory and ADAM/AD LDS backup jobs .....	989
About backing up Active Directory and ADAM/AD LDS .....	989
Microsoft Active Directory backup job options .....	990
About restoring individual Active Directory and ADAM/AD LDS objects .....	991
About recreating purged Active Directory and ADAM/AD LDS objects .....	992
Resetting the Active Directory computer object and the computer object account .....	993

## Appendix L

Symantec Backup Exec Central Admin Server Option .....	995
About the Central Admin Server Option .....	996
Requirements for installing CASO .....	998
How to choose the location for CASO storage and media data .....	999
About installing the Central Admin Server Option .....	1001
Push-installing a managed Backup Exec server from the central administration server .....	1002
About Managed Backup Exec Server Configuration options .....	1006
About installing a managed Backup Exec server across a firewall .....	1007
Changing the dynamic port on the SQL Express instance in CASO to a static port .....	1008
Creating an alias for a managed Backup Exec server when a SQL Express instance is used .....	1009
Creating an alias for a managed Backup Exec server when a SQL 2005 or SQL 2008 instance is used .....	1010
Opening a SQL port in CASO for a SQL 2005 or 2008 instance .....	1010
About upgrading an existing CASO installation .....	1011
Upgrading an existing central administration server .....	1012
About upgrading an existing managed Backup Exec server .....	1013
Changing a Backup Exec server to a central administration server .....	1013
Changing a Backup Exec server to a managed Backup Exec server .....	1014
Changing a managed Backup Exec server to a standalone Backup Exec server .....	1015
About reducing network traffic in CASO .....	1015

About CASO catalog locations .....	1016
Changing the settings for a managed Backup Exec server .....	1018
Managed Backup Exec server settings .....	1018
What happens when CASO communication thresholds are reached .....	1025
Enabling communications between the managed Backup Exec server and the central administration server .....	1025
Disabling communications between the managed Backup Exec server and the central administration server .....	1026
About alerts and notifications in CASO .....	1026
Copying alert configurations to managed Backup Exec servers .....	1027
Enabling managed Backup Exec servers to use any available network interface card .....	1028
About job delegation in CASO .....	1028
About copying jobs instead of delegating jobs in CASO .....	1029
About adding storage devices in a CASO environment .....	1029
How to use Backup Exec server pools in CASO .....	1029
Selecting a Backup Exec server pool for backups .....	1030
Creating a Backup Exec server pool .....	1031
Adding managed Backup Exec servers to a Backup Exec server pool .....	1031
Deleting a Backup Exec server pool .....	1032
Removing a managed Backup Exec server from a Backup Exec server pool .....	1032
How centralized restore works in CASO .....	1033
How CASO restores data that resides on multiple storage devices .....	1034
Best practices for centralized restore in CASO .....	1035
About restoring from the central administration server .....	1035
About recovering failed jobs in CASO .....	1035
Pausing a managed Backup Exec server .....	1037
Resuming a paused managed Backup Exec server .....	1038
Stopping Backup Exec services for a managed Backup Exec server .....	1038
Starting Backup Exec services for a managed Backup Exec server .....	1039
Viewing managed Backup Exec server properties .....	1039
Properties for central administration servers and managed Backup Exec servers .....	1039
Viewing the settings for a central administration server .....	1041
Settings for a central administration server .....	1041
Disaster Recovery in CASO .....	1043

	Troubleshooting CASO .....	1044
	Running the Backup Exec Utility for CASO operations .....	1044
	Uninstalling Backup Exec from the central administration server .....	1045
	Uninstalling Backup Exec from a managed Backup Exec server .....	1046
Appendix M	Symantec Backup Exec Advanced Disk-based Backup Option .....	1047
	About the Advanced Disk-based Backup Option .....	1047
	About installing the Advanced Disk-based Backup Option .....	1048
	About the synthetic backup feature .....	1048
	Requirements for synthetic backup .....	1049
	About true image restore for synthetic backups .....	1050
	About off-host backup .....	1052
	Requirements for off-host backup .....	1053
	Best practices for off-host backup .....	1053
	Advanced Disk-based Backup options .....	1054
	Troubleshooting the off-host backup .....	1055
	Off-host backup issues with hardware providers .....	1058
Appendix N	Symantec Backup Exec NDMP Option .....	1061
	About the NDMP Option .....	1062
	Requirements for using the NDMP Option .....	1062
	About installing the NDMP Option .....	1063
	About adding an NDMP server to Backup Exec .....	1063
	About sharing the devices on an NDMP server between multiple Backup Exec servers .....	1063
	About backing up NDMP resources .....	1063
	Backup options for NDMP .....	1064
	About including and excluding directories and files for NDMP backup selections .....	1066
	How to use patterns to exclude files and directories from an NDMP backup selection .....	1066
	How to duplicate backed up NDMP data .....	1068
	About restoring NDMP data .....	1068
	NDMP restore options .....	1069
	About redirecting restored NDMP data .....	1071
	Setting the default options for NDMP .....	1071
	Viewing the properties of an NDMP server .....	1071
	NDMP server properties .....	1072

Appendix O	Symantec Backup Exec Agent for Linux .....	1073
	About the Agent for Linux .....	1074
	About open files and the Agent for Linux .....	1074
	Requirements for the Agent for Linux .....	1074
	About installing the Agent for Linux .....	1075
	Installing the Agent for Linux .....	1076
	About the Backup Exec operators group for the Agent for Linux .....	1078
	About establishing trust for a remote Linux computer in the Backup Exec list of servers .....	1080
	Establishing trust and adding a remote Linux computer to the Backup Exec list of servers .....	1080
	Adding additional Backup Exec servers to which the Agent for Linux can publish information .....	1081
	About configuring the Agent for Linux .....	1081
	About excluding files and directories from backup jobs for Linux computers .....	1082
	Editing configuration options for Linux computers .....	1083
	Configuration options for Linux computers .....	1083
	About backing up a Linux computer by using the Agent for Linux .....	1090
	Linux backup options .....	1091
	About backing up Novell Open Enterprise Server (OES) components .....	1093
	About restoring data to Linux computers .....	1095
	About restoring Novell OES components .....	1095
	Restore job options for Linux computers .....	1095
	Edit the default backup job options for Linux computers .....	1096
	Default backup job options for Linux computers .....	1097
	Uninstalling the Agent for Linux .....	1100
	Manually uninstalling the Agent for Linux .....	1100
	Runtime scripts to remove when manually uninstalling the Agent for Linux .....	1102
	Starting the Agent for Linux daemon .....	1103
	Stopping the Agent for Linux daemon .....	1103
	Troubleshooting the Agent for Linux .....	1104
Appendix P	Symantec Backup Exec Agent for Mac .....	1107
	About the Agent for Mac .....	1108
	Requirements for the Agent for Mac .....	1108
	About the Backup Exec admin group on Macintosh systems .....	1108

Creating the Backup Exec admin group manually on Macintosh systems .....	1109
About installing the Agent for Mac .....	1110
Installing the Agent for Mac .....	1110
Uninstalling the Agent for Mac .....	1113
Manually uninstalling the Agent for Mac .....	1114
About configuring the Agent for Mac .....	1116
Editing configuration options for Macintosh computers .....	1116
Configuration options for Macintosh computers .....	1117
Starting the Agent for Mac .....	1122
Stopping the Agent for Mac .....	1123
About establishing trust for a remote Macintosh system in the Servers list .....	1123
Establishing trust and adding a remote Macintosh computer to the Backup Exec Servers list .....	1124
Adding additional Backup Exec servers to which the Agent for Mac can publish information .....	1124
About backing up data by using the Agent for Mac .....	1125
Editing the default backup options for Macintosh systems .....	1125
About excluding files and directories from backup jobs for Macintosh computers .....	1127
About restoring Macintosh systems .....	1128
Macintosh restore options .....	1128
Troubleshooting the Agent for Mac .....	1128

## Appendix Q

Symantec Backup Exec Remote Media Agent for Linux .....	1131
About the Remote Media Agent for Linux .....	1132
How the Remote Media Agent for Linux works .....	1133
Requirements for the Remote Media Agent for Linux .....	1133
About open files and the Remote Media Agent for Linux .....	1134
About installing the Remote Media Agent for Linux .....	1134
Installing the Remote Media Agent for Linux .....	1135
Uninstalling the Remote Media Agent for Linux .....	1138
Starting the Remote Media Agent for Linux daemon .....	1139
Stopping the Remote Media Agent for Linux daemon .....	1139
About establishing trust for a Remote Media Agent for Linux computer in the Backup Exec list of servers .....	1140
Establishing trust and adding a Remote Media Agent for Linux computer to the Backup Exec list of servers .....	1140
Adding additional Backup Exec servers to which Remote Media Agent for Linux can publish .....	1140

Finding simulated tape library files .....	1141
About the Backup Exec operators group for the Remote Media Agent for Linux .....	1142
Creating the Backup Exec operators group manually for the Remote Media Agent for Linux .....	1142
About adding a Linux server as a Remote Media Agent for Linux .....	1143
Adding a Linux server as a Remote Media Agent for Linux .....	1143
Remote Media Agent for Linux options .....	1144
Changing the port for communications between the Backup Exec server and the Remote Media Agent for Linux .....	1146
About creating storage device pools for devices attached to the Remote Media Agent for Linux .....	1146
Editing properties for the Remote Media Agent for Linux .....	1147
Remote Media Agent for Linux properties .....	1147
Deleting a Remote Media Agent for Linux from the Backup Exec list of servers .....	1148
Sharing a Remote Media Agent for Linux between multiple Backup Exec servers .....	1148
About backing up data by using the Remote Media Agent for Linux .....	1149
About restoring data by using the Remote Media Agent for Linux .....	1149
About the Tape Library Simulator Utility .....	1149
Creating a simulated tape library .....	1150
Simulated Tape Library options .....	1151
Viewing simulated tape libraries properties .....	1151
Simulated tape library properties .....	1152
Deleting a simulated tape library .....	1153
Managing simulated tape libraries from the command line .....	1154
Command line switches for the Tape Library Simulator Utility .....	1154
Troubleshooting the Remote Media Agent for Linux .....	1155
 Appendix R	
Symantec Backup Exec Storage Provisioning Option .....	1159
About the Storage Provisioning Option .....	1160
Requirements for the Storage Provisioning Option .....	1161
Requirements for the Storage Provisioning Option in a CASO environment .....	1161
About installing the Storage Provisioning Option .....	1161
Viewing storage array components in Backup Exec .....	1162

- About using the Configure Storage Wizard with the Storage Provisioning Option ..... 1162
- Configuring a storage array by using the Configure Storage Wizard ..... 1163
- Viewing properties for a storage array and its physical disks ..... 1164
  - Properties for a storage array and its physical disks ..... 1165
- About the Any Virtual Disk Storage device pool in the Storage Provisioning Option ..... 1171
- About virtual disks in the Storage Provisioning Option ..... 1171
  - Editing default options for a virtual disk on a storage array ..... 1173
  - Configuring a virtual disk on a storage array ..... 1173
  - Viewing properties for unconfigured virtual disks on a storage array ..... 1174
    - Properties for unconfigured virtual disks on storage arrays ..... 1174
    - Editing properties of virtual disks on storage arrays ..... 1180
    - Properties for virtual disks on storage arrays ..... 1180
- About hot spares in the Storage Provisioning Option ..... 1191
  - Adding a hot spare by using the Configure Storage Wizard ....
    - 1                    1                    9                    2
  - Changing a hot spare by using the Configure Storage Wizard ..... 1192
- Detecting a new storage array ..... 1193
- Renaming a virtual disk or storage array ..... 1193
- About identifying the physical disks of a virtual disk ..... 1194
  - Identifying the physical disks of a virtual disk ..... 1195
- Troubleshooting the Storage Provisioning Option ..... 1195

Appendix S      Symantec Backup Exec Archiving Option ..... 1197

- About the Archiving Option ..... 1198
- Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option ..... 1199
  - Requirements for the Exchange Mailbox Archiving Option ..... 1201
  - Requirements for the File System Archiving Option ..... 1204
- About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option ..... 1205
- How to calculate disk space requirements for the Exchange Mailbox Archiving Option ..... 1211
- How to calculate disk space requirements for the File System Archiving Option ..... 1214
- Installing the Backup Exec Archiving Option ..... 1217
  - About using the command line to install the Backup Exec Exchange Mailbox Archiving Option ..... 1218

About the Internet Information Services (IIS) 7.0 role services installed by Backup Exec .....	1218
About uninstalling or reinstalling the Archiving Option .....	1220
About installing Enterprise Vault on a Backup Exec server on which the Archiving Option is installed .....	1221
About Enterprise Vault services for the Archiving Option .....	1221
Repairing the Backup Exec Archiving Option .....	1222
How the Archiving Option works .....	1222
Types of data not included in archive jobs .....	1223
Best practices for the Archiving Option .....	1224
About creating an archive job .....	1225
Viewing the servers that have archiving jobs .....	1225
Setting archive job options .....	1226
Editing default settings for the Archiving Option .....	1230
Default settings for the Archiving Option .....	1231
About single instance storage of archived items .....	1233
Enabling single instance storage of archived items .....	1234
About synchronizing archive permissions and settings .....	1234
About vault stores in the Archiving Option .....	1235
Editing or viewing vault store properties .....	1236
Vault store properties .....	1236
About deleting an Archiving Option vault store .....	1237
Deleting a vault store .....	1238
About vault store partitions in the Archiving Option .....	1238
Editing vault store partition properties .....	1239
Vault store partition properties .....	1239
About archives in the Archiving Option .....	1240
Editing archive properties .....	1240
Deleting an archive .....	1241
Archive properties .....	1241
About Archiving Option operation entries in the audit log .....	1242
About Exchange mailbox groups in archive jobs .....	1242
Managing Exchange mailbox groups .....	1243
Manage mailbox groups options .....	1244
Mailbox group options for mailbox group details .....	1245
About deleting archived data from its original location .....	1247
About archive settings in the Archiving Option .....	1247
Manage Archive Settings options .....	1247
Archive Settings Details .....	1248
About retention categories for archived items .....	1250
About managing index locations in the Backup Exec Archiving Option .....	1254
Viewing index locations .....	1255

Adding a new index location .....	1255
Deleting an index location .....	1256
Opening or closing an index location .....	1257
Manage Index Locations options .....	1257
About restoring items from the archives .....	1259
About searching for data in the archives .....	1260
About deleting data from the archives .....	1260
Deleting data from the archives .....	1260
Delete from Archive options .....	1261
About backing up and restoring the Archiving Option components	
from a remote Backup Exec server .....	1261
Preventing the deletion of expired archived items from an	
archive .....	1262
About backing up Archiving Option components .....	1262
About consistency checks for Archiving Option databases .....	1265
About disabling backup mode for Archiving Option	
components .....	1265
About restoring an Archiving Option component .....	1265
About running the Backup Exec Utility to complete redirected	
restores of Archiving Option components .....	1266
Running the Backup Exec Utility to complete a redirected restore	
of the Archiving Option databases .....	1268
Running the Backup Exec Utility before redirecting the restore	
of an Archiving Option vault store partition .....	1268
Running the Backup Exec Utility before redirecting the restore	
of Archiving Option index files .....	1269
Running the Backup Exec Utility to complete Archiving Option	
operations .....	1270
About moving Archiving Option components to a new location .....	1270
Troubleshooting archive jobs .....	1271
Viewing the Enterprise Vault event log for Archiving Option	
events .....	1272
Reports for the Archiving Option .....	1272
About Backup Exec Virtual Vault .....	1273
About the Backup Exec Outlook Add-In .....	1275
About installing the Backup Exec Outlook Add-In to end users'	
computers .....	1276
About configuring Outlook in cached Exchange mode .....	1281
Best practices for Virtual Vault .....	1281
About the Vault Cache .....	1281
About Vault Cache synchronization .....	1282
About preemptive caching .....	1284

	About the temporary cache location on the Backup Exec server .....	1284
	About enabling and disabling Virtual Vault .....	1286
Appendix T	Accessibility and Backup Exec .....	1289
	About accessibility and Backup Exec .....	1289
	About keyboard shortcuts in Backup Exec .....	1290
	Home tab keyboard shortcuts .....	1290
	Backup and Restore tab keyboard shortcuts .....	1291
	Storage tab keyboard shortcuts .....	1299
	Reports tab keyboard shortcuts .....	1307
	General keyboard navigation within the Backup Exec user interface .....	1307
	Keyboard navigation within dialog boxes in Backup Exec .....	1308
	List box navigation in Backup Exec .....	1309
	Tabbed dialog box navigation in Backup Exec .....	1309
	About setting accessibility options .....	1309
	Glossary .....	1311
	Index .....	1317

# Introducing Backup Exec 2012

This chapter includes the following topics:

- [About Backup Exec](#)
- [How Backup Exec works](#)
- [What's new in Backup Exec 2012](#)
- [What's new in Backup Exec 2012 agents and options](#)

## About Backup Exec

Symantec Backup Exec 2012 is a high-performance data management solution for Windows® servers networks. With its client/server design, Backup Exec provides fast, reliable backup and restore capabilities for servers, applications and workstations across the network.

Backup Exec is available in several configurations that can accommodate networks of all sizes. In addition, Backup Exec's family of agents and options offer solutions for scaling your Backup Exec environment and extending platform and feature support.

You can find more information about Backup Exec's host of solutions at the following URL:

[www.BackupExec.com](http://www.BackupExec.com)

See “[What's new in Backup Exec 2012](#)” on page 46.

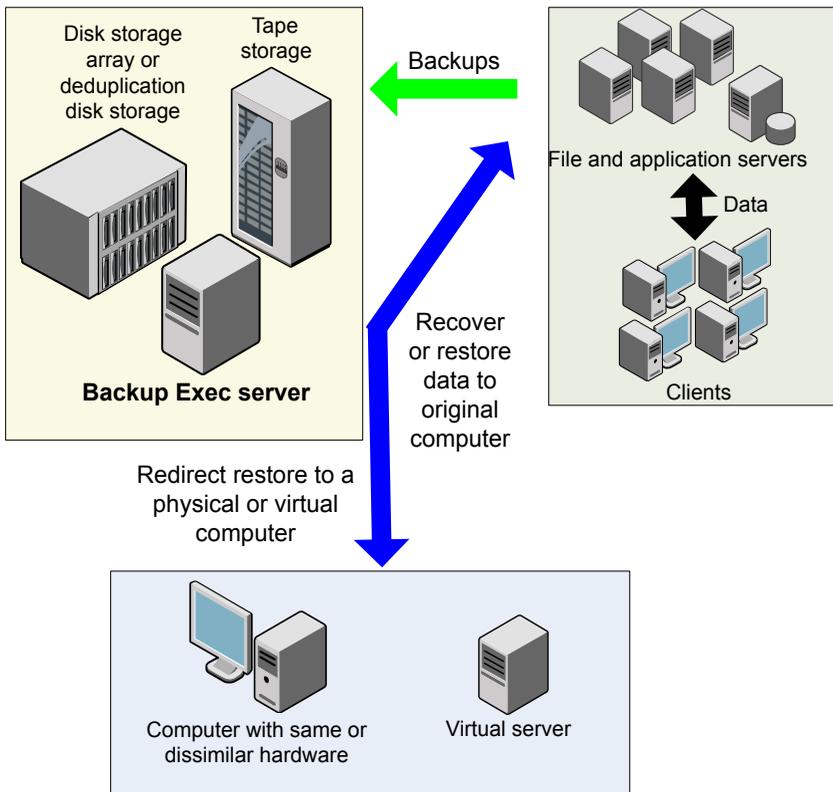
See “[What's new in Backup Exec 2012 agents and options](#)” on page 51.

See “[How Backup Exec works](#)” on page 44.

# How Backup Exec works

You use the Backup Exec Administration Console to interact with Backup Exec for tasks like submitting backups, restoring data, configuring storage, and monitoring jobs. You can run the Administration Console from the Backup Exec server, which is a Windows server on which Backup Exec is installed, or from a remote computer. After backups, restores or other operations are created, the Backup Exec server processes the jobs or delegates the jobs for processing in multi-Backup Exec server environments.

**Figure 1-1** Backup and restore functionality for the entire network



Backup Exec includes the following features:

- Convenient backup scheduling  
Backup Exec administrators can set up scheduled backups for Windows and Linux computers across the network. Backup Exec's flexible calendar-based administration lets you easily schedule backups for processing during off-peak hours.

- **Complete system recovery**

Backup Exec's Simplified Disaster Recovery takes all of the guesswork out of quickly recovering an entire system. While configuring a backup, you get a clear indication that you have selected the data that is necessary to perform a Simplified Disaster Recovery-enabled backup. With a Simplified Disaster Recovery disk and Backup Exec's **Restore Wizard**, you can quickly recover a computer to a system with the same type of hardware or with dissimilar hardware.
- **Comprehensive monitoring and intuitive mechanisms for everyday tasks**

The Home tab lets you view statistics for your entire Backup Exec environment. From the Servers view, you can monitor the backup status for all of the computers on your network. Interactive alerts display the situations that require your attention.

Backup results can be viewed from a backup's job history. The job history contains statistics, errors, and other information pertaining to the backup. Backup Exec's catalog is a database of all backed up data, and Backup Exec uses the catalog to track restore selections.

Wizards guide you through most Backup Exec operations, including the creation of backup and restore jobs, and configuration of storage.
- **Automated data lifecycle management for disk and cloud storage**

Backup Exec uses data lifecycle management to automatically expire backup sets on disk and cloud storage. Backup Exec reclaims the storage space when the amount of time that you specify when you create the backup job expires. If backup sets are dependent on other backup sets, then Backup Exec does not expire the data until all expiration dates are reached. You do not need to manage media when you keep backup data on disk or cloud storage.
- **Simplified device and media management**

Backup Exec uses the Advanced Device and Media Management (ADAMM) feature to manage data retention on tape and disk cartridge media. ADAMM expires the backup sets that are stored on media according to a set of rules that you apply to the media. Through ADAMM, you can logically group similar storage devices together in storage device pools to share the backup workload. Backup Exec's robust management functionality provides you with straightforward tools to organize and monitor all of your disk, cloud, and tape storage.

See [“What's new in Backup Exec 2012”](#) on page 46.

See [“What's new in Backup Exec 2012 agents and options”](#) on page 51.

# What's new in Backup Exec 2012

This release of Backup Exec includes the following new features and capabilities:

**Table 1-1**      What's new in Backup Exec 2012

Item	Description
<b>New user interface</b>	<p>Backup Exec has a new user interface that features a server-centric model that lets you easily back up and restore servers and multi-server distributed applications.</p> <p>With Backup Exec's new tabs, you can move throughout the main areas of the application quickly to monitor and configure backup and restore jobs. Backup Exec's new ribbon bar lets you quickly set up and schedule backups, launch restores, and configure storage.</p> <p>See <a href="#">“About the administration console”</a> on page 131.</p>
<b>Updated Home Tab and management</b>	<p>The <b>Home</b> tab is a central location from which you can quickly access or view the Backup Exec features that you use frequently. From the <b>Home</b> tab, you can manage alerts, view server status, monitor disk storage utilization, and more.</p> <p>Servers or applications can be grouped into logical containers for easier monitoring.</p> <p>See <a href="#">“About the Home tab”</a> on page 136.</p>
<b>New backup paradigm</b>	<p>A new backup paradigm eliminates the need to create policies to combine multiple related operations in a backup job. For example, you no longer have to create a policy to include scheduled full and incremental backups in a backup job. These backups are now created and scheduled as part of the backup workflow.</p> <p>Simplified scheduling lets you configure the most convenient run times for your backup jobs.</p> <p>See <a href="#">“Backing up data”</a> on page 163.</p>

**Table 1-1** What's new in Backup Exec 2012 *(continued)*

Item	Description
<p><b>Guided restore</b></p>	<p>The <b>Restore Wizard</b> guides you through a process that is designed specifically for the type of data that you want to restore. For example, when you restore application data, you are prompted only with the options that apply to that application's data. The <b>Restore Wizard</b> guides you through restoring an entire server, file and folders, volumes, and application data.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>
<p><b>Interactive alerts</b></p>	<p>Alerts are now associated with their source. You can easily distinguish and respond to alerts that are associated with servers, jobs, and storage devices. Global active alerts appear on the <b>Home</b> tab, so you can monitor all Backup Exec alerts at a glance.</p> <p>See <a href="#">“About alerts”</a> on page 279.</p>
<p><b>New storage handling</b></p>	<p>A wizard helps you to configure all of the following types of storage:</p> <ul style="list-style-type: none"> <li>■ Disk</li> <li>■ Tape</li> <li>■ Deduplication</li> <li>■ Network</li> <li>■ Cloud storage</li> <li>■ Storage pools</li> </ul> <p>Disk storage is easier to create now that Backup Exec chooses the best location to store your backups. Backup Exec provides storage trending, and capacity monitoring and reporting.</p> <p>See <a href="#">“About the Configure Storage wizard”</a> on page 145.</p>

**Table 1-1** What's new in Backup Exec 2012 *(continued)*

Item	Description
<p><b>Simplified Disaster Recovery</b></p>	<p>Backup Exec Simplified Disaster Recovery (SDR) replaces Intelligent Disaster Recovery (IDR).</p> <p>SDR provides the following new features:</p> <ul style="list-style-type: none"> <li>■ Pre-built 32-bit and 64-bit recovery DVDs are included with the product media so you can quickly recover from any supported operating system.</li> <li>■ SDR keeps disaster recovery (.dr) information for the systems that the Backup Exec server backs up, so you can conveniently recover a system to its last backup.</li> <li>■ SDR tracks critical backup sets so you can quickly recover a failed computer to a bootable point, after which you can complete the recovery with a recovery wizard.</li> <li>■ SDR no longer requires you to have the original Windows installation media available when you create a bootable recovery disk.</li> <li>■ SDR uses Symantec System Recovery 'Restore Anywhere' technology to restore backups to computers with dissimilar hardware.</li> </ul> <p>See <a href="#">"About Simplified Disaster Recovery"</a> on page 704.</p>
<p><b>Conversion to a virtual machine</b></p>	<p>You can back up a physical computer and convert it to a virtual machine either simultaneously with the backup job or after the backup job. You can also convert an existing backup set to a virtual machine. This feature enables business continuity for both Hyper-V and VMware environments.</p> <p>See <a href="#">"About conversion to virtual machines"</a> on page 437.</p>

**Table 1-1** What's new in Backup Exec 2012 *(continued)*

Item	Description
<b>Improved method of updating the Backup Exec server and remote computers</b>	<p>When you use LiveUpdate to update the Backup Exec server, the Backup Exec services are restarted only once, regardless of the number of updates that are installed.</p> <p>When a Backup Exec server is updated, an alert is generated to warn you that the remote computers need the same update. You can update the remote computers immediately, at a scheduled time, or on a recurring schedule. You can also update a group of remote computers together.</p>
<b>Reporting improvements</b>	<p>Reports include the following improvements:</p> <ul style="list-style-type: none"> <li>■ Color coding highlights important data and prominent titles.</li> <li>■ Improved sizing of the information that is included in the reports.</li> <li>■ New columns provide additional information.</li> <li>■ Reports in HTML or PDF can be assigned to notification recipients.</li> </ul> <p>See <a href="#">“About reports in Backup Exec”</a> on page 556.</p>
<b>Enhanced search for restore</b>	<p>You can now perform a search of backed up data with more granular detail. For example, you can search for mailbox data by subject, SQL databases by name, and SharePoint data by document name. You can also copy and save the search criteria to use for future searches.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>

**Table 1-1** What's new in Backup Exec 2012 *(continued)*

Item	Description
<p><b>Improved notification</b></p>	<p>You can configure Backup Exec to notify people by email or text message when alerts occur. Backup Exec uses SMTP for email notifications and supports SMTP authentication. Notification email messages can be sent to any email address, including Microsoft Outlook, Lotus Notes, and Web-based email applications such as Gmail or Yahoo mail.</p> <p>See <a href="#">“About notifications for alerts”</a> on page 288.</p>
<p><b>Discover data to back up</b></p>	<p>You can configure Backup Exec to browse the network and discover application data and servers that have not been backed up.</p> <p>See <a href="#">“Configuring Backup Exec to discover data to back up”</a> on page 469.</p>
<p><b>True image restore for synthetic backups</b></p>	<p>True image restore is now automatically enabled by default. For true image restore, Backup Exec collects the information that is required to detect files and the directories that have been moved, renamed, or newly installed from a tar or zip archive. With true image restore enabled, Backup Exec compares path names with path names from the previous full or incremental backup. If a name is new or changed, the file or directory is backed up.</p> <p>See <a href="#">“About true image restore for synthetic backups”</a> on page 1050.</p>
<p><b>Checkpoint restart enhancements</b></p>	<p>Checkpoint restart now supports restarting from points of failure on volume, file, and folder backups of local and remote servers.</p> <p>See <a href="#">“About using checkpoint restart”</a> on page 538.</p>

**Table 1-1**      What's new in Backup Exec 2012 *(continued)*

Item	Description
<b>New PowerShell interface</b>	<p>The Backup Exec Command Line Applet has been completely redesigned to support PowerShell commands.</p> <p>You can find more information in the following location:</p> <p>Installation Directory\Modules\BEMCLI\about_BEMCLI_Cmdlets.help.txt</p>

## What's new in Backup Exec 2012 agents and options

This release of Backup Exec includes the following new features and capabilities in the agents and options:

**Table 1-2** What's new in Backup Exec 2012 agents and options

Item	Description
<b>Deduplication Option</b>	<p>The following new features are available:</p> <ul style="list-style-type: none"><li>■ Optimized duplication for backup sets that are enabled for Granular Recovery Technology. This enables off-site replication to be more efficient. Optimized duplication is available for OpenStorage devices from selected vendors. You can find a list of compatible devices at the following URL: <a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a></li><li>■ Improved deduplication ratios for Hyper-V backups when the Granular Recovery Technology option is enabled.</li><li>■ Improved deduplication across virtual machines.</li><li>■ Linux client-side deduplication, which allows a Linux client to locally deduplicate data and send it directly to a deduplication disk storage device or to a PureDisk appliance.</li></ul> <p>See “<a href="#">About copying deduplicated data between OpenStorage devices or deduplication disk storage devices by using optimized duplication</a>” on page 775.</p>

**Table 1-2** What's new in Backup Exec 2012 agents and options (*continued*)

Item	Description
<p><b>Agent for VMware</b></p>	<p>The Agent for VMware now includes the ability to eliminate unused sectors from backups of Windows-based basic, dynamic, and GPT disks. This applies even if the disks are on a non-VMFS-based datastore, such as NFS or iSCSI.</p> <p>The Agent for VMware now includes the following new features to provide compatibility with VMware's vSphere 5.0:</p> <ul style="list-style-type: none"> <li>■ Locks and unlocks the virtual machine automatically during backup and restore operations to prevent activity by the Distributed Resource Scheduler (DRS) and Storage Distributed Resource Scheduler (SDRS).</li> <li>■ Enables the capabilities of the DRS and SDRS to be preserved.</li> <li>■ Provides the ability to redirect the restore to the most recent hardware version that is supported by the destination virtual environment. This includes hardware version 8.</li> <li>■ Supports the following restore options when Datastore Clusters and SDRS are present: <ul style="list-style-type: none"> <li>■ Restore to the original location from where the data was backed up.</li> <li>■ Restore to an unmanaged datastore.</li> <li>■ Restore directly to a datastore cluster. The SDRS properties are maintained.</li> <li>■ Restore directly to a datastore within a datastore cluster. The SDRS properties are not maintained.</li> </ul> </li> </ul> <p>See <a href="#">“About the Agent for VMware”</a> on page 781.</p>

**Table 1-2** What's new in Backup Exec 2012 agents and options (*continued*)

Item	Description
<b>Agent for Hyper-V</b>	<p>The following new features are available:</p> <ul style="list-style-type: none"> <li>■ Automatic disk optimization, which transfers only the virtual disk sectors that are in use. This reduces the amount of data that is transferred across the network and the amount of storage that is required.</li> <li>■ Support for incremental and differential backups.</li> <li>■ Support for granular recovery of individual items from Microsoft SharePoint.</li> <li>■ Improved deduplication ratios for Hyper-V backups when the Granular Recovery Technology option is enabled.</li> </ul> <p>See <a href="#">“About the Agent for Microsoft Hyper-V”</a> on page 797.</p>
<b>Agent for Microsoft Exchange Server</b>	<p>The Exchange Agent now provides the ability to restore mailbox or public folder items into PST files, which can be opened in Outlook or distributed to users.</p> <p>See <a href="#">“About restoring Exchange data”</a> on page 857.</p>
<b>Archiving Option</b>	<p>Archiving is now easier to perform as a result of being integrated as a stage in the backup workflow.</p> <p>See <a href="#">“About creating an archive job”</a> on page 1225.</p>

**Table 1-2** What's new in Backup Exec 2012 agents and options (*continued*)

Item	Description
<b>Agent for Microsoft SharePoint</b>	<p>The following new features are available:</p> <ul style="list-style-type: none"> <li>■ Database or Granular Recovery Technology (GRT) restores from differential backups and incremental backups. Restore jobs combine the last full backup with any differential backups or incremental backups to restore data more efficiently.</li> <li>■ The ability to redirect the restore of a SharePoint site to another site and redirect the site to a new path.</li> <li>■ The ability to search for SharePoint metadata in the Backup Exec catalog. The improved search feature makes it easier to locate the information that you want to restore. After you locate the data, you can restore it directly from the search result screen.</li> </ul> <p>See <a href="#">“About restoring Microsoft SharePoint data”</a> on page 872.</p>
<b>Agent for Mac</b>	<p>The Agent for Mac now allows backups of critical Macintosh server entities.</p> <p>See <a href="#">“About the Agent for Mac”</a> on page 1108.</p>
<b>Agent for Linux</b>	<p>The Agent for Linux allows backup of critical Linux server-based entities. The Agent for Linux also includes the capability to back up open files.</p> <p>See <a href="#">“About the Agent for Linux”</a> on page 1074.</p>
<b>Agent for Enterprise Vault</b>	<p>The Enterprise Vault Agent now supports Enterprise Vault v10.</p> <p>See <a href="#">“About the Agent for Enterprise Vault”</a> on page 917.</p>



# Installation

This chapter includes the following topics:

- About installing Backup Exec
- About the Environment Check
- About Microsoft SQL Server 2005 Express Edition components installed with Backup Exec
- About Backup Exec's standard features
- System requirements
- About the differences between a typical installation and a custom installation
- Installing a typical installation of Backup Exec
- Installing a custom installation of Backup Exec
- Installing additional Backup Exec options to the local Backup Exec server
- Special considerations for installing Backup Exec to remote computers
- Push-installing Backup Exec to remote computers
- About installing the Agent for Windows
- Installing the Remote Administrator
- Installing Backup Exec using the command line (silent mode)
- Installing a trial version of Backup Exec agents and options
- About the installation log
- Repairing Backup Exec
- About updating Backup Exec with LiveUpdate

- [Viewing installed updates](#)
- [Viewing license information](#)
- [Finding installed licenses in your environment](#)
- [About Backup Exec maintenance contract information](#)
- [About upgrading from previous versions of Backup Exec](#)
- [Post-installation tasks](#)
- [Uninstalling Backup Exec](#)
- [Uninstalling Backup Exec using the command line](#)
- [Uninstalling Backup Exec options from the local Backup Exec server](#)

## About installing Backup Exec

The Backup Exec installation wizard guides you through the process of installing Backup Exec and its agents and options. Using the installation wizard, you can install Backup Exec and its agents and options on a local computer or you can push-install them to a remote computer. The computer on which Backup Exec is installed is called the Backup Exec server. Additionally, you can install the Remote Administrator, which lets you administrate the Backup Exec server from a remote Windows server or workstation.

When you install Backup Exec, you have the following licensing options:

**Table 2-1** Licensing options

Item	Description
Enter serial numbers manually	You can type the serial numbers that are listed on your license certificate. Serial numbers contain one letter and 10 numbers, such as M0123456789. After you add your serial numbers, Backup Exec polls the Symantec Web service to verify the serial numbers. An Internet connection is required to enable Backup Exec to verify the serial numbers.

**Table 2-1** Licensing options (*continued*)

Item	Description
Import licenses from the Symantec License File	<p>You can import your Symantec License Files (.slf) from a network share or from a local drive.</p> <p>You may receive Symantec License Files in an email with your license certificate or you may need to go to the Symantec Licensing Portal Web site to obtain them. From the Symantec Licensing Portal Web site, you receive one file with all of the serial numbers that you registered. From the email, you receive multiple files with one serial number in each file.</p> <p>After installation, the .slf files can be found in the following locations:</p> <ul style="list-style-type: none"> <li>■ In Windows 2003: C:\Program Files\Common Files\Symantec Shared\Licenses</li> <li>■ In Windows 2008 and later: C:\Programdata\Symantec Shared\Licenses</li> </ul>
Install a 60-day trial version	<p>A 60-day trial version is available for Backup Exec and many of its agents and options. If you do not enter any serial numbers or Symantec license files during the installation process, a trial version is installed. If you enter a serial number or license file for Backup Exec, trial versions of many of the agents and options are available.</p>

After Backup Exec is installed, you can install additional agents and options from the Backup Exec user interface. You can install additional agents and options on the Backup Exec server or push-install Backup Exec or the Agent for Windows to remote computers.

Installation from a command line is also available. Command line installation is called silent mode installation. The silent mode installation uses the Setup.exe program on the Backup Exec installation media.

Backup Exec may install the following additional products during the installation process:

- Symantec LiveUpdate

- Microsoft XML Core Services (MSXML) 6.0
- Microsoft Report Viewer Redistributable 2005
- Microsoft.NET 4
- Microsoft Windows Imaging Component
- Microsoft SQL Express 2005 SP4
- MDAC 2.8 or later

See [“Installing a typical installation of Backup Exec”](#) on page 68.

See [“Installing a custom installation of Backup Exec”](#) on page 70.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

See [“Push-installing Backup Exec to remote computers”](#) on page 77.

See [“Push-installing the Agent for Windows to remote computers”](#) on page 86.

See [“Installing Backup Exec using the command line \(silent mode\)”](#) on page 104.

See [“Backup Exec pre-installation checklist”](#) on page 60.

## Backup Exec pre-installation checklist

Before you install Backup Exec, you should do the following:

- Run the Backup Exec Environment Check on the computer on which you want to install Backup Exec. The Environment Check analyzes the computer to make sure that the installation process can complete. If Backup Exec finds any configuration issues that can be fixed during the installation, or that may prevent the installation, warnings appear. Although the Environment Check runs automatically during installation, you may want to run it manually before you install Backup Exec or before you back up data with Backup Exec.  
See [“Checking your environment before installing”](#) on page 62.
- Install the storage device hardware (controller, drives, robotic libraries) on the Backup Exec server. Refer to the documentation that is included with your storage device hardware for installation instructions. Use the appropriate Windows hardware setup functions to configure your controller and storage devices. Refer to your Microsoft Windows documentation for more information.
- Check your Windows security settings to make sure that they work properly with the Backup Exec service account.  
See [“About the Backup Exec service account”](#) on page 512.
- If the drive on which you want to install Backup Exec is encrypted or compressed, and you want to use a default SQL Express database, verify that

an unencrypted and uncompressed drive is available for SQL Express installation.

- Check the computer name of the computer on which you want to install Backup Exec. It should only use standard ANSI characters. You may receive errors if you install Backup Exec on a computer with a name that uses non-standard characters.
- If you want to install Backup Exec to a non-English version of Windows, download the SQL Express SP4 setup file from the Microsoft Web site before you install Backup Exec if all of the following are true:
  - You want to use a local Backup Exec SQL Express instance.
  - You have non-English SQL Server instances on the computer on which you want to install Backup Exec.
- Exit all other programs, including your antivirus application.

## About the Environment Check

The Symantec Backup Exec Environment Check is a utility that runs on a computer automatically during installation and that reports the following:

- If the computer meets the minimum requirements for installation, such as the operating system, disk and physical memory, sufficient logon account privileges.  
 See “[System requirements](#)” on page 65.
- If the third-party software that uses Backup Exec ports is configured correctly.
- If required components are installed, and if they are compatible with Backup Exec.
- If previous versions of Backup Exec and Backup Exec options are installed.
- If storage device hardware and associated drivers are properly installed and recognized by the Windows operating system.

One of the following results is reported for each item:

**Table 2-2** Environment Check results

Result	Description
Passed	There are no incompatibilities to prevent the Backup Exec installation. For hardware, this result indicates that the hardware configuration is recognized by Backup Exec.

**Table 2-2** Environment Check results (*continued*)

Result	Description
Warning	An incompatibility with Backup Exec exists, but can be resolved during the Backup Exec installation.
Failed	An incompatibility with Backup Exec exists, and it will cause the installation to fail. Action is required before you can successfully install Backup Exec.

Although the Environment Check runs automatically during installation, you may want to run it manually before installing Backup Exec or before backing up data with Backup Exec.

See [“Checking your environment before installing”](#) on page 62.

## Checking your environment before installing

Although the Environment Check runs automatically during installation, you may want to run it manually before installing Backup Exec or before backing up data with Backup Exec.

See [“About the Environment Check”](#) on page 61.

### To check your environment before installing

- 1 From the installation media browser, click **Pre-installation**, and then click **Backup Exec**.
- 2 Click **Next**.
- 3 Do any of the following:

To check the configuration of the local computer    Check **Local Environment Check**.

To check the configuration of a remote computer    Check **Remote Environment Check**.

- 4 Click **Next**.
- 5 If you checked **Remote Environment Check** in step 3, do one of the following, and then click **Next**:

To select the name of a computer from a list    ■ Click **Add Server From List**.

- Select the computer from the list, and then click **Next**.

- |  |  |
|--|--|
| <p>To add the name of a computer manually</p>  | <ul style="list-style-type: none"> <li>■ Click <b>Add Server Manually</b>.</li> <li>■ In the <b>Domain</b> field, type the name of the domain.</li> <li>■ In the <b>Computer Name</b> field, type the name of the computer.</li> <li>■ Click <b>OK</b>.</li> <li>■ Type the user name and password for this computer.</li> <li>■ Click <b>OK</b>.</li> </ul> |
| <p>To remove the name of a computer from the list of computers on which the Environment Check runs</p> | <ul style="list-style-type: none"> <li>■ Select the computer from the list.</li> <li>■ Click <b>Remove</b>.</li> </ul>   |

- 6 If you want to save the results of the Environment Check, check **Save Results To**.

To change the location where the Environment Check results are saved, click **Change Path** to browse to a new location.

- 7 Click **Finish**.

## About Microsoft SQL Server 2005 Express Edition components installed with Backup Exec

The Backup Exec installation program installs Microsoft SQL Server 2005 Express Edition components that are required to run Backup Exec.

Backup Exec prompts you to do one of the following:

- Install the required Microsoft SQL Express components with Backup Exec and create a default Backup Exec instance.
- Select a Microsoft SQL Server 2005 (SP4) or SQL Server 2008 instance that already exists on the network on which you want to run Backup Exec.

During the installation process and the upgrade process, Backup Exec stops and starts the SQL service. Other user-created databases that use the SQL Server instance are unavailable during the process. To avoid such conflicts, you should install Backup Exec into its own SQL instance.

If you choose to install Backup Exec into an existing SQL 2005 instance, make sure that SQL 2005 Service Pack 4 or later is installed before you continue with the installation.

---

**Caution:** Backup Exec may not function properly if you install it into an existing SQL instance that uses case-sensitive collation. Symantec recommends that you avoid installing Backup Exec to a SQL instance that uses case-sensitive collation.

---

When Backup Exec is installed into an existing instance, the automated master database restore feature is not available. To recover the Master database, you must replace it with the Master database copy that Backup Exec automatically creates and updates when the Master database is backed up.

You cannot install multiple Backup Exec Databases on the same SQL Server instance.

---

**Note:** If you are installing a managed Backup Exec server, it is recommended that you select a local Microsoft SQL Server 2005 (SP4) instance or later on which to install the Backup Exec Database for this managed server. Do not select the same SQL Server instance that is used by the central administration server.

---

See [“System requirements”](#) on page 65.

## About Backup Exec's standard features

The following features are included with Backup Exec at no additional cost. When you install Backup Exec, you can select any of these features that you want to use.

**Table 2-3** Backup Exec's standard features

Feature	Description
<b>Tape Device Drivers</b>	Installs the Symantec tape device drivers for all supported tape devices that are attached to the server. If there are no tape devices attached to your Backup Exec server, uncheck this option.
<b>Online Documentation</b>	Installs the Backup Exec Administrator's Guide in a pdf file format.
<b>Enable Robotic Library Support</b>	Enables support for tape libraries, or optical robotic libraries and library storage systems. Backup Exec includes support for one drive in every robotic library. Each additional drive in a library requires a Library Expansion Option license.

**Table 2-3** Backup Exec's standard features (*continued*)

Feature	Description
<b>Copy Server Configurations</b>	Enables you to copy configuration settings and logon information between Backup Exec servers. This option is recommended for environments that contain multiple Backup Exec servers. This option is required for the Central Admin Server Option.
<b>Managed Backup Exec server</b>	Installs the managed Backup Exec server component of the Central Admin Server Option. You can install managed Backup Exec servers after you install a central administration server.
<b>Virtual Tape Library Support</b>	Provides support for every single-drive Virtual Tape Library (VTL). You must purchase the Virtual Tape Library Unlimited Drive Option to support additional drives in each VTL.  If you select this option, the <b>Enable Robotic Library Support</b> option is selected automatically. You cannot uncheck <b>Enable Robotic Library Support</b> unless you uncheck <b>Virtual Tape Library Support</b> .

All other options and agents require the purchase of additional licenses. Installing a trial version enables many options that must be purchased separately and are not included as part of Backup Exec.

If you have a licensed version of Backup Exec, you can use a trial version of most options and agents for a specified period of time.

See “[Installing a trial version of Backup Exec agents and options](#)” on page 114.

## System requirements

The following are the minimum system requirements to run this version of Backup Exec:

**Table 2-4** Minimum system requirements

Item	Requirements
Operating system	<p>You can find a list of compatible operating systems, platforms, and applications at the following URL:  <a href="http://entsupport.symantec.com/umi/V-269-1">http://entsupport.symantec.com/umi/V-269-1</a></p> <p>You cannot install a Backup Exec server on a computer that runs the Windows Server Core installation option of Windows Server 2008. You can only install the Backup Exec Agent for Windows on Server Core computers.</p> <p>You cannot install SQL Express or SQL Server 2005 on a Windows Server 2008 computer that is configured in a Read Only Domain Controller (RODC) role. The Read Only Domain Controller role does not let you use the local accounts that are required for SQL Express and SQL Server 2005. When you install Backup Exec on an RODC computer you must select a remote SQL instance for the Backup Exec Database.</p>
Additional application support	<p>You can use Backup Exec with Microsoft System Center Operation Manager (SCOM) 2007.</p>
Internet browser	<p>Internet Explorer 7.0 or later.</p>
Processor	<p>Intel Pentium, Xeon, AMD, or compatible.</p>
SQL Server or SQL Express	<p>Service Pack 4 is required.</p>
Memory	<p>Required: 512 MB RAM above the operating system's requirements.  Recommended: 2 GB RAM (or more for better performance)</p> <p><b>Note:</b> RAM requirements may vary depending on the operations performed, the options installed, and the specific computer configuration.</p> <p>For the Central Admin Server Option: 1 GB RAM is required; 2 GB RAM is recommended.</p> <p>Symantec Recovery Disk: 1 GB minimum (dedicated) for the multi-lingual version</p> <p>Virtual Memory Recommendations: 20 MB above the Windows recommended size for total paging file size (total for all disk volumes). Refer to your Microsoft Windows help documentation for instructions on how to view or set the paging file size.</p>

**Table 2-4** Minimum system requirements (*continued*)

Item	Requirements
Installation disk space	1.44 GB (Typical installation) 2.32 GB (Includes all options)  <b>Note:</b> Disk space requirements may vary depending on the operations performed, the options installed, and the specific system configuration. The Backup Exec database and catalogs require additional space. An additional 330 MB is required for SQL Express.
Other Hardware	The following hardware is recommended: <ul style="list-style-type: none"> <li>■ Network interface card or a virtual network adapter card.</li> <li>■ CD/DVD drive.</li> <li>■ (Recommended) A mouse.</li> </ul>
Storage Hardware	You can use storage media drives, robotic libraries, removable storage devices, and non-removable hard drives.  You can find a list of compatible types of storage at the following URL: <a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a>  Support is available for the first drive in each robotic library when you purchase Backup Exec. To enable support for each additional robotic library drive, you must purchase the Backup Exec Library Expansion Option.

See “[Installing a typical installation of Backup Exec](#)” on page 68.

See “[Installing a custom installation of Backup Exec](#)” on page 70.

## About the differences between a typical installation and a custom installation

The Backup Exec installation program provides two methods of installation: typical and custom. A typical installation is a simpler installation method than a custom installation and is designed for small or uncomplicated environments. For example, if you use a local Backup Exec server and a few Backup Exec agents or options, then a typical installation may be best for you. A custom installation is designed for large or complex environments. You can also use the custom installation method if you prefer to set all of your options. For example, if you use a remote Backup Exec server or use the Enterprise Server Option, you should perform a custom installation.

With a typical installation, Backup Exec makes the following decisions for you, based on common installation scenarios:

- Backup Exec is installed to a local Backup Exec server.
- SQL Express is installed with the default instance.
- Agents and options are installed if you enter the licenses for them. If you do not enter any licenses, a trial version of Backup Exec is installed.

---

**Note:** The installation program prevents you from selecting a license for an agent or option that is not compatible with the typical installation method, such as the Enterprise Server Option or the Archiving Option.

---

- LiveUpdate runs automatically.

See “[Installing a typical installation of Backup Exec](#)” on page 68.

See “[Installing a custom installation of Backup Exec](#)” on page 70.

## Installing a typical installation of Backup Exec

A typical installation is designed for small or uncomplicated environments. In a typical installation, Backup Exec makes many decisions for you, based on common installation scenarios. If you prefer to set all of your options, you should use the custom installation option.

See “[Installing a custom installation of Backup Exec](#)” on page 70.

See “[About the differences between a typical installation and a custom installation](#)” on page 67.

---

**Note:** Before you install, make sure that your licenses for Backup Exec and any agents or options are available. If you do not have licenses, go to the following URL to activate the product:

<https://licensing.symantec.com>

Licenses are required to install Backup Exec and its agents and options. However, you can install a trial version of Backup Exec without a license.

---

**To install a typical installation of Backup Exec**

- 1 From the installation media browser, click **Install Products**, and then select **Backup Exec**.

If the required version of Microsoft.NET Framework is not already installed on this computer, Backup Exec installs it. The installation of the Microsoft.NET Framework may take some time.

- 2 On the **Welcome** panel, read the license agreement, and then click **I accept the terms of the license agreement**.
- 3 Click **Next**.
- 4 On the **Installation Type** panel, click **Typical Installation**, and then click **Next**.

For first-time installations and upgrade installations, the Backup Exec Environment Check runs automatically.

- 5 Review the results of the Environment Check.
- 6 Do one of the following:
  - If the Environment Check does not reveal any issues that may prevent a successful installation of Backup Exec, click **Next**.
  - If the Environment Check reveals any issues that may prevent a successful installation of Backup Exec, click **Cancel** to exit the wizard. Correct the issues before you attempt to install Backup Exec again.
- 7 Select one of the following methods to enter licenses:

To enter serial numbers manually

**Note:** An Internet connection is required to validate the serial numbers. If you do not have an Internet connection, import the licenses from the Symantec License File or install a trial version.

Do the following in the order listed:

- In the **Serial number** field, type the appropriate serial number from your license certificate.
- Click **Add**.
- Repeat for each serial number for each option or agent that you want to install.
- Click **Next** to validate the serial numbers.

To import licenses from the Symantec License File

Do the following in the order listed:

- Click **Import from file**.
- Browse to the location of your license files, and then select the appropriate file.

To install a trial version

Do not type a serial number or import a license file. Proceed to the next step.

**8** Click **Next**.

You may be prompted to enter contact information.

**9** On the **Review Licenses** panel, check the check boxes for the products that you want to install, and then click **Next**.

**10** On the **Service Account** panel, provide a user name, password, and domain for an Administrator account that the Backup Exec system services can use.

You cannot install Backup Exec with an account that has a blank password on Windows Server 2003/2008 computers unless Windows is configured to allow it. If you try to do so, the following error message appears when Backup Exec services are created:

The given password is not correct for account [server]\[user name].

You can, however, configure Windows to allow for blank passwords. For more information, see your Windows documentation.

**11** If you want to change the directory where Backup Exec files are installed, click **Change**, and then select a new location.

**12** Click **Next**.

**13** Review the installation summary, and then click **Install**.

The installation process creates an installation log named Bkupinst2012.htm on the computer where Backup Exec is installed.

## Installing a custom installation of Backup Exec

A custom installation is designed for large or complex environments or for customers who prefer to set all of their options. For example, if you use a remote Backup Exec server or use the Central Admin Server Option, you should perform a custom installation. If you prefer to have Backup Exec set default options or if you have a small, uncomplicated environment, you can use the typical installation.

See [“Installing a typical installation of Backup Exec”](#) on page 68.

---

**Note:** If you install Backup Exec through terminal services and the installation media is on a shared drive (network share), you must install it using a UNC path. Installation by mapped drives is not supported in this situation.

---

---

**Note:** Before you install, make sure that your licenses for Backup Exec and any agents or options are available. If you don't have licenses, go to the following URL to activate the product:

<http://licensing.symantec.com>

Licenses are required to install Backup Exec and its agents and options. However, you can install a trial version of Backup Exec without a license.

---

### To install a custom installation of Backup Exec

- 1 From the installation media browser, click **Install Products**, and then select **Backup Exec**.

If the required version of Microsoft.NET Framework is not already installed on this computer, Backup Exec installs it. The installation of the Microsoft.NET Framework may take some time.

- 2 On the **Welcome** panel, read the license agreement, and then click **I accept the terms of the license agreement**.
- 3 Click **Next**.
- 4 On the **Installation Type** panel, click **Custom Installation**, and then click **Next**.
- 5 On the **Menu** panel, check **Local Installation**, and then select **Install Backup Exec software and options**.
- 6 Click **Next**.

For first-time installations and upgrade installations, the Backup Exec Environment Check runs automatically after you click **Next**.

- 7 Review the results of the Environment Check.
- 8 Do one of the following:
  - If the Environment Check does not reveal any issues that may prevent a successful installation of Backup Exec, click **Next**.
  - If the Environment Check reveals any issues that may prevent a successful installation of Backup Exec, click **Cancel** to exit the wizard. Correct the issues before you attempt to install Backup Exec again.
- 9 Select one of the following methods to enter licenses:

To enter serial numbers manually	Do the following in the order listed: <ul style="list-style-type: none"> <li>■ In the <b>Serial number</b> field, type the appropriate serial number from your license certificate.</li> <li>■ Click <b>Add</b>.</li> <li>■ Repeat for each license for each option or agent that you want to install.</li> <li>■ Click <b>Next</b> to validate the serial numbers.</li> </ul>
To import licenses from the Symantec License file	Do the following in the order listed: <ul style="list-style-type: none"> <li>■ Click <b>Import from file</b>.</li> <li>■ Browse to the location of your license files, and then select the appropriate file.</li> </ul>
To install a trial version	Do not type a serial number or import a license file. Proceed to the next step.

**10** Click **Next**.

You may be prompted to enter contact information.

**11** Check the check boxes for the agents or options that you want to install.**12** Click **Next**.

If you selected the File System Archiving Option or the Microsoft Exchange Mailbox Archiving Option, the Archiving Option Environment Check runs. The Archiving Option Environment Check verifies that the computer meets the minimum requirements for installing and configuring the options. If the computer does not meet the minimum requirements, you must uncheck the archiving options or fix the errors before you can continue with the installation.

**13** On the **Configure Options** panel, select any additional options that you want to install.

For example, you can select additional standard features, or you can select agents or options that are available for a trial installation.

**14** Click **Next**.**15** If you want to install Backup Exec for any additional languages, select the language, and then click **Next**.**16** On the **Destination** panel, do the following:

- Review the disk space requirements for the items that you selected to install.

- If you want to change the directory where the Backup Exec files are installed, click **Change**, and then select a new directory or create a new folder.  
Symantec recommends that you do not select a mount point as the destination directory because if you delete the mount point, Backup Exec is uninstalled.

**17** Click **Next**.

- 18** Provide a user name, password, and domain for an Administrator account that the Backup Exec system services can use, and then click **Next**.

You cannot install Backup Exec with an account that has a blank password on Windows Server 2003/2008 computers unless Windows is configured to allow it. If you try to do so, the following error message appears when Backup Exec services are created:

The given password is not correct for account [server]\[user name].

You can, however, configure Windows to allow for blank passwords. For more information, see your Windows documentation.

- 19** On the **Choose SQL Server** panel, do one of the following to select a location to store the Backup Exec Database.

---

**Note:** The **Choose SQL Server** panel does not appear for upgrades. You cannot change the database location during the upgrade process. If you want to change the database location after the upgrade, use BE Utility.

---

To create a local Backup Exec SQL Express instance

Do the following in the order listed:

- Click **Create a local Backup Exec SQL Express instance to store the database on**.
- To change the location of the Backup Exec SQL Express instance, click **Browse**.
- Select the location, and then click **OK**.

To use an existing SQL Server 2005 or SQL Server 2008 instance

Do the following in the order listed:

- Click **Use an existing instance of SQL Server 2005 (SP4a or later) or SQL Server 2008 on the network to store the database on.**
- Select the instance.

When Backup Exec is installed into an existing instance, the automated Master database restore feature is not available. To recover the Master database, replace it with the Master database copy that Backup Exec automatically creates and updates when the Master database is backed up.

**20** Click **Next**.

Backup Exec attempts to connect to the instance.

**21** If the Symantec Backup Exec Database panel appears, perform the following steps to identify the location of the SQL Express SP4 setup file:

- Click **Browse**.
- Navigate to the location where you downloaded the SQL Express SP4 setup file.
- Click **OK**.
- Click **Next**.

**22** If you are prompted, select how the **Symantec Device Driver Installer** should install device drivers for the tape storage devices that are connected to the server, and then click **Next**.

Symantec recommends that you select **Use Symantec device drivers for all tape devices**.

**23** If you are prompted, enter information or choose settings for the additional options that you want to install, and then click **Next** after each selection.

**24** Read the Backup Exec installation summary, and then click **Install**.

The installation process takes several minutes to complete. During the process, the progress bar may not move for several minutes.

**25** When the installation is complete, you can run LiveUpdate, view the readme, and create a shortcut to Backup Exec on the desktop.

**26** Click **Finish** to close the installation wizard.

**27** If Restart System appears, restart the computer in order for the configuration to take effect.

The installation process creates an installation log named Bkupinst2012.htm in one of the following directories on the computer where Backup Exec is installed.

- For Windows 2003: %allusersprofile%\Application Data\Symantec\Backup Exec\Logs
- For Windows 2008 and later: %programdata%\Symantec\Backup Exec\Logs

See [“About the installation log”](#) on page 114.

See [“Post-installation tasks”](#) on page 127.

See [“About Backup Exec’s standard features”](#) on page 64.

See [“About upgrading from previous versions of Backup Exec”](#) on page 124.

## Installing additional Backup Exec options to the local Backup Exec server

You can install agents and options when you install Backup Exec. However, if you have already installed Backup Exec and want to install additional options, review the documentation for those options to ensure that your system meets all minimum requirements. The Backup Exec services may be stopped while the additional options are installed. If any active jobs are running, you are prompted to stop them, or to wait for the jobs to finish.

---

**Note:** If you install Backup Exec through Terminal Services and the installation media is on a shared drive (network share) you must install using a UNC path. Installation by mapped drives is not supported.

---

If you have a licensed version of Backup Exec, you can use a trial version of most options and agents for a specified period of time.

See [“Installing a trial version of Backup Exec agents and options”](#) on page 114.

---

**Note:** If the Central Admin Server Option is installed, and you want to install additional options on a managed Backup Exec server, you can pause the managed Backup Exec server. When a managed Backup Exec server is paused, the administration server does not delegate jobs to it. When the installation is complete, un-pause, or resume, the managed Backup Exec server.

---

See [“Pausing a managed Backup Exec server”](#) on page 1037.

### To install additional Backup Exec options to the local Backup Exec server

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Options and Licenses on this Backup Exec Server**.

- 2 Do one of the following:

To enter serial numbers manually

An Internet connection is required to validate the serial numbers. If you do not have an Internet connection, import the licenses from the Symantec License File or install a trial version.

Do the following in the order listed:

- Type the serial number in the **Serial Number** field.
- Click **Add**.
- Repeat for any additional serial numbers that you want to enter.
- Click **Next** to validate the serial numbers.

To import licenses from the Symantec license file

Do the following in the order listed:

- Click **Import From File**.
- Browse to the location of your license files, and then select the appropriate file.

To install a trial version

Click **Next**. Do not type or import serial numbers.

- 3 Select the additional options that you want to install, and then click **Next**.
- 4 If you are prompted, enter information or choose settings for the additional options that you want to install. Click **Next** after each selection.
- 5 Read the Backup Exec installation summary, and then click **Install**.

The Backup Exec services are stopped while the additional options are installed. If any active jobs are running, you are prompted to stop them, or to wait for the jobs to finish.

When the installation is complete, the services are restarted.

- 6 Click **Finish**.

## Special considerations for installing Backup Exec to remote computers

There are special considerations that you should be familiar with before you install Backup Exec to remote computers.

**Table 2-5** Special considerations for installing Backup Exec to remote computers

Item	Consideration
Windows Server 2003 SP1	<p>To push-install Backup Exec to a Windows Server 2003 computer, you must enable File and Printer Sharing on the Windows Firewall Exceptions list for the following ports:</p> <ul style="list-style-type: none"> <li>■ 135 (RPC)</li> <li>■ 445 (TCP)</li> <li>■ 103X (mostly 1037)</li> <li>■ 441 (RPC)</li> </ul> <p>For more information about the Windows Firewall Exceptions list, refer to your Microsoft Windows documentation.</p> <p>During the installation process, Backup Exec sets the Remote Launch and remote access security permissions for the Administrator's group.</p> <p>You should enable the "Allow remote administration exception" group policy for the computer to which you push the installation.</p>
Windows Server 2008	<p>To push-install Backup Exec to a computer that runs Windows Server 2008, you must enable the following items on the destination computer's Windows Firewall Exceptions list:</p> <ul style="list-style-type: none"> <li>■ File and Printer Sharing</li> <li>■ Windows Management Instrumentation (WMI)</li> </ul> <p>For more information refer to your Microsoft Windows documentation.</p>
Symantec Endpoint Protection (SEP) 11.0 or later	<p>To push-install Backup Exec to a computer that runs Symantec Endpoint Protection (SEP) version 11.0 or later, you must configure SEP to share files and printers. The file and printer sharing feature is turned off by default.</p>

See ["Push-installing Backup Exec to remote computers"](#) on page 77.

## Push-installing Backup Exec to remote computers

If you install Backup Exec through Terminal Services and the installation media is on a shared drive (network share) you must use a UNC path. Installation by mapped drives is not supported.

You can set up multiple server installations. Backup Exec processes up to five remote computer installations concurrently.

Before, you install Backup Exec to remote computers, you should review the special considerations.

See “[Special considerations for installing Backup Exec to remote computers](#)” on page 76.

---

**Note:** You can also use Microsoft’s Add or Remove Programs utility to install Backup Exec to a remote computer. See your Microsoft documentation for more information.

---

The installation process creates an installation log named Bkupinst2012.htm on the computer where Backup Exec is installed.

### To push-install Backup Exec to remote computers

#### 1 Do one of the following:

To push-install Backup Exec to remote computers from the installation media

Do the following steps in the order listed:

- From the installation media browser, click **Installation**, and then click **Backup Exec**.
- On the **Welcome** panel, click **Next**.
- Select **I accept the terms of the license agreement**, and then click **Next**.
- Select **Custom installation**.
- Uncheck **Local Installation**, and then check **Remote Installation**.
- Click **Next**.

To push-install Backup Exec to remote computers from the Backup Exec server

Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Agents and Backup Exec Servers on Other Servers**.

- 2 On the **Remote Computers** panel, click **Add**.
- 3 To install Backup Exec on one remote computer, select **Add a Single Computer**, or to install Backup Exec on multiple computers using the same settings, select **Add Multiple Computers with the Same Settings**.
- 4 Select **Symantec Backup Exec**, and then click **Next**.
- 5 Type the fully qualified name, IP address, or computer name of the remote computer or click **Browse Remote Computers** to locate the remote computer.

- 6** Click **Add to List**, and then repeat steps 3 and 4 for each remote computer to which you want to push-install the programs.

If you are push-installing from the installation media and you selected **Add a Single Computer** in step 3, you can skip this step.

- 7** Under **Remote computer credentials**, type the credentials that Backup Exec can use to connect to the remote servers.

You must use Administrator credentials. These remote computer logon credentials are not the same as the Backup Exec service account credentials in step 15.

- 8** Click **Next**.

- 9** Select one of the following methods to enter licenses:

To enter serial numbers from your license certificate

**Note:** An Internet connection is required to validate the serial numbers. If you do not have an Internet connection, import the licenses from the Symantec License File or install a trial version.

Do the following in the order listed:

- Type a serial number into the **Serial number** field.
- Click **Add**.
- Repeat for each serial number for each option or agent that you want to install.
- Click **Next** to verify the serial numbers that you entered.

To import licenses from a Symantec License File

Do the following in the order listed:

- Click **Import From File**.
- Locate and select the .slf file.

To install a trial version

Leave the **Serial number** field blank.

- 10** Click **Next**.

You may be prompted to enter contact information.

- 11** Check the check boxes for the agents or options that you want to install, and then click **Next**.

- 12 Select any additional items that you want to install, such as Backup Exec standards features or agents and options that are available for a trial installation.
- 13 In the **Destination Folder** field, enter the location where you want to install Backup Exec.
- 14 Click **Next**.
- 15 Complete the service account credentials options as follows:

**User Name**      Type the user name for an Administrator account that the Backup Exec services can use.

If the remote computer is in a domain, use a domain administrators account or an equivalent account that is part of the domain administrators group.

If the remote computer is in a workgroup, use an Administrators account or an equivalent account that is part of the Administrators group on the computer.

**Password**      Type the password for an Administrator account that the Backup Exec services can use.

**Domain**          If the computer is in a domain, select the domain in which the computer is located.

If the computer is in a workgroup, select the computer name.

- 16 Click **Next**.
- 17 Do one of the following to select a location on which to store the Backup Exec Database , and then click **Next**.

To create a local Backup Exec SQL Express instance

Do the following in the order listed:

- Click **Create a local Backup Exec SQL Express instance to store the database on**.
- To change the location of the database, type the new location in the **Destination Folder** field.

To use an existing SQL Server 2005 or SQL Server 2008 instance

Do the following in the order listed:

- Click **Use an existing instance of SQL Server 2005 (SP4 or later) or SQL Server 2008 on the network to store the database on.**
- Select the instance.

When Backup Exec is installed into an existing instance, the automated master database restore feature is not available. To recover the Master database, you must replace it with the Master database copy that Backup Exec automatically creates and updates when the Master database is backed up.

**Caution:** During the installation process and upgrade process, Backup Exec stops and starts the SQL service several times. Other user-created databases that use the SQL Server instance are unavailable during the process. To avoid such conflicts, you should install Backup Exec into its own SQL instance.

Backup Exec attempts to connect to the instance.

This step is skipped during upgrades.

- 18 Click **Next**.
- 19 Make a selection for tape device drivers, and then click **Next**.
- 20 Click **Next**.
- 21 If you are prompted, enter information or choose settings for additional options being installed, and then click **Next** or **OK** after each selection.
- 22 After Backup Exec validates the remote computers, you can change the list in any of the following ways:

To manually add one remote computer      Click **Add**, and then click **Add a Single Computer**.

To manually add multiple remote computers      Click **Add**, and then click **Add Multiple Computers with the Same Settings**.

To add multiple remote computers by importing an existing list of computers	Click <b>Import and Export</b> , and then select one of the following options:
	<ul style="list-style-type: none"> <li>■ Select <b>Import from File</b> to enable Backup Exec to add the names of the remote computers from a selected list.</li> <li>■ Select <b>Import Servers Published to this Backup Exec server</b> to enable Backup Exec to add the names of all the remote computers that are set up to publish to this Backup Exec server.</li> </ul>
	You must enter remote computer logon credentials for the list of remote computers.
To change the product that you selected to install or to change other properties you selected for this installation	Select the remote computer that you want to change, and then click <b>Edit</b> .
To delete a remote computer from the list	Select the remote computer that you want to delete, and then click <b>Delete</b> .
To save this list of remote computers and the associated remote computer logon credentials	Verify that <b>Save the server list for future remote install sessions</b> is checked.
	This option enables the names and the credentials of all of the remote computers to be added automatically the next time you install Backup Exec or options to these remote computers.
To save the list of remote computers to an XML file	Click <b>Import and Export</b> , and then click <b>Export to File</b> .
	You can select the location to save the Push_Export.xml file. This option is useful if you want to use the same list for multiple Backup Exec servers. When you import the list, you must re-enter the remote computer logon credentials.
To fix the errors that were located during the validation	Right-click the name of the computer, and then click <b>Fix Error</b> .
To enable Backup Exec to attempt to re-validate an invalid remote computer	Right-click the name of the computer, and then click <b>Retry Validation</b> .

**23** After all of the computers in the list are validated and the list is complete, click **Next**.

24 Read the Backup Exec installation review, and then click **Install**.

See [“About the installation log”](#) on page 114.

25 Click **Next**, and then click **Finish** to exit the wizard.

If you did not restart the remote computer, you may need to do it now in order for the configuration to take effect.

## About installing the Agent for Windows

You can install the Agent for Windows by using the following methods, depending on your environment:

- Push-install the Agent for Windows to one or more remote computers from the Backup Exec server.  
See [“Push-installing the Agent for Windows to remote computers”](#) on page 86.
- Use the Add Servers option to add a remote computer to the list of servers and install the Agent for Windows on that remote computer.  
See [“Adding servers to the list of servers”](#) on page 158.
- Use a Microsoft Active Directory network to centrally manage the installation of the Agent for Windows to computers in the network.  
See [“How to install the Agent for Windows in an Active Directory network”](#) on page 90.
- Install the Agent for Windows by using command script files.  
See [“Using a command script to install the Agent for Windows”](#) on page 98.

There are special considerations for installing the Agent for Windows.

See [“About push-installing the Agent for Windows to remote computers”](#) on page 83.

## About push-installing the Agent for Windows to remote computers

The Agent for Windows can be push-installed to remote computers from a Backup Exec server. Push installations save time by eliminating the need for local access at the target computer for the installation to be successful. You can push-install the Agent for Windows to as many as five remote computers concurrently.

There are special considerations that you should be familiar with before you install the Agent for Windows on remote computers.

**Table 2-6** Special considerations for push-installing the Agent for Windows to remote computers

Item	Consideration
32-bit and 64-bit computers	If you try to push-install an option from a 32-bit computer to a 64-bit computer, you may be prompted to insert the 64-bit installation media.
Agent for Windows	<p>You cannot push-install the Agent for Windows when the remote computer is in the ForceGuest configuration and it is not in a domain. ForceGuest is an operating system configuration that limits incoming users to Guest-level access. Instead, use the installation media or the network to install the Agent for Windows on the Windows computer. You can also turn off ForceGuest. Refer to your Microsoft Windows documentation for more information.</p> <p>See <a href="#">“Installing Backup Exec using the command line (silent mode)”</a> on page 104.</p> <p>Backup Exec installs a command-line version of the Agent for Windows on the computers that run the Server Core installation option of Windows Server 2008. The Backup Exec Agent Utility command-line applet is installed with the Agent for Windows. This applet lets you monitor Backup Exec operations on the remote computer.</p> <p>See <a href="#">“Backup Exec Agent Utility Command Line Applet switches”</a> on page 747.</p>
Terminal Services	If you install Backup Exec agents and options through Terminal Services and the installation media is on a shared drive (network share) you must install using a UNC path. Installation by mapped drives is not supported.

**Table 2-6** Special considerations for push-installing the Agent for Windows to remote computers *(continued)*

Item	Consideration
Windows Server 2003 SP1	<p>To push-install Backup Exec options to a Windows Server 2003 SP1 computer, you must enable File and Printer Sharing on the Windows Firewall Exceptions list for the following ports:</p> <ul style="list-style-type: none"> <li>■ 135 (RPC)</li> <li>■ 445 (TCP)</li> <li>■ 103X (mostly 1037)</li> <li>■ 441 (RPC)</li> </ul> <p>For more information about the Windows Firewall Exceptions list, refer to your Microsoft Windows documentation.</p> <p>During the installation process, Backup Exec sets the Remote Launch and remote access security permissions for the Administrator's group.</p> <p>You should enable the "Allow remote administration exception" group policy for the computer to which you push the installation.</p>
Windows Vista/Server 2008/ 7	<p>To push-install Backup Exec options to a computer that runs Windows Vista/Server 2008/ 7, you must enable certain items on the destination computer's Windows Firewall Exceptions list. You must enable the following items:</p> <ul style="list-style-type: none"> <li>■ File and Printer Sharing</li> <li>■ Windows Management Instrumentation (WMI)</li> </ul> <p>For more information refer to your Microsoft Windows documentation.</p> <p>To push-install to a Windows Vista computer, the destination computer must be part of a domain.</p> <p>For more information, refer to the Microsoft Knowledge Base.</p>
Symantec Endpoint Protection 11.0 or later	<p>To push-install options to a computer that runs Symantec Endpoint Protection (SEP) version 11.0 or later, you must configure SEP to share files and printers. File and printer sharing is turned off by default.</p>

## Push-installing the Agent for Windows to remote computers

Before you push-install the Agent for Windows to remote computers, review the special considerations.

See [“About push-installing the Agent for Windows to remote computers”](#) on page 83.

The installation process creates an installation log named Bkupinst2012.htm on the computer where Backup Exec is installed, and also creates an installation log named RAWSin2012.htm on the remote computer.

See [“About the installation log”](#) on page 114.

If there are problems installing the Agent for Windows using this method, you can try to manually install the Agent for Windows.

See [“Using a command prompt to install the Agent for Windows on a remote computer”](#) on page 94.

### To push-install the Agent for Windows to remote computers

#### 1 Do one of the following:

To push-install the Agent for Windows to remote computers from the installation media

Do the following steps in the order listed:

- From the installation media browser, click **Installation**, and then click **Backup Exec**.
- On the **Welcome** panel, select **I accept the terms of the license agreement**, and then click **Next**.
- Click **Custom installation**.
- Uncheck **Local Installation**, and then check **Remote Installation**.
- Click **Next**.

To push-install the Agent for Windows to remote computers from the Backup Exec server

Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Agents and Backup Exec Servers on Other Servers**.

#### 2 On the **Remote Computers** panel, click **Add**.

3 To install the Agent for Windows on one remote computer, select **Add a Single Computer**, or to install Backup Exec on multiple computers using the same settings, select **Add Multiple Computers with the Same Settings**.

4 Select **Agent for Windows**, and then click **Next**.

- 5 Type the fully qualified name of the remote computer or click **Browse Remote Computers** to locate the remote computer.
- 6 Click **Add to List**, and then repeat steps 3 and 4 for each remote computer to which you want to push-install the options.

If you are push-installing from the installation media and you selected **Add a Single Computer** in step 3, you can skip this step.

- 7 Under **Remote computer credentials**, type the credentials that Backup Exec can use to connect to the remote servers.

You must use Administrator credentials.

- 8 Click **Next**.

- 9 In the **Destination Folder** field, enter the path where you want to install the files.

- 10 Click **Next**.

- 11 Verify that the option **Enable the Agent for Windows to publish the IP address and name of the remote computer and the version of the Agent for Windows to Backup Exec servers** is selected. Then, add or remove the names or IP addresses of the Backup Exec servers to which the Agent for Windows should publish.

- 12 Click **Next**.

- 13 After Backup Exec validates the remote computers, you can change the list in any of the following ways:

To manually add one remote computer	Click <b>Add</b> , and then click <b>Add a Single Computer</b> .
-------------------------------------	--

To manually add multiple remote computers	Click <b>Add</b> , and then click <b>Add Multiple Computers with the Same Settings</b> .
---	--

To add multiple remote computers by importing an existing list of computers

Click **Import and Export**, and then select one of the following options:

- Select **Import from File** to enable Backup Exec to add the names of the remote computers from a selected list.
- Select **Import Servers Published to this Backup Exec server** to enable Backup Exec to add the names of all the remote computers that are set up to publish to this Backup Exec server.

You must enter remote computer logon credentials for the list of remote computers.

To change the product that you selected to install or to change other properties you selected for this installation

Select the remote computer that you want to change, and then click **Edit**.

To delete a remote computer from the list

Select the remote computer that you want to delete, and then click **Delete**.

To save this list of remote computers and the associated remote computer logon credentials

Verify that **Save the server list for future remote install sessions** is checked.

This option enables the names of all of the remote computers and their credentials to be added automatically the next time you want to install Backup Exec or options to these remote computers.

To save the list of remote computers to an XML file

Click **Import and Export**, and then click **Export to File**.

You can select the location to save the XML file. This option is useful if you want to use the same list for multiple Backup Exec servers. When you import the list, you must re-enter the remote computer logon credentials.

To fix the errors that were located during the validation

Right-click the name of the computer, and then click **Fix Errors**.

To enable Backup Exec to attempt to re-validate an invalid remote computer

Right-click the name of the computer, and then click **Retry Validation**.

**14** After all of the computers in the list are validated and the list is complete, click **Next**.

15 Read the Backup Exec installation review, and then click **Install**.

See [“About the installation log”](#) on page 114.

16 Click **Next**, and then click **Finish** to exit the wizard.

If you did not restart the remote computer, you may need to do it now in order for the configuration to take effect.

## Installing updates to the Agent for Windows on remote computers

When a Backup Exec server is updated with patches, an alert is generated to warn you that the Agent for Windows on remote computers must be updated with the same patches. Additionally, in the properties for the remote computer, the property **Do the updates installed on this server match the updates installed on the backup server** indicates whether the remote computer is up to date with the Backup Exec server. From the Backup Exec console, you can update the remote computers immediately, at a scheduled time, or on a recurring schedule. You can also update a group of remote computers together.

See [“About updating Backup Exec with LiveUpdate”](#) on page 116.

### To install updates for the Agent for Windows

- 1 On the **Backup and Restore** tab, right-click the remote computer or the group that needs to be updated.
- 2 Select **Update**.
- 3 On the **Install Updates** dialog box, select the option for when you want to install the updates.

See [“Install updates options”](#) on page 89.

- 4 Click **OK**.

### Install updates options

The following options let you schedule when you want to install updates to the Agent for Windows on remote computers.

See [“Installing updates to the Agent for Windows on remote computers”](#) on page 89.

**Table 2-7** Install updates options

Item	Description
<b>Recurrence</b>	Lets you create a recurring schedule for the job.

**Table 2-7** Install updates options (*continued*)

Item	Description
<b>Recurrence Pattern</b>	Lets you configure the frequency with which the job recurs, if you choose to make the job recur on a schedule. You can select to run the job in hourly, daily, weekly, monthly, or yearly increments.
<b>Starting on</b>	Designates the date on which the schedule takes effect.
<b>Calendar</b>	Lets you view all scheduled jobs on a calendar to check for scheduling conflicts.
<b>Keep the job scheduled for x hours before it is rescheduled</b>	Specifies the maximum amount of time after the scheduled start time at which Backup Exec considers the job to be missed and reschedules it.
<b>Cancel the job if it is still running x hours after its scheduled start time</b>	Specifies the amount of time after the job's scheduled start time at which you want to cancel the job if it is still running.
<b>Run now with no recurring schedule</b>	Runs the job immediately without scheduling any more instances of it for the future.
<b>Run on</b>	Lets you select a specific date on which to run the job without scheduling any more instances of it for the future.
<b>Restart the computer automatically after installing the updates to the Symantec Backup Exec Agent for Windows when a restart is required</b>	Enables Backup Exec to automatically restart the remote computer if required.

## How to install the Agent for Windows in an Active Directory network

You can centrally manage the installation of the Backup Exec Agent for Windows to computers in an Active Directory network. You configure the installation once, and then use a Group Policy Object to assign that installation to computers in an Organizational Unit. The options are installed automatically whenever a computer in the Organizational Unit is started.

**Note:** Review your organization’s deployment plans before you implement a rollout of the Backup Exec Agent for Windows to client computers. You should also review your Group Policy Desktop Management and Active Directory documentation.

**Table 2-8** Installing the Agent for Windows in an Active Directory network

Action	Description
<p>Create a transform for the Agent for Windows.</p> <p>See <a href="#">“Creating a transform”</a> on page 92.</p>	<p>A transform contains changes that you want to make to the Agent for Windows Installer package when a computer starts, such as installation path, and which computers to publish to. You must create separate transforms for 32-bit computers and 64-bit computers.</p> <p>Requirements to create a transform are as follows:</p> <ul style="list-style-type: none"> <li>■ The computer on which you want to create the transform must have Microsoft Windows 2003 or later.</li> <li>■ The computers on which you want to install the Agent for Windows must be running MSI 3.1.</li> <li>■ The computers on which you want to install the Agent for Windows must be running MSXML 6.0.</li> <li>■ Only assignment to computers is supported. Assignment to users is not supported.</li> </ul>
<p>Create a distribution point (share) that contains the source file of the Agent for Windows that you want to install.</p> <p>See <a href="#">“Creating a software distribution point (share)”</a> on page 93.</p>	<p>You must copy the transform that you create, and the Backup Exec RAWS32 or RAWSX64 directory, to the distribution point.</p>
<p>Configure a Group Policy Object to assign the transform and the RAWS32 or RAWSX64 directory in the distribution point to computers in an Active Directory Organizational Unit.</p> <p>See <a href="#">“Configuring a Group Policy Object”</a> on page 93.</p>	<p>The software is installed automatically when the computers in the Organizational Unit are started.</p>

## Creating a transform

To install the Agent for Windows in an Active Directory network, you must create a transform.

See [“How to install the Agent for Windows in an Active Directory network”](#) on page 90.

### To create the transform

- 1 Do one of the following:
  - From the Backup Exec installation media browser, click **Installation**, and then click **Agent for Windows**.
  - From a Backup Exec server on which Backup Exec is installed, go to `\Program Files\Symantec\Backup Exec\Agents\RAWS32` or `RAWS64` and double-click **Setup.exe**.
- 2 On the **Welcome** panel, click **Next**.
- 3 On the **Install Type** panel, click **Create a Transform to use Active Directory to install the Agent for Windows**, and then click **Next**.
- 4 On the **Install Option** panel, in the **Destination Folder** area, enter the path where you want to install the files.
- 5 Click **Next**.
- 6 Verify that the option **Enable the Agent for Windows to publish the IP address and name of the remote computers and the version of the Agent for Windows to Backup Exec servers** is selected. Then, add or remove the names or IP addresses of the Backup Exec servers to which the Agent for Windows should publish.
- 7 Click **Next**.
- 8 Enter a file name and a path where the transform will be created, and then click **Next**.

Use a meaningful file name for the transform. For example, the name can include the names of the options in the transform and the platform you plan to apply the transform to, such as `AgentDefaultPathNoPublishing`.
- 9 To create the transform, click **Install**.
- 10 After the transform is created, set up a distribution point for the source files. See [“Creating a software distribution point \(share\)”](#) on page 93.

## Creating a software distribution point (share)

To install the Agent for Windows in an Active Directory network, you must create a software distribution point after you create a transform.

See [“Creating a transform”](#) on page 92.

See [“How to install the Agent for Windows in an Active Directory network”](#) on page 90.

**Table 2-9** How to create a software distribution point (share)

Step	Description
Step 1	Create a shared folder, and then set permissions so that the client computers that will run the installation have access to the shared folder.
Step 2	Copy the following directories from the Backup Exec server to the shared folder: <ul style="list-style-type: none"> <li>■ RAWS32 or RAWSX64</li> <li>■ MSXML</li> </ul> <p>By default, these folders are located in \Program Files\Symantec\Backup Exec\Agents.</p>
Step 3	Copy the transform from the path where it was created to the RAWS32 or RAWSX64 directory on the shared folder.
Step 4	Configure a Group Policy Object to deploy the source files.  See <a href="#">“Configuring a Group Policy Object”</a> on page 93.

## Configuring a Group Policy Object

To install the Agent for Windows in an Active Directory network, you must configure a Group Policy Object after you create a software distribution point and create a transform.

See [“Creating a transform”](#) on page 92.

See [“Creating a software distribution point \(share\)”](#) on page 93.

See [“How to install the Agent for Windows in an Active Directory network”](#) on page 90.

### To configure a Group Policy Object to deploy the software

- 1 From the Active Directory snap-in that manages users and groups, click **Properties**, and create a new Group Policy Object or edit an existing one.  
Refer to your Microsoft Windows documentation for information on creating a Group Policy Object.
- 2 Under **Computer Configuration**, expand **Software Settings**.
- 3 Right-click **Software Installation**, click **New**, and then click **Package**.
- 4 On the **File Open** dialog box, browse to the software distribution point by using the Universal Naming Convention (UNC) name, for example, \\server name\share name, select the package file, and then click **Open**.
- 5 Select the package file **Symantec Backup Exec Agent for Windows.msi**, and then click **Open**.
- 6 When you are prompted, apply the **Advanced Option**.
- 7 After Active Directory checks the MSI package, on the **General Properties** tab, make sure that the correct versions of the options are being installed.
- 8 On the **Deployment** tab, set up the configuration for your environment.  
Make sure the option **Make this 32-bit x86 application available to WIN64 machines** is not selected.  
If you want the Agent for Windows to be uninstalled if the computer is removed from the Organization Unit, select the option **Uninstall this application when it falls out of the scope of management**.
- 9 On the **Modifications** tab, click **Add**, browse to the share, and select the transform that you created.
- 10 Select **Open**, and make any other changes that are necessary, and then click **OK**.
- 11 Close all of the dialog boxes.  
When a computer in the Organizational Unit that you specified is started, the transform is processed and the options that you specified are installed.
- 12 View the installation log that is created on the destination computers to verify the installation of the Agent for Windows.

## Using a command prompt to install the Agent for Windows on a remote computer

You can install the Agent for Windows by using a command prompt.

The installation process creates an installation log named RAWSinstant2012.htm.

See [“About the installation log”](#) on page 114.

**To use a command prompt to install the Agent for Windows on a remote computer**

- 1** At a remote computer, map a drive letter to the Agents directory. By default, the Agents directory is located at the following path:

`\Program Files\Symantec\Backup Exec\Agents`

or you can copy the following folders to the same local directory:

To install to a 32-bit computer:                      RAWS32 and MSXML folders

To install to a 64-bit computer:                      RAWSX64 and MSXML folders

- 2** Open a command prompt and type the drive letter that you mapped in step 1 and the following path:

To install to a 32-bit computer:                      `\RAWS32 :`

To install to a 64-bit computer:                      `\RAWSX64 :`

### 3 Do one of the following:

To install the Agent for Windows to a 32-bit computer without publishing enabled:

Run the following command:

```
setup.exe /RANT32: /S: -boot
```

To install the Agent for Windows to a 32-bit computer with publishing enabled:

Run the following command:

```
setup.exe /RANT32: /S: /ADVRT:  
<Backup Exec server name 1>  
<Backup Exec server name 2>
```

To install the Agent for Windows to a 64-bit computer without publishing enabled:

Run the following command:

```
setup.exe /RAWSX64: /S: -boot
```

To install the Agent for Windows to a 64-bit computer with publishing enabled:

Run the following command:

```
setup.exe /RAWSX64: /S: /ADVRT:  
<Backup Exec server name 1>  
<Backup Exec server name 2>
```

The Agent for Windows is installed on the remote computer in the following directory:

If you installed the Agent for Windows to a 32-bit computer: `\Program Files\Symantec\Backup Exec\RAWS32`

If you installed the Agent for Windows to a 64-bit computer: `\Program Files\Symantec\Backup Exec\RAWSx64`

## Using a command prompt to uninstall the Agent for Windows from a remote computer

You can uninstall the Agent for Windows by using a command prompt.

### To use a command prompt to uninstall the Agent for Windows from a remote computer

- 1 At the remote computer, map a drive letter to the Agent for Windows directory using the following path:

To uninstall the Agent for Windows from a 32-bit computer: `\Program Files\Symantec\Backup Exec\Agents\RAWS32`

To uninstall the Agent for Windows from a 64-bit computer: `\Program Files\Symantec\Backup Exec\Agents\RAWSX64`

- 2 Open a command prompt, and then type the drive letter that you mapped in step 1.
- 3 Run the following command:

To uninstall the Agent for Windows from a 32-bit computer: `setup.exe /RANT32: /S: -u`

The `/S:` parameter is used to run the operation in silent mode, without the benefit of a user interface. The `-u` parameter specifies an uninstall operation.

To uninstall the Agent for Windows from a 64-bit computer: `setup.exe /RAWSX64: /S: -u`

See [“Using a command prompt to install the Agent for Windows on a remote computer”](#) on page 94.

## Using a command script to install the Agent for Windows

You can use command script files to install the Agent for Windows. The command script files are included in the Backup Exec installation directory.

The installation process creates an installation log named `RAWSinst2012.htm`.

See [“About the installation log”](#) on page 114.

**To use a command script to install the Agent for Windows**

- 1 Map a drive letter to the Agents directory on a Backup Exec server. By default, the Agents directory is located at the following path:

\Program Files\Symantec\Backup Exec\Agents

- 2 Do one of the following:

To install the Agent for Windows on a 32-bit computer Double-click **setupaa** in the RAWS32 directory.

To install the Agent for Windows on a 64-bit computer Double-click **setupaax64** in the RAW64 directory.

**Using a command script to uninstall the Agent for Windows**

A command script file is available to uninstall the Agent for Windows.

**To use a command script to uninstall the Agent for Windows**

- 1 Map a drive letter to the Backup Exec server by using one of the following paths:

To a 32-bit computer            \Program Files\Symantec\Backup Exec\Agents\RAWS32

To a 64-bit computer            \Program Files\Symantec\Backup Exec\Agents\RAW64

- 2 Do one of the following:

For a 32-bit computer            Double-click **Removeaafo**.

For a 64-bit computer            Double-click **Uninstallaaofo64**.

- 3 Restart the remote computer.

See [“Using a command script to install the Agent for Windows”](#) on page 98.

# Installing the Remote Administrator

The Remote Administrator lets you administer the Backup Exec server from a remote Windows server or workstation. To support the Remote Administrator, the Backup Exec system services must be running on the Backup Exec server that you want to administer.

**To install the Remote Administrator**

- 1 From the installation media browser, click **Installation**.
- 2 Click **Backup Exec**.
- 3 On the **Welcome** panel, select **I accept the terms of the license agreement**, and then click **Next**.
- 4 On the **Installation Type** panel, select **Custom installation**, and then click **Next**.
- 5 Check **Local Installation**, and then click **Install Remote Administration Console only**.
- 6 Click **Next**.
- 7 On the **Destination** panel, do the following:
  - Review the disk space requirements for the installation.
  - To change the location where the files are installed, click **Change** to select another directory for the installation.
- 8 Click **Next**.
- 9 Review the installation summary, and then click **Install**.
- 10 Click **Finish**.

See [“Running the Remote Administrator”](#) on page 102.

## Installing the Remote Administrator using the command line

You can also use silent mode installation to install the Remote Administrator. Options for the Remote Administrator are specified with the use of additional command switches.

**To install the Remote Administrator using the command line**

- 1 Open a Windows command prompt.
- 2 Change to the drive containing the Backup Exec installation media.
- 3 Change directories to one of the following:

For 32-bit computers `\be\winnt\install\be32`

For 64-bit computers `\be\winnt\install\bex64`

- 4 Type `setup /RA:` and the appropriate switches. For example:

```
setup /RA: /S:
```

The command line switches used for silent mode installation of the Remote Administrator are described in the following table.

Remember the following general rules for using these switches:

- Substitute values appropriate for your environment for values in italics; for example, substitute your password for *password*.
- Enclose the value in quotation marks if it contains spaces, such as "Program Files\Symantec\Backup Exec".

**Table 2-10** Command line switches for Remote Administrator silent mode installation

Switch	Additional Switches	Description
/RA:		Installs Remote Administrator using the options that are specified with the additional switches.
	/DEST:" <i>path</i> "	Specifies the path where Remote Administrator will be installed. Otherwise, the default path Program Files\Symantec\Backup Exec is used.
	/DOCS:	Installs the online documentation.
	/NOINSTALL:	Lets you select all install options without actually installing the Backup Exec software. This option can be used with the /CPF: switch.

**Table 2-10** Command line switches for Remote Administrator silent mode installation (*continued*)

Switch	Additional Switches	Description
	<code>/CPF:"path\filename.cpf"</code>	Creates a file containing all of the installation parameters provided. Note that the file is not encrypted, which exposes parameters such as the password
-?		Provides help on all command line operations, usage, and special switches.

See [“Installing Backup Exec using the command line \(silent mode\)”](#) on page 104.

## Running the Remote Administrator

The Remote Administrator lets you administer the Backup Exec server from a remote Windows server or workstation. To support the Remote Administrator, the Backup Exec server requires that the Backup Exec system services must be running.

You may be prompted for a user name and password to browse some network shares even if you are logged into the Remote Administrator computer under an account that is valid for those shares. Provide a domain-qualified user name and password when prompted (for example, domain1\howard).

For workgroup accounts, when logging in between different workgroups, you can provide only a user ID when prompted, and leave the workgroup line blank.

See [“Installing the Remote Administrator ”](#) on page 99.

### To run the Remote Administrator

- 1 Click **Start**.
- 2 Point to Programs, and then click **Symantec Backup Exec**.

If you are connecting to a Remote Administration Console from a Backup Exec server, click the Backup Exec button, and then select **Connect to Backup Exec Server**.

- 3 Select the appropriate options.

See [“Connect to Backup Exec Server options”](#) on page 103.

The status of the local services appears at the bottom of this dialog box. If you try to connect to a server and the connection fails, this dialog box displays the services status for the server you attempted to connect to.

- 4 Click **OK**.

### Connect to Backup Exec Server options

On this dialog box, you can enter the credentials that are required to administer a Backup Exec server from a remote Windows server or workstation.

See [“Running the Remote Administrator ”](#) on page 102.

**Table 2-11**      **Connect to Backup Exec Server options**

Item	Description
<b>Manage services</b>	Lets you access the Backup Exec Services Manager to stop and start services or to set the logon credentials that are used to run the services.
<b>Server name</b>	Indicates the name of the Backup Exec server. You can select the name from the list or type the name of the server if you are running the Remote Administrator from a Backup Exec server.  Each server in the domain that has Backup Exec installed automatically appears in the list box.
<b>User name</b>	Indicates an administrator user name for the server to which you want to connect.  You cannot log on to the Remote Administration Console with a user name that has a blank password on Windows Server 2003/2008 and Vista computers. You must configure Windows to allow blank passwords. Otherwise, the error message "Logon failure: user account restriction" appears. For more information, see your Windows documentation.
<b>Password</b>	Indicates the password for the user.

Table 2-11 Connect to Backup Exec Server options (*continued*)

Item	Description
Domain	Indicates the domain to which the user belongs. You can select the domain from the list or type the domain name.

## Installing Backup Exec using the command line (silent mode)

Installing Backup Exec using the command line is referred to as silent mode installation. This method of installation uses the setup.exe program on the Backup Exec installation media, a series of command switches, and the /S: switch.

Requirements for Command Line Installation include the following:

- Backup Exec installation media.
- Administrator privileges on the computer where you want to install, configure, or uninstall Backup Exec.

The installation process creates an installation log named Bkupinst2012.htm on the computer where Backup Exec is installed.

See [“About the installation log”](#) on page 114.

### To install Backup Exec using the command line (silent mode)

- 1 Open a Windows command prompt.
- 2 Change to the drive containing the Backup Exec installation media.
- 3 Change directories to one of the following:

For 32-bit computers `be\winnt\install\be32`

For 64-bit computers `\be\winnt\install\bex64`

4 Type `setup /TS:` and the appropriate switches. For example:

```
setup /TS: /USER:<user> /DOM:domain /PASS:password /SLF:C:\path\slf.slf
```

See [“Command line switches for silent mode installation of Backup Exec”](#) on page 105.

If you use the command line switches without the /S: switch, the Backup Exec installation program launches with the command line parameters as defaults for the installation options. For example, if /S: had been left in the above example, the Backup Exec installation program launches with the user name, domain, password, and license appearing on the installation dialog boxes.

5 Press **Enter**.

## Command line switches for silent mode installation of Backup Exec

The command line switches used for silent mode installation of Backup Exec are described in the following table.

Note the following general rules for using these switches:

- Substitute values appropriate for your environment for the values that are shown in italics; for example substitute your password for *password*.
- Enclose the value in quotation marks if it contains spaces, such as "Operations Weekly Backup".

See [“Installing Backup Exec using the command line \(silent mode\)”](#) on page 104.

**Table 2-12** Command line switches for silent mode installation of Backup Exec

Switch	Additional Switches	Description
/TS:		Installs Backup Exec using the options that are specified with the additional switches. The /USER:" <i>user</i> " /DOM:" <i>dm</i> " /PASS:" <i>pw</i> " switch is required.

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
(continued)

Switch	Additional Switches	Description
	/USER:" <i>user</i> " /DOM:" <i>dm</i> " /PASS:" <i>pw</i> "	Required. Specifies an existing user, domain, and password for the Backup Exec system service account. Silent mode installation will not create a user.  <b>Note:</b> When using /PASS;, if a quote is needed as part of the password, specify it as \". For example, if the password is pass\"word, type it as /PASS:pass\"word. If the characters \" are used as part of the password, you must precede each character with a \. For example, if the password is pass\"word, type it as /PASS:pass\\\"word.
	/DEST:" <i>path</i> "	Specifies the path where Backup Exec will be installed. Otherwise, the default path Program Files\Symantec\Backup Exec is used.
	/DOCS:	Installs the online documentation.

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
*(continued)*

Switch	Additional Switches	Description
	/NOINSTALL:	Lets you select all install options without actually installing the Backup Exec software. This option can be used with the /CPF: switch.
	/SLF: <i>slf file</i>	<p>Specifies one or more licenses to use for installing Backup Exec and additional options. Licenses are not required to install the Remote Administrator. You may specify up to 99 licenses. If none are specified, then a trial copy of Backup Exec is installed.</p> <p>The following examples show how the /SLF switch can be used:</p> <pre>/SLF:"C:\path\slf1.slf"</pre> <pre>/SLF:"C:\path\slf1.slf","C:\path\slf2.slf","C:\path\slf3.slf"</pre> <p><b>Note:</b> If you install a license for an option or agent, you must also type a switch that specifies the option or agent. The switches that specify an option or agent are included in this table.</p>

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
(continued)

Switch	Additional Switches	Description
	/TD:NEW or ALL	<p>/TD:NEW installs tape drivers only for the drives that do not have drivers loaded.</p> <p>/TD:ALL installs tape drivers for all drives.</p> <p><b>Note:</b> To install the Symantec tape drivers, the Windows driver signing policy must be set to Ignore. However, for Windows 2003/2008, the driver installation fails when the signing policy is set to Ignore. You can install the drivers using Tapeinst.exe instead. See your Microsoft Windows documentation for more information about the signing policy.</p>
	/CPF:"path\filename.cpf"	Creates a file containing all of the installation parameters provided. Note that the file is not encrypted, which exposes parameters.
	/DBSERVER:<server\instance>	Installs the Backup Exec Database to the specified SQL server.

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
*(continued)*

Switch	Additional Switches	Description
	/DBINSTPATH: <SQL Express destination folder>	Installs the default instance of SQL Express in the specified folder.
	/NOUPDATE:	Skips the installation of Symantec LiveUpdate.
	/DISADVRT	Installs the Agent for Windows without publishing it.
	/SQLXSETUP:<SQL Express Install Package>	Specifies the location of the language-specific install package for Microsoft SQL Server 2005 Express Edition.
	/LOADER:	Installs the Library Expansion Option.
	/APPLICATIONS:	Installs the Agent for Applications and Databases.
	/VIRT:	Installs the Agent for VMware and Hyper-V

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
(continued)

Switch	Additional Switches	Description
	/ENTSERVER:	<p>Installs the Enterprise Server Option.</p> <p>You must use one or both of the following switches with the Enterprise Server Option switch to indicate which options you want to install.</p> <ul style="list-style-type: none"> <li>■ /CASO: Installs the Central Admin Server Option.</li> <li>■ /ADBO: Installs the Advanced Disk-based Backup Option.</li> </ul>
	/MMS:<CAS server name>	Creates a managed Backup Exec server for use with the Central Admin Server Option.
	/CASOPVLOCAL: <1 or 0>	<p>/CASOPVLOCAL:&lt;1&gt; indicates that device and media data will be stored locally on the managed server. Use this switch with /MMS:.</p> <p>/CASOPVLOCAL:&lt;0&gt; indicates that device and media data will be stored on the administration server. Use this switch with /MMS:.</p>

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
*(continued)*

Switch	Additional Switches	Description
	/ACCESSCATALOGSANDRESTORE:	Enables unrestricted access to catalogs and backup sets for restore.  This switch is used with the /MMS:<CAS server name> switch and it replaces the /SSO:<primary server name> switch.
	/NTA:	Installs the Agent for Windows.
	/ADBO:	Installs the Advanced Disk-based Backup Option.  You must use /ENTSERVER: with this switch.
	/CASO:	Installs the Central Admin Server Option.  You must use /ENTSERVER: with this switch.
	/NDMP:	Installs the NDMP Option.
	/MAC:	Installs the Agent for Mac.
	/RAULUS:	Installs the Agent for Linux.
	/STORPROV:	Installs the Storage Provisioning Option.

**Table 2-12** Command line switches for silent mode installation of Backup Exec  
(continued)

Switch	Additional Switches	Description
	/DEDUPE:	Installs the Deduplication Option.
	/EXCHARCH:	Installs the Exchange Mailbox Archiving Option.
	/NTFS:	Installs the File System Archiving Option.
	/VTL:	Installs the VTL Unlimited Drive Option.
	/FIXEDSPO:	Installs the Storage Provisioning Option - Basic.
	/RMAL:	Installs the Remote Media Agent for Linux.
	/COPYCONFIG:	Installs the Copy Server Configuration option.
-?		Provides help on all command line operations, usage, and special switches.

## Creating installation parameter files

If you use the command line switches without the /S: switch, the Backup Exec installation program launches with the command line parameters as defaults for the installation options. For example, suppose you type:

```
SETUP /TS: /USER:user /DOM:domain /PASS:password /SLF:"C:\path\slf1.slf
```

The Backup Exec installation program is launched. The screens that let you enter the logon credentials and the license will appear with the information you provided on the command line.

You can also use the /CPF: command to create a parameter file that contains all of the command line options you provided. This parameter file can then be used to provide the options for installing either Backup Exec or the Remote Administrator. Note that the file is not encrypted, which exposes parameters such as the password.

**To create installation parameter files**

- 1 Open a Windows command prompt.
- 2 Change to the drive containing the Backup Exec installation media.
- 3 Change directories to one of the following:

For 32-bit computers \be\winnt\install\be32

For 64-bit computers \be\winnt\install\be64

- 4 Type `setup /TS:` and the appropriate switches, including /CPF: and the full path name of the parameter file. For example, type:

```
setup /TS: /USER:user /DOM:domain /PASS:password/SLF: "C:\path\slf1..
```

Backup Exec will be installed on your server and a parameter file containing the user name, domain, password, and license will be saved to a removable device. You can use this parameter file to install to another computer.

See [“Using installation parameter files”](#) on page 113.

**Using installation parameter files**

You can use the /CPF: command to create a parameter file that contains all of the command line options you provided. This parameter file can then be used to provide the options for installing either Backup Exec or the Remote Administrator.

See [“Creating installation parameter files”](#) on page 112.

**To use installation parameter files**

- 1 Open a Windows command prompt.
- 2 Change to the drive containing the Backup Exec installation media.
- 3 Change directories to `\WINNT\INSTALL\BE.`

- 4 Type:`SETUP /PARAMS:"A:\file name" /S:`
- 5 If you want to overwrite a parameter, specify the new parameter. For example, to change the password, type:`SETUP /PARAMS:"A:\file name" /PASS:new password/S:`

## Installing a trial version of Backup Exec agents and options

You can install a trial version of most Backup Exec agents and options at any time after the core product is licensed. Each agent and each option has its own independent trial period. When a trial period is about to expire, Backup Exec warns you with an alert.

You can view a list of agents and options that are available for a trial period. You can also view the amount of time that is left in each individual trial period.

See [“Viewing license information”](#) on page 120.

### To install a trial version of Backup Exec agents and options

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Options and Licenses on this Backup Exec Server**.
- 2 Click **Next**.  
Do not enter any license file information or serial numbers.
- 3 Select the agents or options that you want to evaluate.
- 4 Click **Next**.
- 5 If you are prompted, enter information or choose settings for the additional options that you want to install. Click **Next** after each selection.
- 6 Read the Backup Exec installation review, and then click **Install**.  
The Backup Exec services are stopped while the additional options are installed. If any active jobs are in progress, you are prompted to stop them, or to wait for the jobs to finish.  
When the installation is complete, the services restart.
- 7 Click **Finish**.

## About the installation log

Backup Exec creates an installation log file, named `Bkupinst2012.htm`, when you install Backup Exec and when you install patches. This log file can help you

troubleshoot installation problems. The log file provides links to Technotes for the most common errors. If you install the Agent for Windows, a log file called RAWSin2012.htm is also created.

In addition, the text in the log file uses the following colors so you can identify warnings and errors:

**Table 2-13** Installation log colors

This color	Indicates
Black	Normal operations
Orange	Warning messages
Red	Error messages

The Bkupinst2012.htm file is located in the following locations:

- For Windows 2003: C:\allusersprofile\Application Data\Symantec\Backup Exec\Logs
- For Windows 2008 and later: C:\ProgramData\Symantec\Backup Exec\Logs

---

**Note:** The ProgramData folder is a hidden folder. If you do not see the ProgramData folder, refer to the Microsoft Windows documentation for instructions on how to display hidden folders.

---

## Repairing Backup Exec

If you have missing or corrupted Backup Exec files or registry keys on the local Backup Exec server, run the Repair option. The program stops all Backup Exec services, reinstalls corrupted files and registry keys, reinstalls tape devices (stand-alone drives and libraries), and restarts the services. The database is not reinstalled.

Any changes that are made to Backup Exec program files and registry keys are reset to the original settings.

### To repair Backup Exec

- 1 Close the Backup Exec application.
- 2 From the Windows Control Panel, select the option to uninstall a program.
- 3 Select **Symantec Backup Exec**, and then click **Change**.

- 4 Select **Local installation** and **Repair**, and then click **Next**.  
Make sure the option **Remote installation** is not selected.
- 5 If you are prompted to enter credentials for the Backup Exec service account, type the correct credentials, and then click **Next**.
- 6 Select **Install**.
- 7 Click **Finish**.

## About updating Backup Exec with LiveUpdate

Symantec LiveUpdate, which provides updates, upgrades, and new versions of Backup Exec, is installed automatically with Backup Exec. Backup Exec installs the latest version of LiveUpdate. If a previous version of LiveUpdate is detected on the computer, Backup Exec upgrades it.

LiveUpdate can be run manually or can be configured to run automatically. If you enable the automatic update option, you can configure LiveUpdate to poll the main Symantec Web server on a scheduled interval. By default, LiveUpdate checks for updates every Sunday night at 10pm. If there is an update, LiveUpdate notifies you with an alert. The automatic update option only searches for Backup Exec updates. It does not show updates for other Symantec products that use LiveUpdate. Likewise, when LiveUpdate is scheduled to automatically update other Symantec products, it does not search for Backup Exec updates. In addition to scheduling LiveUpdate, you can also run it manually at any time. You can access LiveUpdate from Backup Exec, but you cannot access it from the Windows Start menu. If LiveUpdate installs any files, the Bkupinst2012.htm installation log file is updated with information about those files.

---

**Note:** During the installation and update process, the Backup Exec services are stopped and started one time during a LiveUpdate session, regardless of the number of updates that are being installed. All selected patches are installed in order.

---

When LiveUpdate installs updates on the Backup Exec server, it also determines if computers on which the Agent for Windows is installed have the latest updates. If you do not have the latest updates you receive an alert to install the updates.

You can use the LiveUpdate Administrator Utility with LiveUpdate. The LiveUpdate Administrator Utility allows an administrator to modify LiveUpdate so that network users can download program and virus definition updates from an internal server rather than going to the Symantec LiveUpdate server over the Internet.

Go to [ftp://ftp.symantec.com/public/english\\_us\\_canada/liveupdate/luadmin.pdf](ftp://ftp.symantec.com/public/english_us_canada/liveupdate/luadmin.pdf)

See [“About scheduling automatic updates using LiveUpdate”](#) on page 117.

See [“Running LiveUpdate manually”](#) on page 119.

See [“Viewing installed updates”](#) on page 119.

See [“Installing updates to the Agent for Windows on remote computers”](#) on page 89.

## About scheduling automatic updates using LiveUpdate

You can schedule LiveUpdate to check for updates as follows:

- Every day at a specific time
- Every week on a specific day of the week and at a specific time
- Every month on a specific day of the month and at a specific time

When you schedule automatic updates through Backup Exec, the settings apply only to updates for Backup Exec. Changes that you make to the LiveUpdate schedule for Backup Exec do not affect the schedule for any other software applications that use LiveUpdate.

At the scheduled time, LiveUpdate automatically connects to the appropriate Web site, and then determines if your files need to be updated. Depending on the options that you select, Backup Exec either downloads and installs the files in the proper location or sends an alert to notify you that updates are available.

Backup Exec sends the following LiveUpdate alerts:

**Table 2-14** LiveUpdate alerts

Backup Exec sends this alert	When
LiveUpdate Informational Alert	An update is installed successfully.
LiveUpdate Warning Alert	An update is installed successfully. However, you must restart the computer.
LiveUpdate Error Alert	An update fails to install.

See [“Scheduling automatic updates using LiveUpdate”](#) on page 117.

## Scheduling automatic updates using LiveUpdate

You can schedule LiveUpdate to check for updates for Backup Exec.

See [“About scheduling automatic updates using LiveUpdate”](#) on page 117.

### To schedule automatic updates using LiveUpdate

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**
- 2 In the left pane, select **LiveUpdate**.
- 3 Complete the appropriate options.  
See “[Application settings for LiveUpdate](#)” on page 118.
- 4 Click **OK**.

## Application settings for LiveUpdate

You can schedule LiveUpdate to check for updates for Backup Exec.

See “[Scheduling automatic updates using LiveUpdate](#)” on page 117.

**Table 2-15** Application settings for LiveUpdate

Item	Description
<b>Check for updates automatically according to a schedule</b>	Lets you schedule automatic updates, and then choose the frequency of the updates.
<b>Daily</b>	Enables Backup Exec to check for new updates every day. In the At field, enter the time to check for new updates.
<b>Weekly</b>	Enables Backup Exec to check for new updates once a week. In the Every field, select the day of the week on which to check for updates. In the At field, enter the time to check for new updates.
<b>Monthly</b>	Enables Backup Exec to check for new updates once a month. In the Every field, select the day of the month on which to check for updates. In the At field, enter the time to check for new updates.
<b>Interval</b>	Lets you set the date and time that you want Backup Exec to check for new updates.
<b>Download and install all available updates automatically</b>	Enables Backup Exec to download and install all updates that are available without prompting you first.

**Table 2-15** Application settings for LiveUpdate (*continued*)

Item	Description
<b>Send an alert when updates are available; do not download or install updates</b>	Enables Backup Exec to alert you when updates are available. Updates are not downloaded or installed. This option is the default.  If you select this option, you need to run LiveUpdate manually to download and install the available updates.

## Running LiveUpdate manually

You can either set a schedule for LiveUpdate or run LiveUpdate manually at any time to check for updates. You can configure LiveUpdate to run in either Interactive mode or Express mode. Interactive mode gives you the flexibility to choose which updates you want to install. Express mode automatically installs all of the Backup Exec updates. For information about how to change the LiveUpdate mode, see the LiveUpdate documentation.

---

**Note:** By default, LiveUpdate is configured for Interactive mode. If you change it to Express mode you must cancel the LiveUpdate session and restart it before the change takes place.

---

### To run LiveUpdate manually

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **LiveUpdate**.
- 2 Do one of the following:

If LiveUpdate is set for Express mode      Click **Start**.

If LiveUpdate is set for Interactive mode      Click **Next**.

See “[Scheduling automatic updates using LiveUpdate](#)” on page 117.

## Viewing installed updates

You can view hot fixes and service packs that are installed on a Backup Exec server. You must be logged on with administrator privileges.

If a hot fix is installed before a service pack, that hot fix no longer displays as installed since the service pack contains the hot fix.

A hot fix that is offered after the service pack is released is displayed with the previous service pack.

**To view installed updates**

- ◆ Click the Backup Exec button, select **Installation and Licensing**, and then select **Installed Updates**.

## Viewing license information

You can view information about the Backup Exec options that are licensed and installed on a Backup Exec server. You can also view a list of agents and options that are available for a trial, as well as how much time is left in each individual trial period.

**To view license information**

- ◆ Click the Backup Exec button, select **Installation and Licensing**, and then select **License Information**.

## Finding installed licenses in your environment

The License Assessment Tool lets you run a license scan on the computers on which the following are installed:

- Backup Exec 2010 or later
- Symantec System Recovery

Both of these products are Backup Exec installations.

You can also use the License Assessment Tool to view maintenance contract expiration dates so that you can renew contracts before they expire.

The License Assessment Tool reports maintenance contract information when the following conditions are met:

- The Backup Exec server in the license scan must run Backup Exec 2010 R2 or later.
- The Backup Exec server must have maintenance contract information available.
- The Backup Exec server must have a network connection.

See [“About Backup Exec maintenance contract information”](#) on page 121.

On each Backup Exec installation for which you run a license scan, the License Assessment Tool reviews the resources that are backed up. Resources are files such as Windows shares, or application databases such as Microsoft SQL Server.

A report compares the number of resources that are backed up with the number of licenses that are installed.

---

**Note:** Scans for time periods and date ranges do not apply to the Backup Exec Archiving Option. Only the resources that are backed up by Agent for Windows are scanned if you select a time period or date range.

---

The License Assessment Tool report provides the following information:

- The number of additional licenses that are recommended for a Backup Exec installation.
- The versions of Backup Exec that are installed so that you can consider purchasing upgrades.

Running the License Assessment Tool does not ensure license compliance. For more information about licensing, contact your reseller, or go to the following URL:

<https://licensing.symantec.com>

#### To find installed licenses in your environment

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Backup Exec License Assessment Tool**.
- 2 Follow the on-screen prompts.

## About Backup Exec maintenance contract information

After you purchase maintenance contracts for your Backup Exec products, Symantec automatically updates the Symantec Licensing Portal Web site with your maintenance contract information. Maintenance contract information includes the contract serial number and the contract expiration date.

To retrieve the contract expiration dates, you enter your maintenance contract serial numbers in the installation wizard. The installation wizard connects to the Symantec Web service, at which point you may be prompted to enter customer and technical contact information. The installation wizard then retrieves the maintenance contract information for each contract that you have purchased. Backup Exec then uses the contract expiration information to automatically set Backup Exec alerts that remind you to renew the maintenance contracts before they expire. Reminder alerts are set at 30-day, 60-day, and 90-day intervals, based on the expiration date of the maintenance contract.

All Backup Exec products and maintenance contracts have Symantec serial numbers. The serial numbers appear on the printed certificate that you receive

with your order. To determine the correct serial numbers to enter in the installation wizard, look for the Maintenance/Subscription columns on your certificate. Each maintenance contract specifies a start date and an end date; these dates appear in the Maintenance/Subscription columns.

Maintenance contract serial numbers consist of a letter and a series of numbers. They are not the same as Backup Exec licenses, nor do they use the same format as licenses.

See [“Viewing Backup Exec maintenance contract information”](#) on page 122.

See [“Updating expired maintenance contracts”](#) on page 123.

## Viewing Backup Exec maintenance contract information

You can view maintenance contract information after you enter the serial numbers for your contracts in the installation wizard. Backup Exec stores maintenance contract details locally on the Backup Exec server after it retrieves the information from the Symantec Web service.

See [“About Backup Exec maintenance contract information”](#) on page 121.

### To view Backup Exec maintenance contract information

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Maintenance Contract Information**.

See [“Backup Exec maintenance contract information”](#) on page 122.

- 2 Click **OK**.

## Backup Exec maintenance contract information

You can view the maintenance contract information that Backup Exec has retrieved from the Symantec Web service.

See [“About Backup Exec maintenance contract information”](#) on page 121.

See [“Viewing Backup Exec maintenance contract information”](#) on page 122.

**Table 2-16** Maintenance contract information details

Item	Description
<b>Feature</b>	Shows the name of the feature that the maintenance contract covers.  A green check icon indicates that the maintenance contract for the feature is valid.  A red X icon indicates that the maintenance contract for the feature has expired.
<b>Serial Number</b>	Shows the serial number of the maintenance contract.
<b>Expiration Date</b>	Shows the expiration date of the maintenance contract.

## Updating expired maintenance contracts

When your maintenance contracts expire, follow these steps to update them.

**Table 2-17** How to update expired maintenance contracts

Step	Additional information
Purchase new maintenance contracts.	Access the Symantec Licensing Portal Web site to purchase new contracts.
Wait for your new serial numbers to arrive.	The new serial numbers should arrive by email within two to five business days of the purchase date.
Launch the installation wizard from the Backup Exec Administration Console.	Use the option <b>Install options and licenses on this Backup Exec server</b> on the <b>Installation and Licensing</b> menu, which is accessed from the Backup Exec button.
Use the installation wizard to add the new serial numbers, and then remove the expired serial numbers.	After you select the expired serial numbers from the list, use the <b>Remove</b> option.

See [“About Backup Exec maintenance contract information”](#) on page 121.

## Managing maintenance contract customer numbers

Backup Exec provides a place where you can store all of your maintenance contract customer numbers. You need to provide these numbers when you call technical support.

### To manage maintenance contract customer numbers

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Maintenance Contract Customer Numbers**.
- 2 Do one of the following:
  - To add a new customer number, click **New**, and then enter your customer number and any notes for this number.
  - To remove a customer number, select the number from the list, and then click **Delete**.

See [“Maintenance Contract Customer Number options”](#) on page 124.
- 3 Click **Close**.

### Maintenance Contract Customer Number options

The following options are available for maintenance contract customer numbers. See [“Managing maintenance contract customer numbers”](#) on page 124.

**Table 2-18** Maintenance contract customer number options

Item	Description
<b>Customer Number</b>	Indicates the customer number that is listed on your maintenance contract.
<b>Notes</b>	Lets you enter notes about each customer number.

## About upgrading from previous versions of Backup Exec

You can use the Backup Exec installation media to upgrade from Backup Exec version 12.5 and later to the current version. The current version of Backup Exec replaces any previous versions. Separate installations of different versions of Backup Exec cannot exist on the same computer. Most settings and all catalogs and all data directories from previous versions of Backup Exec are kept, unless you choose to remove them. This version of Backup Exec can read and restore

data from any previous version of Backup Exec or Backup Exec for NetWare, except where Symantec has made end-of-life decisions.

---

**Note:** Upgrading to the current version of Backup Exec from a version before 12.5 requires a multi-step process.

---

When you upgrade, Backup Exec automatically converts your existing definitions, configurations, and jobs to the current version. After the migration has completed, Backup Exec displays a Data Migration report. In this report, you can see how your jobs were migrated. Due to the new backup paradigm in Backup Exec 2012, some of your jobs may be combined, split, or moved.

See [“About the Data Migration report”](#) on page 127.

Backup Exec 2012 provides backward compatibility as follows:

- Backup Exec 2012 can communicate with Backup Exec 12.5 Remote Agent for Windows Systems and later.
- Backup Exec 2012 supports side-by-side installations of the Remote Administration Console for Backup Exec 2010 and later.
- Backup Exec 2012 Central Admin Server Option server can communicate with Backup Exec 2010 R3 (with the most recent service packs) for the purpose of rolling upgrades.

A Remote Administration Console that uses a previous version of Backup Exec cannot be used with a Backup Exec server on which the current version is installed. For example, a Backup Exec 2010 Remote Administration Console cannot manage a Backup Exec 2012 Backup Exec server.

Before you upgrade Backup Exec, do the following:

- Delete the job histories and the catalogs that you no longer need to shorten the upgrade window.
- Run a database maintenance job.
- Verify that all available updates are installed for your current version of Backup Exec.
- Locate your license information and verify that your licenses are current. You must enter license information for Backup Exec 2012 when you upgrade.

You cannot change the configuration of your Backup Exec servers during an installation. For example, you cannot change an administration server to a managed server. If you want to change the configuration of your Backup Exec servers, do it either before or after you upgrade to the current version. You cannot

change the database location during the upgrade process. If you want to change the database location after the upgrade, use BEUtility.

---

**Note:** If you upgrade from a previous version of Backup Exec that uses a non-English version of Windows, you must download the SQL Express SP4 setup file for that language from the Microsoft Web site.

---

See “[Installing a typical installation of Backup Exec](#)” on page 68.

See “[Installing a custom installation of Backup Exec](#)” on page 70.

## Backup Exec pre-upgrade checklist

Before you upgrade from a previous version of Backup Exec to the current version, you should do the following:

- Ensure that your backups are up to date. Also, if you have backup-to-disk files on your Backup Exec server, ensure that those files are copied to another location.
- Disable your antivirus software.
- Verify that your system meets the system requirements for the new version of Backup Exec.  
See “[System requirements](#)” on page 65.
- Check the Backup Exec Software Compatibility List to verify that the applications that you want to back up are still supported.  
You can find a list of compatible operating systems, platforms, and applications at the following URL:  
<http://entsupport.symantec.com/umi/V-269-1>
- Download all available upgrades and hot fixes for the version of Backup Exec that you want to install.
- Plan to perform the upgrade when system downtime won't affect users.
- Ensure that your serial numbers or Symantec License Files are available. You must enter new Backup Exec 2012 license information during the upgrade.
- Review the document *Best practices for installing Backup Exec* on the Backup Exec Knowledge Base.
- Review the topic *About upgrading from previous versions of Backup Exec* to learn about the upgrade process.  
See “[About upgrading from previous versions of Backup Exec](#)” on page 124.

## About the Data Migration report

When you upgrade to Backup Exec 2012 from a previous version of Backup Exec, your existing definitions, configurations, and jobs are converted automatically to the current version. After the migration has completed, Backup Exec displays a migration report. In this report, you can see how your jobs were migrated. Due to the new backup paradigm in Backup Exec 2012, some of your jobs may be combined, split, or moved.

Symantec recommends that you review the Data Migration report thoroughly to determine how your existing jobs have changed and how you may need to adjust your jobs manually. The Data Migration report is available for viewing from the Backup Exec Administration Console at any time after the migration has completed.

See [“Viewing the Data Migration report”](#) on page 127.

## Viewing the Data Migration report

The Data Migration report lists the ways in which your previous jobs were changed during the migration to Backup Exec 2012. The Data Migration report is available for viewing from the Backup Exec Administration Console at any time after the migration has completed.

See [“About the Data Migration report”](#) on page 127.

### To view the Data Migration report

- ◆ Click the Backup Exec button, select **Installation and Licensing**, and then select **Post-Migration Report**.

## Post-installation tasks

For best results before starting Backup Exec, do the following:

- Create disk storage so that Backup Exec can automatically manage the lifecycle of your backup data.  
See [“About disk storage”](#) on page 307.
- Make sure that your storage devices are connected and configured properly.  
See [“About the Configure Storage wizard”](#) on page 145.
- Decide what types of storage devices you want to use for your backup jobs. You can configure storage devices when you prepare your Backup Exec environment.
- Understand how Backup Exec provides overwrite protection for your tape and disk cartridge media.

See [“About media overwrite protection levels for tape and disk cartridge media”](#) on page 377.

- Understand the default media set for tape and disk cartridge media, and its four-week overwrite protection period.  
See [“About the default media set Keep Data for 4 Weeks”](#) on page 373.
- Learn about creating new media sets with different retention periods.  
See [“Creating media sets for tape and disk cartridge media”](#) on page 373.
- Decide which credentials you want your Backup Exec logon account to use when browsing and making backup selections. You can use an existing Backup Exec logon account, or create a new one.  
See [“Creating a Backup Exec logon account”](#) on page 500.

## Uninstalling Backup Exec

Use Microsoft’s Add or Remove Programs option to remove Backup Exec from a computer. For additional information on Add or Remove Programs, refer to your Microsoft documentation.

Uninstalling Backup Exec also removes Symantec tape class drivers. If you reinstall Backup Exec and want to use Symantec tape class drivers, you must reinstall them.

### To uninstall Backup Exec

- 1 Close Backup Exec.
- 2 From the Windows Control Panel, select the option to uninstall a program.
- 3 Select **Symantec Backup Exec 2012**, and then click **Uninstall**.
- 4 When you are prompted to confirm that you want to uninstall Backup Exec from your computer, click **Yes**.
- 5 Select whether you want to remove only the Backup Exec program files or Backup Exec and all of its associated files.
- 6 Click **Next**.

If the uninstall program fails, click **View Installation Log File** for additional information.

- 7 If you are prompted, restart the computer.

See [“Uninstalling Backup Exec options from the local Backup Exec server”](#) on page 129.

# Uninstalling Backup Exec using the command line

If Backup Exec is already installed, you can use the setup.exe program to uninstall Backup Exec program files and Backup Exec data.

## To uninstall Backup Exec using the command line

- 1 Open a Windows command prompt.
- 2 Change to the drive containing the Backup Exec installation media.
- 3 Change directories to one of the following:

For 32-bit computers `\be\winnt\install\be32`

For 64-bit computers `\be\winnt\install\bex64`

- 4 To remove the Backup Exec program files but keep all of the Backup Exec data, type:

```
SETUP /UNINSTALL:
```

To remove the Backup Exec program files and the Backup Exec data, type:

```
SETUP /REMOVEALL:
```

See [“Installing Backup Exec using the command line \(silent mode\)”](#) on page 104.

## Uninstalling Backup Exec options from the local Backup Exec server

The Installation Wizard removes Backup Exec options from the local Backup Exec server. All corresponding files, registry keys, and configurations are removed.

---

**Note:** Symantec license files remain on the server after options are uninstalled. Do not delete the Symantec license files while Backup Exec is installed. Deleting the Symantec license files causes the trial version to go into effect.

---

### To uninstall Backup Exec options from the local Backup Exec server

- 1 Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Options and licenses on this Backup Exec Server**.
- 2 On the **Add Licenses** panel, in the **Available Licenses** list, select the item that you want to remove, and then click **Remove**.

- 3 Click **Next**.
- 4 On the **Configure Options** panel, verify that the option you want to remove is not checked, and then click **Next**.
- 5 If you are prompted to enter credentials for the Backup Exec service account, type the correct credentials, and then click **Next**.
- 6 Read the installation summary, and then click **Install** to start the process.
- 7 When the Installation Wizard has completed, click **Finish**.

See [“Uninstalling Backup Exec”](#) on page 128.

# Getting Started

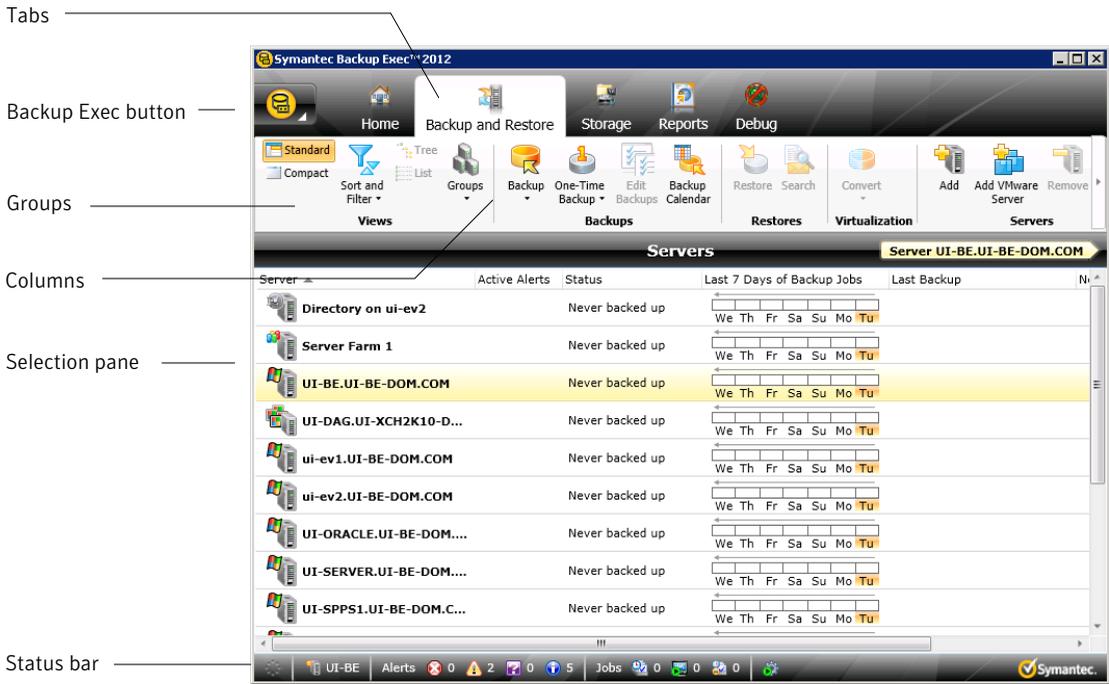
This chapter includes the following topics:

- [About the administration console](#)
- [About sorting and filtering information](#)
- [About the Home tab](#)
- [About the Symantec RSS Reader](#)
- [Getting ready to back up your computer](#)

## About the administration console

From the administration console, you can access the Backup Exec features.

**Figure 3-1** Administration console



The administration console screen includes the following components:

**Table 3-1** Administration console components

Item	Description
Backup Exec Button	The Backup Exec button displays on the upper left side of the administration console. To display the options in the Backup Exec button, click the Backup Exec button, select the menu name, and then select an option. You can launch Backup Exec operations by clicking options from a menu.

**Table 3-1** Administration console components (*continued*)

Item	Description
Tabs	<p>Tabs appear across the top your screen and enable you to navigate to Backup Exec's views.</p> <p>Views that can be accessed through the navigation bar include the following:</p> <ul style="list-style-type: none"><li>■ <b>Home.</b> Use this view to quickly access the Backup Exec features that you use frequently. You can customize the Home view by adding or deleting items.</li><li>■ <b>Backup and Restore.</b> Use this view to create a backup or restore job.</li><li>■ <b>Storage.</b> Use the view to configure your storage and perform storage operations, manage your media, and launch utility jobs.</li><li>■ <b>Reports.</b> Use this to view, print, save, and schedule reports about your Backup Exec server, its operations, and its device and media usage. Also, you can use this to create a custom report. You can view a report in Backup Exec in a PDF or HTML format. You can also save and print reports in PDF, XML, HTML, Microsoft Excel (XLS), and Comma Separated Value (CSV) formats.</li></ul>
Groups	<p>Groups display on the tabs in the administration console. The contents of the groups are items that you can use to initiate actions such as creating a new backup job or configure storage. The items in the groups are dynamic, changing according to the selection. Some options may be unavailable until an item is selected from the console screen or a prerequisite task is performed.</p>
Selection pane	<p>The Selection pane is where you select items to work with, such as servers to back up or restore.</p>
Status bar	<p>The status bar appears on the bottom of the administration console and provides information about the Backup Exec server, jobs running or scheduled to run, alerts, and services running.</p>
Columns	<p>You can change the location of columns by dragging and dropping them. In addition, you can right-click a column to select the columns you would like to make visible, configure column settings, or sort the columns. You can also change the order of the entries in a column by clicking the column heading. For example, names of reports display in alphabetical order by default. To display report names in reverse alphabetical order, click the Name column heading on the Reports view.</p>

## Displaying the Backup Exec version

You can display information about the version of Backup Exec that you have installed.

### To display the Backup Exec version

- 1 Click the Backup Exec button, and then select **Help and Documentation** and then click **About Backup Exec**.
- 2 Click **OK**.

## About sorting and filtering information

You can customize the information that displays on the **Backup and Restore** tab and on the **Storage** tab.

You can do any or all of the following actions:

- Choose a default configuration that Backup Exec provides, such as **Servers with Active Jobs** or **Failed Jobs**.
- Specify a sort order for the columns that appear in the views.
- Specify the values that you want to use to filter the information that Backup Exec displays.
- Specify the columns that you want to appear and the order in which they should appear.
- Create and save a configuration to use again.

See [“Sorting and filtering information”](#) on page 134.

See [“Deleting a configured view”](#) on page 135.

See [“Editing a configured view”](#) on page 136.

## Sorting and filtering information

You can customize a view on the **Backup and Restore** tab and on the **Storage** tab.

See [“About sorting and filtering information”](#) on page 134.

### To sort and filter information

#### 1 Do one of the following:

- |   |   |
|---|---|
| To customize a view of the computers in the list of servers | On the <b>Backup and Restore</b> tab, in the <b>Views</b> group, click <b>Sort and Filter</b> .                   |
| To customize a view of the storage devices                  | On the <b>Storage</b> tab, in the <b>Views</b> Group, click <b>List</b> , and then click <b>Sort and Filter</b> . |

#### 2 Do any of the following:

- |  |  |
|--|--|
| To select a default configuration, such as <b>Servers with Failed Backups</b> , or to select a configuration that you created and saved previously | Click <b>Configurations</b> and select a configuration.                              |
| To specify an ascending or descending sort order for the columns   | Click <b>Sort</b> , choose the options as appropriate, and then click <b>OK</b> .    |
| To specify one or more columns to filter for specific values   | Click <b>Filter</b> , choose the options as appropriate, and then click <b>OK</b> .  |
| To specify the columns that you want to display and the order in which they should appear  | Click <b>Columns</b> , choose the options as appropriate, and then click <b>OK</b> . |
| To create and save a configuration   | Click <b>Save</b> , choose the options as appropriate, and then click <b>OK</b> .    |

## Deleting a configured view

You can delete a configuration that you created that you no longer need.

See [“About sorting and filtering information”](#) on page 134.

### To delete a configured view

- 1 Do one of the following:

To delete a configuration from the **Backup and Restore** tab      On the **Backup and Restore** tab, in the **Views** group, click **Sort and Filter**.

To delete a configuration from the **Storage** tab      On the **Storage** tab, in the **Views** group, click **Sort and Filter**.

- 2 Click **Configurations**.
- 3 Select the configuration that you want to delete, and then click the delete icon.

## Editing a configured view

You can change the options for a configured view that you created.

See [“About sorting and filtering information”](#) on page 134.

### To edit a configured view

- 1 Do one of the following:

To edit a configuration from the **Backup and Restore** tab      On the **Backup and Restore** tab, in the **Views** group, click **Sort and Filter**.

To edit a configuration from the **Storage** tab      On the **Storage** tab, in the **Views** group, click **Sort and Filter**.

- 2 Click **Configurations**.
- 3 Select the configuration that you want to edit, and then click the pencil icon.

## About the Home tab

The **Home** tab on the Backup Exec administration console is a central location from which you can quickly access or view the Backup Exec features that you use frequently. You can customize the Home tab by adding or deleting items. The **Home** tab contains Backup Exec data and links to features. You can configure the **Layout**, and hide or display items in the **System Health** and the **Support** groups.

See [“Configuring the Home tab”](#) on page 140.

See [“Restoring the Home tab's default layout”](#) on page 140.

See [“Layout group”](#) on page 137.

See [“System Health group”](#) on page 137.

See [“Support group”](#) on page 139.

## Layout group

You can select one of the following layout configurations to display the items on the **Home** tab.

See [“About the Home tab”](#) on page 136.

**Table 3-2 Home Tab Layout items**

Item	Description
<b>One Column</b>	Displays the <b>Home</b> tab items in one column.
<b>Two Columns</b>	Displays the <b>Home</b> tab items in two columns.
<b>Narrow/Wide</b>	Displays the <b>Home</b> tab items in two columns with a narrow panel and a wide panel.
<b>Three Columns</b>	Displays the <b>Home</b> tab items in three columns.
<b>Reset Home Tab</b>	Restores the contents of the <b>Home</b> tab to the default configuration.

## System Health group

The items in the **System Health** group provide overviews of alerts, backup jobs, backup size data, storage and the Symantec ThreatCon Level. You can select the following items to display on the Backup Exec **Home** tab.

See [“Configuring the Home tab”](#) on page 140.

**Table 3-3** System Health group items

Item	Description
<b>Active Alerts</b>	<p>Lets you view all alerts that have not received a response. You can filter the alerts to view specific types of alerts, the source of the alerts, and the amount of time that alerts occurred.</p> <p>You can display any or all of the following types of alerts:</p> <ul style="list-style-type: none"> <li>■ <b>Error</b></li> <li>■ <b>Warning</b></li> <li>■ <b>Attention Required</b></li> <li>■ <b>Information</b></li> </ul>
<b>Alert History</b>	<p>Lets you view the property and response information for alerts.</p>
<b>Backup Status</b>	<p>Provides a summary view of the backup job status for the servers that are backed up or available for backup.</p>
<b>Backup Size</b>	<p>Provides a summary view of the amount of data that is backed up. You can customize the number of days for which you display information about the backup size. You can also select the type of backups that display.</p>
<b>Storage Status</b>	<p>Provides a summary view of the amount of space that is available on your storage. The storage information includes the total capacity that displays the amount space that is used for the different types of data.</p>
<b>Symantec ThreatCon Level</b>	<p>Provides an overall view of global Internet security level. Symantec's ThreatCon levels are based on a 1-4 rating system, with level 4 being the highest threat level.</p> <p>You must have Symantec Endpoint Protection 11.0 or later installed on the same computer as Backup Exec to view this item.</p>

## Support group

The items in the **Support** group provide technical support, documentation, licensing and maintenance contracts, and the Symantec RSS Reader resources. You can select the following items to display on the Backup Exec **Home** tab.

See “[Configuring the Home tab](#)” on page 140.

**Table 3-4** Support group items

Item	Description
<b>Technical Support</b>	Provides the following support options to help you understand product features and functionality or troubleshoot issues: <ul style="list-style-type: none"> <li>■ <b>Backup Exec Tech Center</b></li> <li>■ <b>Backup Exec Technical Support</b></li> <li>■ <b>Best Practices</b></li> <li>■ <b>Use MySupport to manage new or existing support cases</b></li> <li>■ <b>Symantec Remote Assistance</b></li> <li>■ <b>Register to receive notifications</b></li> <li>■ <b>Get Backup Exec updates</b></li> </ul>
<b>Documentation</b>	Provides the following documentation options to help you understand product features and functionality or troubleshoot issues: <ul style="list-style-type: none"> <li>■ <b>View Readme</b></li> <li>■ <b>View Administrator's Guide (PDF)</b></li> <li>■ <b>View Administrator's Guide Addendum (PDF)</b></li> </ul>
<b>Licensing and Maintenance</b>	Provides the following licensing and maintenance options to help you manage maintenance contracts and licenses, and run the License Assessment Tool: <ul style="list-style-type: none"> <li>■ <b>View license information</b></li> <li>■ <b>View maintenance contract information</b></li> <li>■ <b>Run the License Assessment Tool</b></li> </ul>
<b>Symantec RSS Reader</b>	Lets you view and add Backup Exec and Symantec RSS feeds.

## Configuring the Home tab

You can customize the **Home** tab by selecting the items that you want to display. You can drag and drop items to move them to another location on the **Home** tab or you can maximize a single item. The **Home** tab items contain Backup Exec data and links to features that you use frequently.

See [“Configuring the Home tab”](#) on page 140.

You can quickly restore the **Home** tab to its default configuration at any time.

See [“Restoring the Home tab's default layout”](#) on page 140.

### To configure the Home tab

- 1 On the **Home** tab, in the **Layout** group, click the layout for the items that you want to display.
- 2 In the **System Health** and **Support** groups, select the check box for the items that you want to display.
- 3 Drag the items to a column and position in which you want them to display to further customize the **Home** tab.

## Restoring the Home tab's default layout

You can customize the **Home** tab by selecting the items for the Backup Exec features that you use frequently.

See [“Configuring the Home tab”](#) on page 140.

You can quickly restore the **Home** tab to its default configuration at any time.

### To restore the Home tab's default configuration

- ◆ On the **Home** tab, in the **Layout** group, click **Reset Home Tab**.

## About the Symantec RSS Reader

The Symantec RSS Reader is an item that you can choose to display on the **Home** tab. You can customize the Symantec RSS Reader and select the default Backup Exec feeds that display in the reader. You can also add additional Symantec RSS feeds to the reader. The Symantec RSS Reader refreshes the RSS feeds every 15 minutes when the item is open in the **Home** tab.

See [“About the Home tab”](#) on page 136.

See [“Viewing an article in the Symantec RSS Reader”](#) on page 141.

See [“Customizing the Symantec RSS Reader”](#) on page 141.

See [“Removing a default RSS feed from the Symantec RSS reader”](#) on page 142.

## Viewing an article in the Symantec RSS Reader

The Symantec RSS Reader sorts articles by the date and the time. The reader displays the last entry of an article in the RSS feed; however, you can also choose to view the full article.

See [“About the Symantec RSS Reader”](#) on page 140.

### To view an article in the Symantec RSS Reader

- 1 On the **Home** tab, in the **Support** group, select the **Symantec RSS Reader** check box.
- 2 In the **Symantec RSS Reader**, click the arrow next to the RSS feed that contains the article.
- 3 Click the hyperlink for the article that you want to open.

The Symantec RSS Reader opens a new window that contains a portion of the article from the RSS feed.

- 4 Click **Go to full Article** to open Internet Explorer and view the entire contents of the article.

## Customizing the Symantec RSS Reader

You can customize and add Symantec RSS feeds to the reader in addition to the default Backup Exec RSS feeds. You can only add Backup Exec and Symantec RSS feeds to the Symantec RSS Reader.

See [“About the Symantec RSS Reader”](#) on page 140.

### To customize the Symantec RSS feeds to the Symantec RSS Reader

- 1 On the **Home** tab, in the **Support** group, select the **Symantec RSS Reader** check box.
- 2 In the **Symantec RSS Reader**, click the pencil icon to add an RSS feed.
- 3 Type the URL and the name of the RSS feed that you want to add. Or click the hyperlink to view additional Symantec RSS feeds.

See [“Add Symantec RSS Feed options”](#) on page 142.

- 4 Click **OK**.

## Add Symantec RSS Feed options

You can enter property information for an RSS feed that you want to add to the Symantec RSS Reader.

See [“Customizing the Symantec RSS Reader”](#) on page 141.

**Table 3-5** Symantec RSS Feed options

Item	Description
URL	Indicates the location of the RSS feed that you want to add to the Symantec RSS Reader.
Name	Indicates the name of the RSS feed that you want to display in the Symantec RSS Reader.
<a href="#">Click here to see more Symantec RSS feeds</a>	Shows a list of Symantec RSS feeds that you can add to the Symantec RSS Reader.

## Removing a default RSS feed from the Symantec RSS reader

You can remove the RSS feeds that display in the Symantec RSS reader. If the RSS feed is not open in the reader, the RSS feed does not refresh.

See [“About the Symantec RSS Reader”](#) on page 140.

### To remove an RSS feed from the Symantec RSS reader

- 1 On the **Home** tab, in the **Support** group, select the **Symantec RSS Reader** check box.
- 2 Do one of the following:

To remove a default Backup Exec RSS feed    Clear the check box of the Backup Exec RSS feed.

To remove an RSS feed that you added to the Symantec RSS reader    Click the red X next to the name of the RSS feed.

## Getting ready to back up your computer

Before you back up your computer, you should become familiar with how to do the following:

- **Configure Storage**  
See [“About the Configure Storage wizard”](#) on page 145.

- Configure logon accounts  
See [“About logon accounts”](#) on page 498.
- Select data to back up  
See [“Backing up data”](#) on page 163.



# Storage configuration

This chapter includes the following topics:

- [About the Configure Storage wizard](#)
- [About the All Storage view in Backup Exec](#)

## About the Configure Storage wizard

Use the Configure Storage wizard to set up different types of storage to which you can back up data. The Configure Storage wizard creates the storage that uses the best possible defaults for your environment. However, you can customize the defaults in the storage properties.

**Configure Storage** on the **Storage** tab launches the Configure Storage wizard.

After Backup Exec is installed and the Backup Exec services are started, any storage that is attached to the Backup Exec server is automatically detected. However, you must use the Configure Storage wizard to configure the storage for backups.

**Table 4-1** Storage that you can configure in the Configure Storage wizard

Type of storage	Description
Disk-based storage	<p>Storage that remains attached to the server.</p> <p>Types of disk-based storage include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Disk storage</b>            A location on a locally attached internal hard drive, a USB device, a FireWire device, or a NAS (network-attached storage) device.            See <a href="#">“About disk storage”</a> on page 307.</li> <li>■ <b>Disk cartridge storage</b>            Storage that usually remains attached to the server while you remove the media. Disk cartridges use disk cartridge media such as an RDX device, or devices that appear in Windows as removable storage.            See <a href="#">“About disk cartridge storage”</a> on page 317.</li> <li>■ <b>Deduplication disk storage</b>            A location on a hard drive that reduces the size of backups by storing only unique data.            See <a href="#">“About the Deduplication Option”</a> on page 752.</li> <li>■ <b>Storage arrays</b>            See <a href="#">“About the Storage Provisioning Option”</a> on page 1160.            Disk arrays that contain multiple disk drives that support data redundancy and failover.</li> <li>■ <b>Virtual disks</b>            Virtual disk storage that consists of multiple physical disks in a storage array.            See <a href="#">“About virtual disks in the Storage Provisioning Option”</a> on page 1171.</li> <li>■ <b>Vault store</b>            Disk storage for the archived data that the Backup Exec Archiving Option archives from one server.            See <a href="#">“About vault stores in the Archiving Option”</a> on page 1235.</li> </ul>

**Table 4-1** Storage that you can configure in the Configure Storage wizard  
(continued)

Type of storage	Description
Network storage	<p>Network storage includes the following:</p> <ul style="list-style-type: none"><li>■ <b>NDMP servers</b> Network attached storage (NAS) that supports the Network Data Management Protocol to allow the use of devices that are attached to the servers. See <a href="#">“About the NDMP Option”</a> on page 1062.</li><li>■ <b>OpenStorage devices</b> Network-attached storage that supports Symantec's OpenStorage technology. See <a href="#">“About OpenStorage devices”</a> on page 757.</li><li>■ <b>Cloud storage</b> A storage device to which you can send backup data to the cloud. You must have an account with a public cloud storage device vendor, and have the associated plug-in for the device. See <a href="#">“About cloud storage devices”</a> on page 323.</li><li>■ <b>Remote Media Agent for Linux</b> Storage that lets you back up data from remote computers to the storage devices that are directly attached to a Linux server. You can also back up to a simulated tape library on a Linux server. See <a href="#">“About the Remote Media Agent for Linux”</a> on page 1132.</li></ul>

**Table 4-1** Storage that you can configure in the Configure Storage wizard  
*(continued)*

Type of storage	Description
Tape storage	<p>Tape storage includes the following:</p> <ul style="list-style-type: none"> <li>■ Stand-alone tape drives Storage that uses a tape cartridge for reading and writing data. See <a href="#">“About tape drives and robotic libraries”</a> on page 334.</li> <li>■ Robotic libraries Storage that contains tape drives, slots, and an automated method for loading tapes. See <a href="#">“About robotic libraries in Backup Exec”</a> on page 349.</li> <li>■ Virtual tape libraries (VTLs) See <a href="#">“About the Virtual Tape Library Unlimited Drive Option ”</a> on page 334.</li> </ul>
Storage pools	<p>Storage pools include the following:</p> <ul style="list-style-type: none"> <li>■ Storage device pools</li> <li>■ Managed Backup Exec server pools</li> </ul>
Media sets and vaults	<p>Media sets include the following:</p> <ul style="list-style-type: none"> <li>■ Append period</li> <li>■ Overwrite protection period</li> <li>■ Vaulting rules for removable media, such as tapes.</li> </ul> <p>You can also run wizards to update media vaults.</p> <p>See <a href="#">“About tape and disk cartridge media”</a> on page 365.</p>

**Table 4-1** Storage that you can configure in the Configure Storage wizard (continued)

Type of storage	Description
Archiving	<p>Archiving lets you configure the following items that are required when you use the Archiving Option:</p> <ul style="list-style-type: none"> <li>■ Vault stores</li> <li>■ Vault store partitions</li> </ul> <p>See “<a href="#">About vault stores in the Archiving Option</a>” on page 1235.</p> <p>See “<a href="#">About vault store partitions in the Archiving Option</a>” on page 1238.</p>

You can find a list of compatible types of storage devices at the following URL:  
<http://entsupport.symantec.com/umi/V-269-2>

See “[About storage device pools](#)” on page 403.

See “[About storage operation jobs](#)” on page 410.

## About the All Storage view in Backup Exec

On the **Storage** tab, Backup Exec provides overview information for each storage device that you configure. You can also double-click each storage device to view details, such as properties, usage, and error statistics.

**Table 4-2** All Storage view

Item	Description
<b>Name</b>	<p>Indicates the name of the storage device.</p> <p>By default, Backup Exec provides a name for the storage device based on the type of storage and an incrementing number, such as Disk storage 0001. You can change the name of the storage device in the storage properties.</p> <p>See “<a href="#">Renaming a storage device</a>” on page 421.</p>

**Table 4-2** All Storage view (*continued*)

Item	Description
<b>State</b>	Indicates the state of the storage device, such as if it is online, offline, disabled, or if services need to be restarted.  See <a href="#">“Backup Exec server and storage device states”</a> on page 434.
<b>Active Alerts</b>	Indicates that an event or condition in Backup Exec has occurred for which a message is displayed or a response is required.  See <a href="#">“About alerts”</a> on page 279.
<b>Storage Trending</b>	Indicates the estimate for the number of days of storage that is left for disk storage and virtual disk storage.  See <a href="#">“About storage trending for disk storage and virtual disks”</a> on page 306.

**Table 4-2** All Storage view (*continued*)

Item	Description
<b>Capacity</b>	<p>Indicates the amount of disk space that is used for disk storage on the Backup Exec server.</p> <p>For tape and disk cartridge media, this column indicates the used native capacity and total native capacity of the media.</p> <p>Backup Exec provides overview information of used and free storage capacity, as well as capacity details for each storage that you configure. Storage capacity information is rolled up for any items that are collapsed under a storage type, such as a robotic library. The information that displays in the <b>Capacity</b> column includes all of the storage capacity of all of the collapsed items. When you expand the items, individual storage capacity information displays.</p> <p>Before capacity information can display for storage, you must inventory and catalog the storage.</p> <p>You can view storage capacity in the following places:</p> <ul style="list-style-type: none"> <li>■ On the <b>Storage</b> tab, in the <b>Capacity</b> column. When you hover the mouse over the capacity bar, additional details display in the tool tip.</li> <li>■ On the <b>Backup and Restore</b> tab, when you specify the storage for a backup job.</li> <li>■ On the <b>Home</b> tab, in <b>Disk Storage Status</b>.</li> <li>■ On the <b>Storage</b> tab, when you view properties for disk storage devices.</li> </ul> <p>See <a href="#">“About catalogs”</a> on page 242.</p> <p>See <a href="#">“About inventorying a storage device”</a> on page 422.</p>
<b>Compression</b>	<p>Displays the ratio of the uncompressed size of a file over its compressed size.</p>

**Table 4-2** All Storage view (*continued*)

Item	Description
<b>Jobs</b>	Indicates the jobs that have been sent to this storage.

# Backups

This chapter includes the following topics:

- [About preparing for your first backup](#)
- [About backing up data](#)
- [About the list of servers](#)
- [About server groups](#)
- [Backing up data](#)
- [Creating a one-time backup](#)
- [Creating a new backup from an existing backup](#)
- [Backing up server groups](#)
- [Running the next scheduled backup job](#)
- [Editing backups](#)
- [Backup menu options](#)
- [About testing or editing credentials for jobs](#)
- [Viewing or editing credentials for a computer or a computer's contents](#)
- [About selecting data to back up](#)
- [About including or excluding files for backup jobs](#)
- [About stages](#)
- [About backup job settings](#)
- [About backup sets](#)

- [About duplicating backed up data](#)
- [About test run jobs](#)
- [About verifying backed up data](#)
- [How to copy data directly from a virtual tape library to a physical tape device](#)
- [Copying data from a virtual tape library to a physical tape device](#)
- [Viewing all scheduled backup jobs on a calendar](#)
- [Excluding dates from the schedule using the backup calendar](#)

## About preparing for your first backup

Before you back up data, you should develop a backup strategy that includes the backup method, frequency, and data retention methods that are appropriate for your organization. You may have different strategies for different areas of the organization.

See [“About backup strategies”](#) on page 526.

You should also ensure that you have the proper user rights to run back up jobs.

See [“Required user rights for backup jobs”](#) on page 157.

You must configure storage before creating backup jobs. You can set up Backup Exec to use specific storage devices or logical groupings of devices, such as storage pools.

See [“About the Configure Storage wizard”](#) on page 145.

Specifically, you might want to perform the following tasks to help you manage storage hardware and media most effectively:

- Create disk storage so that Backup Exec can automatically manage backup data retention.  
See [“About disk-based storage”](#) on page 305.
- Set up storage device pools to load-balance jobs.  
See [“About storage device pools”](#) on page 403.
- Create media sets to manage data retention for tape or disk cartridge media.  
See [“About media sets”](#) on page 366.
- Configure deduplication disk storage to optimize storage and network bandwidth.  
See [“About the Deduplication Option”](#) on page 752.
- Configure vault stores for the Archiving Option.

See [“About vault stores in the Archiving Option”](#) on page 1235.

## About backing up data

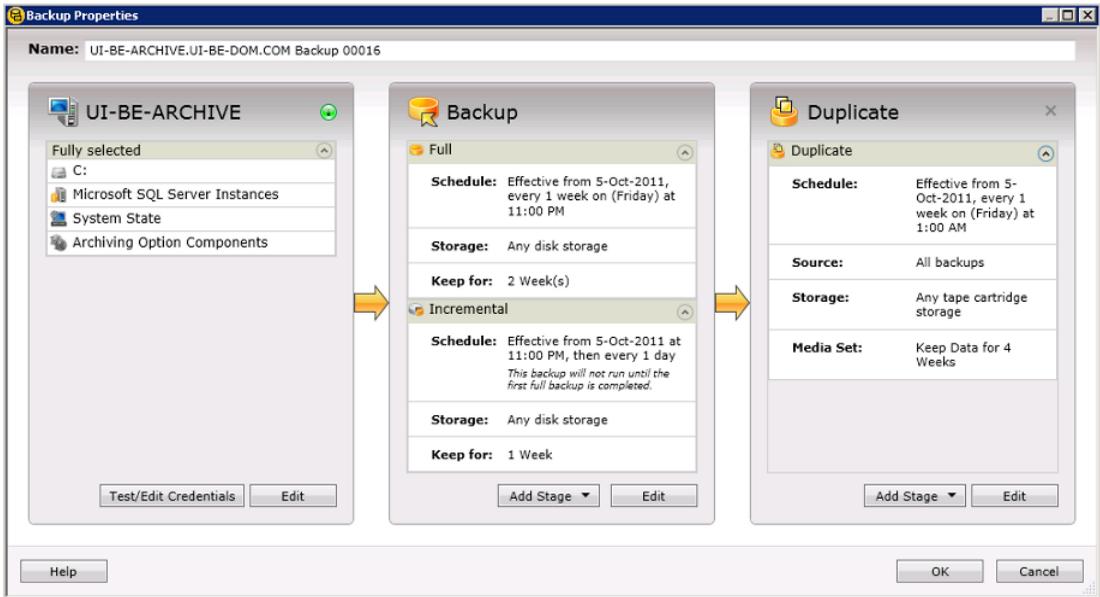
When you want to back up data, you create a container that is called the backup definition.

Backup definitions contain backup selections, backup jobs, and stages.

**Table 5-1** Backup definition contents

Item	Description
Backup selections	Backup selections include any servers, volumes, or data that you have selected to back up.  See <a href="#">“About selecting data to back up”</a> on page 177.
Backup job or jobs and settings	Backup definitions always contain one backup job that uses the full backup method, but recurring jobs can also contain additional incremental or differential backup jobs. Backup job settings can include encryption, scheduling options, or notifications, for example.  See <a href="#">“About backup methods”</a> on page 528. See <a href="#">“About backup job settings”</a> on page 185.
Stages	Stages are optional tasks that you can run with backup jobs. Backup definitions can contain one or more stages. You can create stages that duplicate your backup data, create virtual machines with your backup data, or archive your backup data.  See <a href="#">“About stages”</a> on page 183.

**Figure 5-1** Backup Definition (with backup selections, full and incremental backup jobs, and a duplicate stage)



Backup Exec offers you many choices for creating backup jobs to protect your data, including the following:

- Back up the full or partial contents of a single server  
See [“Backing up data”](#) on page 163.
- Back up multiple servers at one time  
See [“Backing up data”](#) on page 163.
- Schedule recurring backup jobs  
See [“Backing up data”](#) on page 163.
- Create a backup job to run only once  
See [“Creating a one-time backup”](#) on page 164.
- Create a new backup definition using an existing backup definition's settings  
See [“Creating a new backup from an existing backup”](#) on page 165.
- Edit existing backup definitions to modify their schedules, backup selections, or other settings  
See [“Editing backups”](#) on page 170.
- Create a server group out of similar computers and back up the entire group at once.

See [“Backing up server groups”](#) on page 168.

To protect remote computers, you must install the Agent for Windows on the remote computer. The Agent for Windows is a system service that runs on Windows servers and workstations. It provides efficient backup processing by locally performing the tasks that, in typical backup technologies, require extensive network interaction.

See [“About installing the Agent for Windows”](#) on page 83.

## Required user rights for backup jobs

To perform any backup operations, the following Windows user rights are required for the service account and any Backup Exec logon accounts:

- Act as part of the operating system.
- Create a token object.
- Back up files and directories.
- Restore files and directories.
- Manage auditing and security log.
- Logon as a batch job (only for Windows Vista and later).

For more information about user rights in Windows operating systems, see your Microsoft documentation.

See [“About the Backup Exec service account”](#) on page 512.

See [“About logon accounts”](#) on page 498.

## About the list of servers

You can view a list of servers on the **Backup and Restore** tab. The servers that display in the list include any servers that you manually add to Backup Exec and any servers that Backup Exec discovers during a catalog operation. Servers must be added to the list so that you can select them for backup jobs.

Windows servers must have the Agent for Windows installed on them before you can add them to the list of servers. When you add Windows servers to Backup Exec, you have the option to install the Agent for Windows to them remotely.

See [“Adding servers to the list of servers”](#) on page 158.

You can also monitor server activity and job status from the list of servers. By default, Backup Exec displays a server's alerts, backup status, and a calendar of the last seven days of backup jobs. It also displays the date and time of the previous

and upcoming scheduled backups. You can customize the columns on this list to display additional information.

You can select to view any of the following details about each server in the list:

- Server
- Active alerts
- Status
- Last seven days of backup jobs
- Last backup
- Next backup
- Server type
- Version of the server
- Backup Exec version
- Data source types
- Backup selections
- Percent complete
- Elapsed time
- Byte count
- Average job rate

If you no longer want to monitor or back up a server with Backup Exec, you can delete it from the list of servers.

See [“Removing servers from the list of servers”](#) on page 159.

## Adding servers to the list of servers

Before you can create a backup definition, you must add the servers that you want to protect to the list of servers.

See [“About the list of servers”](#) on page 157.

### To add servers to the list of servers

- 1 Click the **Backup and Restore** tab, in the **Servers** group, click **Add**.
- 2 Complete the steps to add a server or servers to the list of servers.

---

**Note:** If Backup Exec discovered servers using the **Discover Data to Back Up** option, they display on the **Browse** dialog box under the heading **Servers without an Agent for Windows installed**.

See [“About discovering data to back up”](#) on page 537.

---

## Removing servers from the list of servers

If you no longer want to monitor or back up a server with Backup Exec, you can remove it from the list of servers.

See [“About the list of servers”](#) on page 157.

---

**Note:** If you remove a server from the list and it has scheduled jobs pending, the jobs are deleted. The jobs do not run as scheduled. Do not remove a server from the list of jobs if you still want to back up that server.

---

### To remove servers from the list of servers

- 1 On the **Backup and Restore** tab, right-click the server that you want to remove from the list of servers.
- 2 Click **Remove**.
- 3 Click **Yes** to confirm that you want to remove the server from the list of servers.

## About server groups

Server groups are a way to organize and view server information in the list of servers. You can create server groups based on any criteria. You may want to group servers with a specific type of data or servers that reside in a specific location. Then, when you view server groups, only the server group that you select displays in the list of servers. Viewing server groups lets you quickly monitor the status of all of the servers in the group at a glance. You can also back up an entire server group.

You can double-click a server group to view more detailed information about the server group's jobs, job history, and any active alerts.

Backup Exec comes with one preconfigured server group that is called All Servers. The All Servers server group contains all of the servers in the list of servers for a Backup Exec server. You cannot delete or edit the All Servers server group.

See [“Viewing server groups”](#) on page 160.

See [“Creating a server group”](#) on page 160.

See [“Editing a server group”](#) on page 161.

See [“Deleting a server group”](#) on page 162.

See [“Backing up server groups”](#) on page 168.

## Viewing server groups

You can create server groups to organize and view server information in the list of servers. To view server groups, you must enable the **Groups** pane.

See [“About server groups”](#) on page 159.

### To view server groups

- 1 On the **Backup and Restore** tab, in the **Views** group, click **Groups**.
- 2 Select **Enable**.

The **Enable** option lets you hide or show the **Groups** pane to the left of the list of servers.

## Creating a server group

Server groups let you organize and view server information in the list of servers. You select the servers that you want to add to a server group. You may want to group servers with a specific type of data or servers that reside in a specific location, for example.

See [“About server groups”](#) on page 159.

### To create a server group

- 1 On the **Backup and Restore** tab, in the **Views** group, click **Groups**.
- 2 Select **Add**.
- 3 Complete the necessary options.  
See [“Server Group options”](#) on page 161.
- 4 Click **OK**.

## Editing a server group

Server groups let you organize and view server information in the list of servers. Existing server groups can be edited.

See [“About server groups”](#) on page 159.

You can do the following:

- Add servers to the server group.
- Remove servers from the server group.
- Change the name of the server group.
- Change the server group's description.

You must enable the **Groups** pane to view and edit server groups.

See [“Viewing server groups”](#) on page 160.

### To edit a server group

- 1 On the **Backup and Restore** tab, in the **Groups** pane, right-click the group that you want to edit.
- 2 Select **Edit**.
- 3 Complete the necessary options.  
See [“Server Group options”](#) on page 161.
- 4 Click **OK**.

## Server Group options

You can create server groups to organize and view server information in the list of servers. Existing server groups can be edited.

You can do the following:

- Add servers to the server group.
- Remove servers from the server group.
- Change the name of the server group.
- Change the server group's description.

See [“Creating a server group”](#) on page 160.

See [“Editing a server group”](#) on page 161.

**Table 5-2** Server Group options

Item	Description
<b>Group name</b>	Indicates the name of the server group.  The name of the server group displays on the <b>Groups</b> pane. You should choose a unique name to help identify the server group later.
<b>Description</b>	Provides a unique description of the server group.  The description that you enter in this field displays with the name of the server group on the <b>Groups</b> pane. You may want to enter a unique description in this field to help you identify the server group later. The description is optional.
<b>Name contains</b>	Lets you enter part or all of a server name to filter the selection results.
<b>Server type</b>	Lets you select a type of server to filter the selection results.
<b>Data sources</b>	Lets you select the servers' data sources to filter the selection results.  Data sources include specific types of application data and files and folders.
<b>Name</b>	Displays the name of the servers that you can add to the server group.
<b>Server Type</b>	Displays the type of server.
<b>Version</b>	Displays the operating system for each server.

## Deleting a server group

Server groups let you view only specific servers in the list of servers. If you no longer want to use a server group, you can delete it. Deleting a server group does not delete the servers from Backup Exec. You can still back up and monitor servers after you delete the server group to which they belong.

See [“About server groups”](#) on page 159.

You must enable the **Groups** pane to view and delete server groups.

See [“Viewing server groups”](#) on page 160.

**To delete a server group**

- 1 On the **Backup and Restore** tab, in the **Groups** pane, right-click the group that you want to delete.
- 2 Select **Delete**.
- 3 Confirm that you want to delete the server group.

## Backing up data

You can create a backup definition by selecting data and setting the properties that you want.

See [“About backing up data”](#) on page 155.

Before you create a backup definition, you must configure storage and add servers to the list of servers.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About the list of servers”](#) on page 157.

**To back up data**

- 1 On the **Backup and Restore** tab, do one of the following:
  - To back up a single server, right-click the server name.
  - To back up multiple servers, Shift + click or Ctrl + click the server names, and then right-click one of the selected servers.
- 2 On the **Backup** menu, select the backup option that you want to use.  
See [“Backup menu options”](#) on page 171.
- 3 In the **Name** field, type a unique name for the backup definition.

---

**Note:** If you back up data from multiple servers, Backup Exec appends the server name to the text you enter in the **Name** field. Backup Exec uses the server name and the text you entered to create unique names for each backup definition.

---

4 Do any of the following:

- |   |  |
|---|--|
| To test or edit the credentials that Backup Exec uses to access backup selections | In the <b>Selections</b> box, click <b>Test/Edit Credentials</b> .<br><br>See <a href="#">“About testing or editing credentials for jobs”</a> on page 175. |
| To change the backup selections   | In the <b>Selections</b> box, click <b>Edit</b> .<br><br>See <a href="#">“About selecting data to back up ”</a> on page 177.                               |
| To add a stage to the backup definition   | In the <b>Backup</b> box, click <b>Add Stage</b> .<br><br>See <a href="#">“About stages”</a> on page 183.  |
| To modify the job settings  | In the <b>Backup</b> box, click <b>Edit</b> .<br><br>See <a href="#">“About backup job settings”</a> on page 185.  |

5 When you are finished configuring the backup definition, click **OK** on the **Backup Properties** dialog box.

## Creating a one-time backup

A one-time backup is a job that only runs once without any recurring instances. You may want to create a one-time backup to create a baseline for a server before you upgrade it or install new software. After Backup Exec finishes running a one-time backup, it deletes the job rather than saving it with your recurring jobs. If you want to view information about a one-time backup after the job is complete, you can still view its job history.

See [“About backing up data”](#) on page 155.

See [“About the Job History”](#) on page 260.

One-time backup jobs do not affect any jobs that you have scheduled.

---

**Note:** You cannot add a stage to a one-time backup.

---

Before you create a backup definition, you must configure storage and add servers to the list of servers.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About the list of servers”](#) on page 157.

### To create a one-time backup

- 1 On the **Backup and Restore** tab, do one of the following:
  - To back up a single server, select the server name.
  - To back up multiple servers, Shift + click or Ctrl + click the server names.
- 2 In the **Backups** group, click **One-Time Backup**.
- 3 Select the one-time backup method that you want to use.
- 4 In the **Name** field, type a unique name for the backup definition.

---

**Note:** If you back up data from multiple servers, Backup Exec appends the server name to the text you enter in the **Name** field. Backup Exec uses the server name and the text you entered to create unique names for each backup definition.

---

- 5 Do any of the following:

To test or edit the credentials that Backup Exec uses to access backup selections

In the **Selections** box, click **Test/Edit Credentials**.

See “[About testing or editing credentials for jobs](#)” on page 175.

To change the backup selections

In the **Selections** box, click **Edit**.

See “[About selecting data to back up](#)” on page 177.

To modify the job settings

In the **Backup** box, click **Edit**.

See “[About backup job settings](#)” on page 185.

- 6 When you are finished configuring the backup definition, click **OK** on the **Backup Properties** dialog box.

## Creating a new backup from an existing backup

If you want to create a backup definition that is similar to an existing backup definition, you can apply the existing definition's settings to a new definition. Any backup methods, job settings, and stages are copied into a new backup definition for the server or servers that you selected to back up. All that you have

to do is select the backup selections. You can override any of the job settings, if necessary.

See [“About backing up data”](#) on page 155.

#### To create a new backup from an existing backup

- 1 On the **Backup and Restore** tab, do one of the following:
  - To back up a single server, right-click the server name.
  - To back up multiple servers, Shift + click or Ctrl + click the server names, and then right-click one of the selected servers.
- 2 On the **Backup** menu, select **Create a New Backup Using the Settings from an Existing Backup**.
- 3 Select the existing backup definition that contains the settings that you want to apply to the new definition, and then click **OK**.  
See [“Backup Job Selection options”](#) on page 167.
- 4 In the **Name** field, type a unique name for the new backup definition.

---

**Note:** If you back up data from multiple servers, Backup Exec appends the server name to the text you enter in the **Name** field. Backup Exec uses the server name and the text you entered to create unique names for each backup definition.

---

**5** Do any of the following:

- |   |  |
|---|--|
| To test or edit the credentials that Backup Exec uses to access backup selections | In the <b>Selections</b> box, click <b>Test/Edit Credentials</b> .<br><br>See <a href="#">“About testing or editing credentials for jobs”</a> on page 175. |
| To change the backup selections   | In the <b>Selections</b> box, click <b>Edit</b> .<br><br>See <a href="#">“About selecting data to back up ”</a> on page 177.                               |
| To add a stage to the backup definition   | In the <b>Backup</b> box, click <b>Add Stage</b> .<br><br>See <a href="#">“About stages”</a> on page 183.  |
| To modify the job settings  | In the <b>Backup</b> box, click <b>Edit</b> .<br><br>See <a href="#">“About backup job settings”</a> on page 185.  |

**6** When you are finished configuring the backup definition, click **OK** on the **Backup Properties** dialog box.

## Backup Job Selection options

You can select a backup definition to edit it or you can copy its settings to create a new backup definition.

See [“Editing backups”](#) on page 170.

See [“Creating a new backup from an existing backup”](#) on page 165.

**Table 5-3 Backup Job Selection options**

Item	Description
<b>Name contains</b>	Lets you enter part or all of a backup definition's name to filter the selection results.
<b>Name</b>	Displays the names of the backup definitions for the server that you selected.
<b>Server</b>	Displays the name of the server that was backed up.
<b>Selections</b>	Displays the data that was selected to be backed up.

## Backing up server groups

Creating server groups can help you to manage and monitor the servers on your network. You can also back up entire server groups at once.

See [“About server groups”](#) on page 159.

See [“About backing up data”](#) on page 155.

Before you create a backup definition, you must configure storage and add servers to the list of servers.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About the list of servers”](#) on page 157.

### To back up server groups

- 1 On the **Backup and Restore** tab, in the **Views** group, click **Groups**.
- 2 Click **Enable**.
- 3 In the **Groups** pane, right-click the server group that you want to back up.
- 4 On the **Backup** menu, select the backup option that you want to use.  
See [“Backup menu options”](#) on page 171.
- 5 In the **Name** field, type a unique name for the backup definition.

---

**Note:** When you back up data from multiple servers, Backup Exec appends the server name to the text you enter in the **Name** field. Backup Exec uses the server name and the text you entered to create unique names for each backup definition.

---

## 6 Do any of the following:

To test or edit the credentials that Backup Exec uses to access backup selections	In the <b>Selections</b> box, click <b>Test/Edit Credentials</b> . See <a href="#">“About testing or editing credentials for jobs”</a> on page 175.
To change the backup selections	In the <b>Selections</b> box, click <b>Edit</b> . See <a href="#">“About selecting data to back up”</a> on page 177.
To add a stage to the backup definition	In the <b>Backup</b> box, click <b>Add Stage</b> . See <a href="#">“About stages”</a> on page 183.
To modify the job settings	In the <b>Backup</b> box, click <b>Edit</b> . See <a href="#">“About backup job settings”</a> on page 185.

## 7 When you are finished configuring the backup definition, click **OK** on the **Backup Properties** dialog box.

# Running the next scheduled backup job

You can run the next scheduled backup job in a backup definition at any time. You may want to run a scheduled backup job early to ensure that important data gets backed up or to make sure that a scheduled job completes successfully. Running a scheduled backup job early does not affect its regular schedule. The job still runs normally as scheduled.

See [“About backing up data”](#) on page 155.

### To run the next scheduled backup job

- 1 On the **Backup and Restore** tab, do one of the following:
  - To run the next scheduled backup for a single server's backup jobs, right-click the server name.
  - To run the next scheduled backup for multiple servers' backup jobs, Shift + click or Ctrl + click the server names, and then right-click one of the selected servers.
- 2 Click **Run Next Backup Now**.
- 3 Click **Yes** to confirm that you want to run the job or jobs now.

# Editing backups

You can edit existing backup definitions.

See [“About backing up data”](#) on page 155.

---

**Note:** You cannot edit a backup definition while one of its backup jobs is running.

---

## To edit a backup

- 1 On the **Backup and Restore** tab, do one of the following:
  - To edit backups for a single server, right-click the server name.
  - To edit backups for multiple servers, Shift + click or Ctrl + click the server names, and then right-click one of the selected servers.
- 2 Click **Edit Backups**.
- 3 If the server or servers that you selected have multiple backup definitions, select the definitions that you want to edit on the **Backup Job Selection** dialog box. Then click **OK**.

See [“Backup Job Selection options”](#) on page 167.

#### 4 Do any of the following:

To test or edit the credentials that Backup Exec uses to access backup selections	In the <b>Selections</b> box, click <b>Test/Edit Credentials</b> .  See <a href="#">“About testing or editing credentials for jobs”</a> on page 175.
To change the backup selections	In the <b>Selections</b> box, click <b>Edit</b> .  See <a href="#">“About selecting data to back up ”</a> on page 177.
To add a stage to the backup definition	In the <b>Backup</b> box, click <b>Add Stage</b> .  See <a href="#">“About stages”</a> on page 183.
To modify the job settings	In the <b>Backup</b> box, click <b>Edit</b> .  See <a href="#">“About backup job settings”</a> on page 185.

---

**Note:** If you choose to edit more than one backup definition at once, you can edit only the properties that the definitions have in common. For example, if you choose to edit two backup definitions at once and the definitions use different backup selections, you cannot edit the selections. If you do not see the settings that you want to edit, repeat this procedure, but select only one definition to edit at a time.

---

- 5 When you are finished editing the backup definition, click **OK** on the **Backup Properties** dialog box.

## Backup menu options

When you create a backup definition, you must choose the type of storage to which you want to send the backup sets.

See [“About the Configure Storage wizard”](#) on page 145.

You can also choose a stage, which is an additional operation or step in addition to the backup job itself.

See [“About stages”](#) on page 183.

Backup Exec comes with preconfigured backup menu options that combine different types of storage with stages. When you create a backup definition, you begin by selecting one of these backup menu options. You can add additional stages to the backup menu option to further customize the definition.

---

**Note:** Backup menu options appear only if your system is configured to support them. For example, if you do not have a tape storage device, the Back Up to Tape option does not appear in the list of backup menu options.

---

You can select from the following backup menu options:

**Table 5-4** Backup menu options

Backup menu option	Description
<b>Back Up to Deduplication Disk Storage</b>	Sends the backup data to a deduplication storage device.  See <a href="#">“About deduplication disk storage”</a> on page 760.
<b>Back Up to Deduplication Disk Storage and then Duplicate to Deduplication Disk Storage</b>	Sends the backup data to a deduplication storage device and then creates a duplicate copy of the backup sets for a deduplication storage device.  See <a href="#">“About deduplication disk storage”</a> on page 760.  See <a href="#">“About duplicating backed up data”</a> on page 218.
<b>Back Up to Deduplication Disk Storage and then Duplicate to Tape</b>	Sends the backup data to a deduplication storage device and then creates a duplicate copy of the backup sets for tape storage.  See <a href="#">“About deduplication disk storage”</a> on page 760.  See <a href="#">“About duplicating backed up data”</a> on page 218.
<b>Back Up to Deduplication Disk Storage and then Convert to Virtual Machine</b>	Sends the backup data to a deduplication storage device and then converts a duplicate copy of the backup sets into a virtual machine.  See <a href="#">“About deduplication disk storage”</a> on page 760.  See <a href="#">“About conversion to virtual machines”</a> on page 437.

**Table 5-4** Backup menu options (*continued*)

Backup menu option	Description
<b>Back Up to Deduplication Disk Storage and Simultaneously Convert to Virtual Machine</b>	<p>Sends the backup data to a deduplication storage device while simultaneously converting a duplicate copy of the backup sets into a virtual machine.</p> <p>See <a href="#">“About deduplication disk storage”</a> on page 760.</p> <p>See <a href="#">“About conversion to virtual machines”</a> on page 437.</p>
<b>Back Up to Deduplication Disk Storage and then Archive</b>	<p>Sends the backup data to a deduplication storage device and then creates a duplicate copy of the backup sets for archive storage.</p> <p>See <a href="#">“About deduplication disk storage”</a> on page 760.</p> <p>See <a href="#">“About the Archiving Option”</a> on page 1198.</p>
<b>Back Up to Disk</b>	<p>Sends the backup data to a disk storage device.</p> <p>See <a href="#">“About disk-based storage”</a> on page 305.</p>
<b>Back Up to Disk and then Duplicate to Tape</b>	<p>Sends the backup data to disk and then creates a duplicate copy of the backup sets for tape storage.</p> <p>See <a href="#">“About disk-based storage”</a> on page 305.</p> <p>See <a href="#">“About duplicating backed up data”</a> on page 218.</p>
<b>Back Up to Disk and then Convert to Virtual Machine</b>	<p>Sends the backup data to a disk storage device and then converts a duplicate copy of the backup sets into a virtual machine.</p> <p>See <a href="#">“About conversion to virtual machines”</a> on page 437.</p>
<b>Back Up to Disk and Simultaneously Convert to Virtual Machine</b>	<p>Sends the backup data to a disk storage device while simultaneously converting a duplicate copy of the backup sets into a virtual machine.</p> <p>See <a href="#">“About conversion to virtual machines”</a> on page 437.</p>

**Table 5-4** Backup menu options (*continued*)

Backup menu option	Description
<b>Back Up to Disk and then Archive</b>	<p>Sends the backup data to disk and then creates a duplicate copy of the backup sets for archive storage.</p> <p>See “<a href="#">About disk-based storage</a>” on page 305.</p> <p>See “<a href="#">About the Archiving Option</a>” on page 1198.</p>
<b>Back Up to Tape</b>	<p>Sends the backup data to tape storage.</p> <p>See “<a href="#">About tape drives and robotic libraries</a>” on page 334.</p>
<b>Back Up to Tape and then Archive</b>	<p>Sends the backup data to tape and then creates a duplicate copy of the backup sets for archive storage.</p> <p>See “<a href="#">About tape drives and robotic libraries</a>” on page 334.</p> <p>See “<a href="#">About the Archiving Option</a>” on page 1198.</p>
<b>Create a Synthetic Backup</b>	<p>Creates a synthetic backup by combining the data from a full backup and any subsequent incremental backups.</p> <p>See “<a href="#">About the synthetic backup feature</a>” on page 1048.</p>
<b>Back Up to Disk and then Duplicate to Cloud</b>	<p>Sends the backup data to disk and then creates a duplicate copy of the backup sets for cloud storage.</p> <p>See “<a href="#">About disk-based storage</a>” on page 305.</p> <p>See “<a href="#">About duplicating backed up data</a>” on page 218.</p>
<b>Create a New Backup Using the Settings from an Existing Backup</b>	<p>Lets you select an existing backup definition and apply its settings to a new backup definition.</p> <p>See “<a href="#">Creating a new backup from an existing backup</a>” on page 165.</p>

## About testing or editing credentials for jobs

You should test to make sure that you have the appropriate credentials to access the content that you want to back up. If Backup Exec does not have the correct credentials to access content, the backup job fails. You can test the credentials when you create a backup definition. If you need to change credentials for a computer or a computer's contents, you can do so from the **Test/edit credentials** dialog box when you create or edit backups.

---

**Note:** You cannot test credentials for virtual machines, but the job runs if you provide the correct credentials. If the job fails, you may need to retry the job with different credentials.

---

See [“About backing up data”](#) on page 155.

See [“Test/edit credentials options”](#) on page 175.

You can also change the credentials for a computer or a computer's contents on the **Backup and Restore** tab from the **Credentials** pane.

See [“Viewing or editing credentials for a computer or a computer's contents”](#) on page 176.

See [“Credentials properties”](#) on page 176.

### Test/edit credentials options

You can test or edit the credentials for a computer or content before you run a job.

See [“About testing or editing credentials for jobs”](#) on page 175.

**Table 5-5** Test/edit credentials options

Item	Description
<b>Name</b>	Lists the name of each computer or piece of content that the backup job contains.
<b>Logon Account</b>	Lists the logon account that Backup Exec uses to access the computer or content.  If the credential test fails, or if you want to change the account for a computer or content, select a new logon account. The <b>&lt;new logon account&gt;</b> option enables you to enter a new logon account.  See <a href="#">“Add Logon Credentials options”</a> on page 508.

**Table 5-5** Test/edit credentials options (*continued*)

Item	Description
<b>Credential Status</b>	Indicates whether the credentials were able to successfully access the computer or content.
<b>Date Last Attempted</b>	Indicates the last time a credentials test was run.
<b>Test All</b>	Tests all credentials to ensure that they can access the computers or content in the backup job.
<b>Test Selected</b>	Tests only the selected credentials to ensure that they can access the computer or content.
<b>Cancel Test</b>	Cancels the test when it is running.

## Viewing or editing credentials for a computer or a computer's contents

You can view or edit the credentials for any computer or any computer's contents that you protect with Backup Exec. If Backup Exec does not have the correct credentials to access a piece of content, your jobs fail. You can test the credentials when you create a backup definition.

See [“About testing or editing credentials for jobs”](#) on page 175.

You may need to change the credentials for a piece of content so that Backup Exec can access it. If a credentials test fails or if the credentials for a piece of content change, you can enter new credentials for the content.

### Viewing or editing credentials for a computer or a computer's contents

- 1 On the **Backup and Restore** tab, double-click the server whose properties you want to view.
- 2 In the left pane, click **Credentials**.
- 3 View or edit the information that displays.

See [“Credentials properties”](#) on page 176.

## Credentials properties

You can view or edit the credentials for a computer or a computer's content.

See [“Viewing or editing credentials for a computer or a computer's contents”](#) on page 176.

Table 5-6 Credentials properties

Item	Description
<b>Backup Source</b>	Lists the name of the computer and the content on the computer.
<b>Backup Selection</b>	Indicates whether backup selections for this computer were full, partial, or none.
<b>Backup Status</b>	Lists the current backup status of each piece of content.
<b>Logon Account</b>	<p>Lists the logon account that Backup Exec uses to access the computer or content.</p> <p>If a credentials test fails, or if you want to change the account for a computer or content, select a new logon account. The <b>&lt;new logon account&gt;</b> option enables you to enter a new logon account.</p> <p>See <a href="#">“Add Logon Credentials options”</a> on page 508.</p>
<b>Credential Status</b>	Indicates whether the credentials were able to successfully access the computer or content. If you have not tested the credentials, Backup Exec displays <b>Unknown, Test</b> .
<b>Date Last Attempted</b>	Indicates the last time a credentials test was run.

## About selecting data to back up

When you back up a server, Backup Exec includes all of the data on the server in the backup selections by default. If you want to modify the backup selections, you can do so from the **Selections** box on the **Backup Job Properties** dialog box.

See [“Backing up data”](#) on page 163.

Instead of backing up all of the data on a server, you can select drives, folders, files, System State, network shares, or databases on the **Browse** tab.

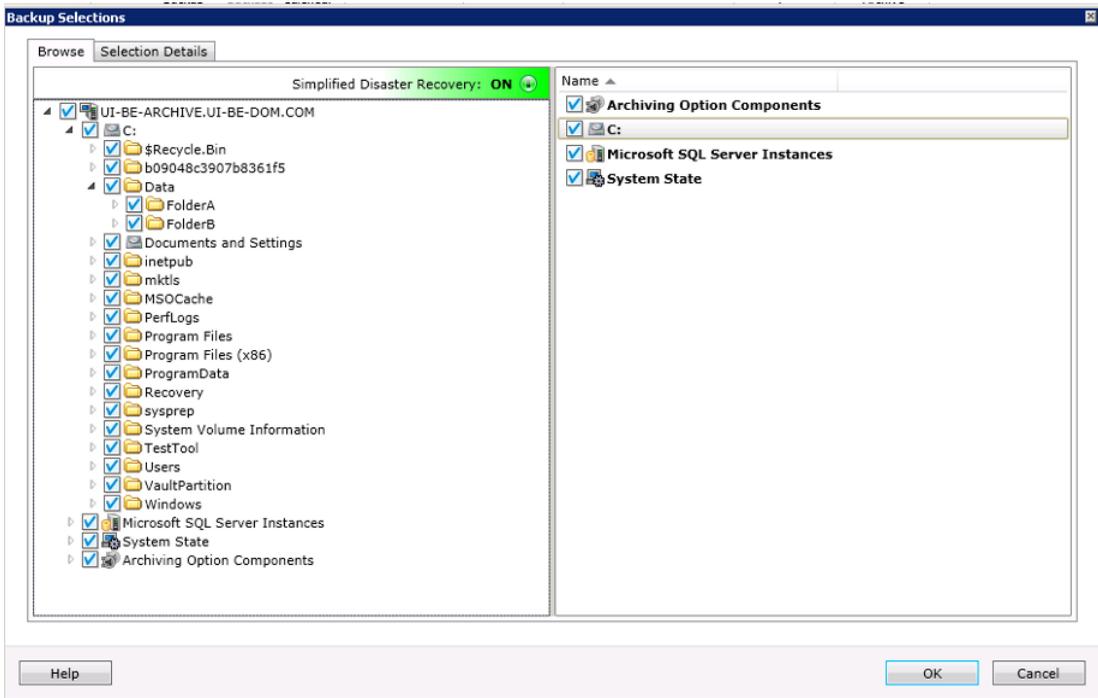
To expand or collapse the view for an item, click the arrow next to it or double-click the item's name. To view the contents of an item, double-click the item's icon. The item's contents appear in the right frame of the backup selections view. You can traverse file levels from either side of the window by clicking folders and subfolders as they appear.

The scheduling options selected for this job do not allow it to start later than \$. It will be considered missed and rescheduled. Check the scheduling options to ensure that they allow enough time for the job to finish running.

When you browse remote selections, Backup Exec requires a valid logon account to expand the computer contents. If the default logon account does not enable access to a remote selection, Backup Exec prompts you to select another existing logon account. You can also create a new logon account that can access the selection.

To include data in the backup, select the check box next to the drive or directory that you want to back up.

**Figure 5-2** Selecting data for a single server



You also can include or exclude specific files or specific types of files using the **Selection Details** tab.

See [“About including or excluding files for backup jobs”](#) on page 180.

If you select to back up data from more than one server, the selections are combined in one dialog box. Similar types of content are grouped together. You can edit the backup selections, but the backup selections apply to each server that you back up. For example, if you select to back up two servers, you can either select or deselect System State for both. But you cannot choose to back up System State for one server and not the other. You cannot select individual files and folders if you choose to back up multiple servers at once. Selecting multiple servers

is a good way to back up servers in their entirety. If you want to back up more granular selections for each server, you should select them separately and create new backup jobs.

Figure 5-3 Selecting data for multiple servers



When all the critical system components are included in your backup job selections, the **Simplified Disaster Recovery** indicator on the selections pane reads **ON**. If

you deselect one or more critical system component files, the indicator changes to **OFF**.

See [“About backing up critical system components”](#) on page 539.

If you deselect any critical system components, it can disqualify your backup data from being used in certain types of restore scenarios.

You must include all critical system components in your backup selections if you intend to use any of the following restore scenarios:

- Simplified Disaster Recovery
- Physical to virtual
- Backup set to virtual
- Online disaster recovery

## About including or excluding files for backup jobs

If you want to modify a backup definition's backup selections, you can do so from the **Selections** box on the **Backup Job Properties** dialog box. The **Selection Details** tab lets you quickly include or exclude files for backups by specifying file attributes. Exclusions can be added to incremental and differential backup jobs, but not full backup jobs.

You can do any of the following:

- Include or exclude subdirectories. For example, you can choose to back up a parent folder without backing up any folders that reside inside it.
- Include only modified files. For example, you can choose to back up only the files that have changed since the last backup job.
- Include only read-only files.
- Include or exclude files by file name attributes. For example, you can select only files with .txt extensions, or exclude files with .exe extensions from a backup. If you exclude files by an attribute that does not exist, all files of that type are excluded. For example, excludes based on SQL database dates result in global SQL excludes since SQL databases do not have date attributes.
- Select only any files that fall within a specified date range. For example, you can select any files that were created or modified during the month of December.
- Specify the files that have not been accessed in a specified number of days. For example, you can select the files that have not been accessed in 30 days from your "My Documents" folder. Then, run a full backup job for which you select the method to back up and delete the files.

The Backup Exec Archive Option offers more features for data archiving. See [“About the Archiving Option”](#) on page 1198.

You can also configure global exclusions. Global exclusions apply to all the backup jobs that you create.

See [“Excluding selections from all backups”](#) on page 462.

## Include/Exclude options

Advanced file selection lets you quickly include or exclude files for backups by specifying file attributes.

See [“About including or excluding files for backup jobs”](#) on page 180.

**Table 5-7** Include/Exclude options

Item	Description
<b>Include</b>	Lets you include all files that match the criteria that you specify.
<b>Exclude</b>	Lets you exclude all files that match the criteria that you specify.
<b>Resource name</b>	Lets you include or exclude files from a backup of a different drive than the one you selected previously from the backup selections.

**Table 5-7** Include/Exclude options (*continued*)

Item	Description
<b>Path</b>	<p>Specifies the name of the folder and/or subfolder that contains any specific file that you want to include or exclude.</p> <p>You can use wildcard characters. Use a question mark (?) to represent any single character. Use two asterisks (**) to represent any number of characters.</p> <p>For example, on your C: drive you have a My Documents folder that contains a subfolder called Work Files. There are three Work Files subfolders that are called 2010, 2011, 2012. Each one of these subfolders has a subfolder called Personnel.</p> <p>If you type the path as \My Documents\**\Personnel, the backup includes or excludes the following:</p> <ul style="list-style-type: none"> <li>■ C:\My Documents\Work Files\2010 Personnel</li> <li>■ C:\My Documents\Work Files\2011 Personnel</li> <li>■ C:\My Documents\Work Files\2012 Personnel</li> </ul> <p>In addition, every subfolder below the ** wildcard is included or excluded. However, the only files from the subfolders that are included or excluded are those that match the file name that you type in the <b>Name</b> field.</p> <p>So in the example above, every subfolder of C:\My Documents is included in or excluded from the backup. Only any files that match the name in the <b>Name</b> field would be included or excluded.</p>

Table 5-7 Include/Exclude options (*continued*)

Item	Description
<b>Name</b>	<p>Specifies the name of the file that you want to include in or exclude from the backup.</p> <p>You can use wildcard characters. Use a question mark (?) to represent any single character. Use two asterisks (**) to represent any number of characters.</p> <p>For example, to include all files with the .exe extension, type *.exe.</p>
<b>Apply to subdirectories</b>	<p>Includes the contents of all the subfolders when a directory is selected.</p>
<b>Only modified files</b>	<p>Includes or excludes modified files in the path that you specify.</p>
<b>Only read-only files</b>	<p>Includes or excludes the files that cannot be modified.</p>
<b>Files dated</b>	<p>Includes or excludes the files that were created or modified during a specific time period. Then select the beginning and ending dates.</p>
<b>Files not accessed in X days</b>	<p>Includes or excludes any files that have not been accessed in a specified number of days. This is useful when you need to migrate older files from your system.</p>

## About stages

Stages are the additional tasks that you can run with backup jobs as part of the backup definition. You may choose to add stages to the backup definition to customize it. You can add one or more stages for virtualization, duplication, and archiving when you create a backup definition. Stages can also be added to existing backup definitions.

See [“About backing up data”](#) on page 155.

For example, you may create a backup job that contains any important data that must be sent off-site. You can add a duplicate stage to the backup definition that contains that job. The duplicate stage automatically sends the backup data to tape storage when the backup job is complete. Then you can take the tape off-site to ensure that your data is safe.

See [“Backing up data”](#) on page 163.

See [“Editing a stage”](#) on page 184.

**Table 5-8** Types of stages

Stage	Description
Duplicate to Disk	Creates a duplicate copy of your backup and sends it to disk storage.  See <a href="#">“About duplicating backed up data”</a> on page 218.
Duplicate to Tape	Creates a duplicate copy of your backup and sends it to tape storage.  See <a href="#">“About duplicating backed up data”</a> on page 218.
Convert to Virtual Machine After Backup	Creates a virtual machine from your backup sets after the backup job is complete.  See <a href="#">“About conversion to virtual machines”</a> on page 437.
Convert to Virtual Machine Simultaneously with Backups	Creates a virtual machine from your backup sets while the backup job is running.  See <a href="#">“About conversion to virtual machines”</a> on page 437.
Archive	Creates an archive job to archive the selected file system shares and folders and Exchange mailboxes to a vault store.  See <a href="#">“About the Archiving Option”</a> on page 1198.

## Editing a stage

You can edit a stage that is part of a backup definition.

See [“About stages”](#) on page 183.

### To edit a stage

- 1 On the **Backup and Restore** tab, select the server that contains the backup definition that you want to edit.
- 2 In the **Backups** group, click **Edit Backups**.

- 3 If the server has more than one backup definition, select the definition that contains the stage that you want to edit, and then click **OK**.
- 4 Click **Edit** in the box that contains the stage that you want to edit.
- 5 Make any necessary changes.
- 6 When you are finished making changes to the stage, click **OK** on the **Backup Properties** dialog box.

## About backup job settings

Backup Exec is preconfigured with default options for backup jobs. If you want to override the default options for a specific backup job, you can modify them when you create the backup definition. When you create a new backup job, the job inherits the default settings that you configure.

See [“About job defaults”](#) on page 456.

See [“About backing up data”](#) on page 155.

---

**Note:** Some backup job settings appear in Backup Exec only if your network is configured to support them and you have the appropriate Symantec Backup Exec agent installed.

---

**Table 5-9** Backup job settings

Setting	Description
<b>Schedule</b>	<p>Lets you configure the time and the frequency with which you want to run the backup job or jobs.</p> <p>You can also add additional incremental, differential, and full backup jobs to the backup definition.</p> <p><b>Note:</b> You cannot add incremental and differential jobs to the same backup definition. You must delete the default incremental job before you can add a differential job.</p> <p>See <a href="#">“Schedule options”</a> on page 188.</p>

**Table 5-9** Backup job settings (*continued*)

Setting	Description
<p><b>Storage</b></p>	<p>Lets you specify the storage device that you want to use for a backup job.</p> <p>You can configure different storage devices for each backup job. For example, you may select disk storage for a full backup and a storage pool for an incremental backup in the same backup definition. You can also configure compression, encryption, and the length of time to keep the backup sets.</p> <p>See “<a href="#">Storage options</a>” on page 190.</p>
<p><b>Network</b></p>	<p>Lets you specify the network interface that Backup Exec uses to access remote computers.</p> <p>See “<a href="#">Network options</a>” on page 195.</p>
<p><b>Notification</b></p>	<p>Lets you configure Backup Exec to notify specified recipients when the backup job is completed.</p> <p>Each backup job and stage can be configured with different notification recipients. Backup Exec can notify people by email or text message.</p> <p>See “<a href="#">Notification options for jobs</a>” on page 299.</p>
<p><b>Test Run</b></p>	<p>Lets you configure a test job that tests storage capacity, credentials, and media integrity.</p> <p>The test job can help you determine if there are any problems that might keep the backup job from completing successfully.</p> <p>See “<a href="#">Test Run options</a>” on page 196.</p>
<p><b>Verify</b></p>	<p>Lets you create a job that verifies whether all of the data was successfully backed up when the job is completed.</p> <p>A verify job can also help you determine whether the media you use is defective.</p> <p>See “<a href="#">Verify options</a>” on page 197.</p>
<p><b>Advanced Open File</b></p>	<p>Lets you configure the snapshot settings that Backup Exec uses to process the backup job.</p> <p>You can also enable checkpoint restart, which lets you resume interrupted backup jobs.</p> <p>See “<a href="#">Advanced Open File options</a>” on page 199.</p>

Table 5-9 Backup job settings (continued)

Setting	Description
<b>Advanced Disk-based Backup</b>	Lets you configure off-host backup for the backup job. Off-host backup may provide you with better performance. See “ <a href="#">Advanced Disk-based Backup options</a> ” on page 1054.
<b>Security</b>	Lets you configure encryption settings for the backup job. Encrypting your backup sets can help protect sensitive data. See “ <a href="#">Security options</a> ” on page 201.
<b>Pre/Post Commands</b>	Lets you configure any commands that you want to run either before the backup job begins or after the backup job is completed. See “ <a href="#">Pre/post commands options</a> ” on page 202.
<b>Files and Folders</b>	Lets you configure how Backup Exec processes file system attributes such as junction points and symbolic links. See “ <a href="#">Files and Folders options</a> ” on page 204.
<b>Linux and Macintosh</b>	Lets you configure options for any Linux or Macintosh computers that are included in the backup job. See “ <a href="#">Linux backup options</a> ” on page 1091. See “ <a href="#">Default backup job options for Macintosh systems</a> ” on page 1126.
<b>Lotus Domino</b>	Lets you configure options for any Lotus Domino data that is included in the backup job. See “ <a href="#">Lotus Domino Agent backup options</a> ” on page 970.
<b>Microsoft Active Directory</b>	Lets you configure options for any Microsoft Active Directory data that is included in the backup job. See “ <a href="#">Microsoft Active Directory backup job options</a> ” on page 990.
<b>Microsoft Exchange</b>	Lets you configure options for any Microsoft Exchange data that is included in the backup job. See “ <a href="#">Microsoft Exchange backup options</a> ” on page 854.

**Table 5-9** Backup job settings (*continued*)

Setting	Description
<b>Virtual Machines</b>	Lets you configure options for any virtual machines that are included in the backup job.  See <a href="#">“Virtual machine backup options”</a> on page 785. See <a href="#">“Microsoft Hyper-V backup options”</a> on page 802.
<b>Microsoft SharePoint</b>	Lets you configure options for any Microsoft SharePoint data that is included in the backup job.  See <a href="#">“Microsoft SharePoint backup options”</a> on page 872.
<b>Microsoft SQL</b>	Lets you configure options for any Microsoft SQL data that is included in the backup job.  See <a href="#">“SQL backup options”</a> on page 817.
<b>NDMP</b>	Lets you configure options for any NDMP data that is included in the backup job.  See <a href="#">“Backup options for NDMP”</a> on page 1064.
<b>Oracle</b>	Lets you configure options for any Oracle data that is included in the backup job.  See <a href="#">“Oracle backup options ”</a> on page 903.
<b>Exclusions</b>	Lets you configure a certain file or types of files that you want Backup Exec to exclude from the backup job.  See <a href="#">“Exclusions options”</a> on page 209.

## Schedule options

The following table lists the options that you can select for scheduling jobs. You can configure default options for schedules, which all your backup jobs inherit when you create them. Or you can override the default schedule settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

---

**Note:** Some of these options may not display depending upon how you configure schedule options. For example, the global schedule options are different than the schedule options for a single backup job.

---

**Table 5-10**      Schedule options

Item	Description
<b>Schedule</b>	Specifies whether the job runs on a recurring pattern or if it runs immediately without any recurrences.
<b>Recurrence</b>	Lets you create a recurring schedule for the job.
<b>Recurrence Pattern</b>	Lets you configure the frequency with which the job recurs, if you choose to make the job recur on a schedule.  You can select to run the job in hourly, daily, weekly, monthly, or yearly increments.
<b>Starting on</b>	Designates the date on which the schedule takes effect.
<b>Calendar</b>	Lets you view all scheduled jobs on a calendar to check for scheduling conflicts.
<b>Keep the job scheduled for X hours before it is rescheduled</b>	Specifies the maximum amount of time past its scheduled start time at which Backup Exec considers the job to be missed and reschedules it.
<b>Cancel the job if it is running X hours after its scheduled start time</b>	Specifies the amount of time after the job's scheduled start time at which you want to cancel the job if it is still running.
<b>Run initial full backup now in addition to the selected schedule</b>	Runs the initial full backup as soon as the job is created without affecting the schedule of future jobs.
<b>Run now with no recurring schedule</b>	Runs the job immediately without scheduling any more instances of it for the future.
<b>Submit job on hold</b>	Lets you submit the job with an on-hold status.  You should select this option if you want to submit the job, but you do not want the job to run until a later date. The job runs later when you change the job's hold status.
<b>Add Backup Jobs By Method</b>	Lets you add additional full, incremental, or differential backups to the backup definition.  <b>Note:</b> You cannot add incremental and differential jobs to the same backup definition. You must delete the default incremental job before you can add a differential job.

## Storage options

The storage options let you select the storage and media set on which you want the backup job to run. You can configure different storage devices for each backup job. For example, you may select disk storage for a full backup and a storage pool for an incremental backup in the same backup definition. You can configure default options for storage, which your backup jobs inherit when you create them. Or you can override the default storage settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

---

**Note:** Some of these options display only in Central Admin Server Option (CASO) environments.

---

**Table 5-11** Storage options

Item	Description
<b>Backup Exec server or Backup Exec server pool</b>	<p>Specifies if you want a job to run on devices on a specific managed Backup Exec server or on devices that are on a group of managed Backup Exec servers.</p> <p>This option displays only if you have the Central Admin Server Option installed. This option is an additional filter that lets you control where certain jobs are delegated. For example, to always run backups of Exchange databases only on the devices that are attached to managed Backup Exec servers in a pool named Exchange Backups, select this option. Then select the Exchange Backups Backup Exec server pool.</p>
<b>Storage</b>	<p>Specifies the storage device to which you want to send backup data.</p> <p>See <a href="#">“About storage device pools”</a> on page 403.</p> <p>See <a href="#">“About the Any Virtual Disk Storage device pool in the Storage Provisioning Option”</a> on page 1171.</p> <p>See <a href="#">“About the Remote Media Agent for Linux”</a> on page 1132.</p> <p>See <a href="#">“About disk-based storage”</a> on page 305.</p>

Table 5-11 Storage options (continued)

Item	Description
<p><b>Enable the remote computer to directly access the storage device and to perform client-side deduplication, if it is supported</b></p>	<p>Enables a remote computer to send data directly to an OpenStorage device or a deduplication disk storage device, and to perform client-side deduplication if the device supports it. The Backup Exec server is bypassed, which leaves the Backup Exec server free to perform other operations. If client-side deduplication cannot be performed, then either Backup Exec server deduplication or Appliance deduplication is performed.</p> <p>This option appears if the Deduplication Option is installed and an OpenStorage device or a deduplication disk storage device is selected in the <b>Storage</b> field.</p> <p>See <a href="#">“About client-side deduplication”</a> on page 773.</p>
<p><b>Enable the remote computer to access the storage device through the Backup Exec server and to perform Backup Exec server-side deduplication, if it is supported</b></p>	<p>Enables a remote computer to send data through the Backup Exec server to an OpenStorage device or a deduplication disk storage device, and to perform Backup Exec server-side deduplication if it is supported. If the Backup Exec server does not support deduplication, the data is deduplicated on an intelligent disk device, such as Symantec PureDisk or a device from a third-party vendor.</p> <p>This option appears if the Deduplication Option is installed and an OpenStorage device or a deduplication disk storage device is selected in the <b>Storage</b> field.</p> <p>See <a href="#">“About the Deduplication Option”</a> on page 752.</p>
<p><b>Keep for</b></p>	<p>Designates the amount of time for which you want to keep the backup sets or job history.</p>
<p><b>Media set</b></p>	<p>Indicates the media set to use for the backup job. The media set specifies the overwrite protection period and the append period for the backup data on the media.</p> <p>If you want to create a new media set for this backup job, click the icon to the right of the media set drop-down menu.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“About media sets”</a> on page 366.</p>

**Table 5-11** Storage options (*continued*)

Item	Description
<p><b>Overwrite media</b></p>	<p>Indicates that the backup job is placed on an overwritable media. Ensure that appropriate media is in the storage device that you select.</p> <p>Appropriate media for an overwrite job include the following:</p> <ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Media for which the overwrite protection period has expired</li> </ul> <p>Allocated or imported media may also be overwritten depending on the media overwrite protection level that is set.</p> <p>Depending on your configuration, overwritable media is selected from scratch media or recyclable media.</p> <p>If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“About tape and disk cartridge media”</a> on page 365.</p> <p>See <a href="#">“About media overwrite protection levels for tape and disk cartridge media”</a> on page 377.</p> <p>See <a href="#">“How Backup Exec searches for overwritable media in tape drives and disk cartridges”</a> on page 378.</p>
<p><b>Append to media, overwrite if no appendable media is available</b></p>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec searches for an overwritable media and adds it to the media set.</p> <p>If the append fills a media, the backup job continues on an overwritable media. If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p>

**Table 5-11** Storage options (*continued*)

Item	Description
<b>Append to media, terminate job if no appendable media is available</b>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec terminates the job.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p>
<b>Eject the media after job completes</b>	<p>Ejects the media from the drive or slot when the operation completes. You can also schedule a job to eject media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“Ejecting media from a disk cartridge or tape drive”</a> on page 428.</p>
<b>Retension the media after the job completes</b>	<p>Runs the tape in the drive from beginning to end at a fast speed. Retensioning helps the tape wind evenly and run more smoothly past the tape drive heads. This option is available only if you select a tape drive that supports retensioning.</p>
<b>Use Write once, read many (WORM) media</b>	<p>Specifies the use of WORM (write once, read many) media for this backup job. Backup Exec confirms that the destination device is or contains a WORM-compatible drive, and that the WORM media is available in the drive. If WORM media or a WORM-compatible drive is not found, an alert is sent.</p> <p>See <a href="#">“About WORM media”</a> on page 383.</p>
<b>Export media to vault after job completes</b>	<p>Logically moves the media from the robotic library to the specified media vault.</p> <p>This operation moves media from robotic library slots into a portal. An alert reminds you to remove the media from the portal or from a slot. If a job requires multiple media, the export media operation starts after the backup job completes, not after each media is filled.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“About media vaults”</a> on page 384.</p>

**Table 5-11** Storage options (*continued*)

Item	Description
<b>Compression</b>	<p>Provides the following compression options:</p> <ul style="list-style-type: none"> <li> <p>■ <b>None</b></p> <p>Copies the data to the media in its original form (uncompressed). Using some form of data compression can help expedite backups and preserve storage space. Hardware data compression should not be used in environments where storage devices that support hardware compression are used interchangeably with devices that do not have that functionality. In this situation, hardware compression is automatically disabled. You can manually turn on hardware compression on the drives that support it, but this results in media inconsistency. If the drive that supports hardware compression fails, the compressed media cannot be restored with the non-compression drive.</p> </li> <li> <p>■ <b>Software</b></p> <p>Uses STAC software data compression, which compresses the data before it is sent to the storage device.</p> </li> <li> <p>■ <b>Hardware (if available, otherwise none)</b></p> <p>Uses hardware data compression if the storage device supports it. If the drive does not feature data compression, the data is backed up uncompressed.</p> </li> <li> <p>■ <b>Hardware (if available, otherwise software)</b></p> <p>Uses hardware data compression if the storage device supports it. If the drive does not feature hardware data compression, STAC software compression is used.</p> </li> </ul>
<b>Encryption type</b>	<p>Specifies the type of encryption that you want to use, if any.</p> <p>See <a href="#">“About encryption”</a> on page 551.</p>
<b>Encryption key</b>	<p>Specifies the encryption key that you want to use, if you selected to use encryption.</p> <p>See <a href="#">“Encryption keys”</a> on page 552.</p>
<b>Manage Keys</b>	<p>Lets you manage your encryption keys.</p> <p>You can delete or replace existing encryption keys. You can also create a new encryption key.</p> <p>This option is available only if you select an encryption type.</p> <p>See <a href="#">“About encryption key management”</a> on page 477.</p>

## Network options

The following table lists the options that you can select for networks. You can configure default options for networks, which your backup jobs inherit when you create them. Or you can override the default network settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

---

**Note:** Some of these options do not display in Central Admin Server Option (CASO) environments.

---

**Table 5-12** Network options

Item	Description
<b>Network interface</b>	Specifies the name of the network interface card that connects the Backup Exec server to the network that you want to use for this backup job. The list includes all available network interfaces on the Backup Exec server.
<b>Protocol</b>	Specifies the protocol you want to use for this backup job. The options are as follows: <ul style="list-style-type: none"> <li>■ Use any available protocol</li> <li>■ IPv4</li> <li>■ IPv6</li> </ul>
<b>Subnet</b>	Displays the 32-bit number that determines the subnet to which the network interface card belongs.
<b>Allow use of any available network interface, subnet, or protocol for Backup Exec agents not bound to the above network interface, subnet, or protocol</b>	Lets Backup Exec use any available network if the remote system that you selected for backup or restore is not part of the specified backup network.  If you do not select this option and the remote system is not part of the specified backup network, the job fails. Backup Exec cannot access the data from the remote system.
<b>Interface Details</b>	Displays the Media Access Control (MAC) address, adapter type, description, IP addresses, and subnet prefixes for the interface that you selected for the backup network.

**Table 5-12** Network options (*continued*)

Item	Description
<b>Allow managed Backup Exec server to use any network interface to access Backup Exec agents</b>	<p>Lets a job use any network interface to access Backup Exec agents if the selected network interface is unavailable. Enabling this option lets the managed Backup Exec server use an alternate network interface to run any important backup jobs that would otherwise fail.</p> <p>This option is available only if the Central Admin Server Option (CASO) is installed.</p> <p>See <a href="#">“About the Central Admin Server Option”</a> on page 996.</p>

## Test Run options

You can set up test run jobs to check the following items:

- If the credentials are correct
- If enough capacity is available on the media
- If the media is online and able to be overwritten

See [“About test run jobs”](#) on page 222.

You can configure default options for test run jobs, which your backup jobs inherit when you create them. Or you can override the default test run job settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

**Table 5-13** Test Run options

Item	Description
<b>Enable test run</b>	<p>Enables the test run process.</p> <p>If you select this option, you can configure test run jobs when you create backup jobs.</p>
<b>Schedule</b>	<p>Lets you schedule when and how often the test run job runs.</p> <p>See <a href="#">“Schedule options”</a> on page 188.</p>
<b>Check logon account credentials</b>	<p>Verifies that the Backup Exec logon account is correct for the data that you want to back up.</p>

Table 5-13 Test Run options (*continued*)

Item	Description
<b>Check for sufficient storage space</b>	<p>Tests if there is enough available capacity on the media to complete the job.</p> <p>During the test run job, the number of scheduled jobs in the queue is not checked. Jobs that were scheduled before the test run may use any media that was available when the test run was performed.</p>
<b>Check that media is available</b>	Tests whether the media is online and able to be overwritten.
<b>Use previous job history, if available</b>	<p>Uses any past job histories to determine if enough media is available to run the scheduled backup job.</p> <p>Checking that the previous job history is faster than performing a pre-scan.</p>
<b>Perform pre-scan</b>	<p>Enables Backup Exec to scan the scheduled backup job to determine if enough media is available to run the job.</p> <p>A pre-scan is the most accurate method of determining media capacity. You should select this option if there is not an existing job history.</p>
<b>Upon any failure, place the scheduled backup jobs on hold</b>	Places the scheduled job on hold if Backup Exec detects any failures during the test run.

## Verify options

You can verify backup sets to ensure the integrity of the collection of data and the storage on which it resides. By default, Backup Exec runs a verify operation automatically when a backup job is completed. However, you can schedule the verify operation to run at a different time or you can disable it altogether.

See [“About verifying backed up data”](#) on page 222.

You can configure default options for verify operations, which your backup jobs inherit when you create them. Or you can override the default verify settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

**Table 5-14** Verify options

Item	Description
<b>At the end of the job</b>	Runs a verify operation automatically when the backup job is completed.
<b>After job finishes, as a separate job</b>	<p>Creates a verify operation and schedules it to run as a separate job when the backup job is completed.</p> <p>You can use the <b>Edit</b> option to configure options for the separate verify job.</p> <p>See <a href="#">“Verify Schedule options”</a> on page 198.</p> <p>See <a href="#">“Notification options for jobs”</a> on page 299.</p>
<b>As a separate scheduled job</b>	<p>Creates a verify operation and schedules it to run as a separate job at a later time.</p> <p>You can use the <b>New</b> option to create a new job.</p> <p>The <b>Edit</b> option lets you configure options for the verify job.</p> <p>See <a href="#">“Verify Schedule options”</a> on page 198.</p> <p>See <a href="#">“Notification options for jobs”</a> on page 299.</p>
<b>Do not verify data for this job</b>	Disables the verify operation for the backup job.

## Verify Schedule options

You can configure schedule options for verify operations. You can also configure whether you want the verify operation to run locally on the Backup Exec server or remotely on the Backup Exec agent.

See [“About verifying backed up data”](#) on page 222.

---

**Note:** Some options may not display depending on whether you run the verify operation immediately after a backup job or later as a separate scheduled job.

---

Table 5-15 Verify Schedule options

Item	Description
<b>Verify the data on the client (remote agent) if the device supports it; otherwise the data is sent directly to the device for Backup Exec server or appliance verification</b>	<p>Lets you run the verify operation remotely, if the Backup Exec agent supports it. If the agent is unable to verify the backup sets, the Backup Exec server or appliance completes the verify operation.</p> <p>Running verify operations remotely can help free system resources for your Backup Exec server to run additional backup or restore jobs.</p> <p><b>Note:</b> This option is available only if you choose to run the verify operation as a separate job after the backup is completed.</p>
<b>Schedule</b>	Specifies when you want the separate, scheduled verify job to run.
<b>Enable direct access</b>	<p>Lets the remote Backup Exec agent perform the verify operation. If you do not select this option, the Backup Exec server performs the verify operation.</p> <p><b>Note:</b> This option is only available if you choose to run the verify operation as a separate scheduled job after the backup is completed.</p>

## Advanced Open File options

Backup Exec can use snapshot technology to capture any files that are open when a backup runs. You can configure default options for open files, which your backup jobs inherit when you create them. Or you can override the default open file settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

Table 5-16 Advanced Open File options

Item	Description
<b>Use snapshot technology</b>	Enables the use of snapshot technology for backup jobs.
<b>Automatically select snapshot technology</b>	Enables Backup Exec to select the best snapshot method to use for the type of data that you back up.

**Table 5-16**      **Advanced Open File options** (*continued*)

Item	Description
<p><b>Microsoft Volume Shadow Copy Server (Windows 2003 and later)</b></p>	<p>Enables third-party hardware and software vendors to create snapshot add-ins for use with Microsoft technology.</p> <p>Microsoft, as well as other third party software vendors, often provide the additional components that work with VSS. These components are called Writers. Writers flush application data or file data (if a file is open) that resides in the computer's memory. The data is flushed before the Microsoft Volume Shadow Copy Service makes a snapshot of the volume to be backed up.</p> <p>See your software documentation for information about any VSS Writers that the software vendor may provide.</p> <p>If you turn off Active Directory, Microsoft Volume Shadow Copy Service (VSS) is not available. Jobs that require VSS fail.</p>
<p><b>Snapshot provider</b></p>	<p>Lets you select one of the following snapshot providers for jobs:</p> <ul style="list-style-type: none"> <li>■ Automatic - Allow VSS to select the snapshot provider. Select this option to enable VSS to select the best provider for the selected volume. The order in which a snapshot provider is selected is hardware provider and then the system provider.</li> <li>■ System - Use Microsoft Software Shadow Copy Provider.</li> <li>■ Hardware - Use technology provided by hardware manufacture.</li> </ul> <p>If you select Hardware as the snapshot provider, then the following information applies:</p> <ul style="list-style-type: none"> <li>■ If multiple volumes are selected, then the same type of provider must be able to snap all volumes.</li> <li>■ Hardware providers cannot both be used to snap different volumes in the same job. You must either create another job, or select the option <b>Process logical volumes for backup one at a time</b>.</li> </ul>

Table 5-16 Advanced Open File options (*continued*)

Item	Description
<b>Process logical volumes for backup one at a time</b>	<p>Enables the backup of multiple volumes in one job, with only one logical volume being snapped at a time. To ensure database integrity, or if a volume contains mount points, multiple volumes may need to be snapped one at a time. A volume with mount points to other volumes is considered a logical volume for snapshot purposes. Therefore, that volume and the mount point volumes are snapped together simultaneously.</p> <p>After the logical volume is snapped and backed up, the snapshot is detected before the next logical volume is snapped. This option increases the ability to meet the minimum quiet time that is needed to complete a snapshot.</p> <p>A logical volume can comprise multiple physical volumes. A single logical volume can encompass all of the volumes on which databases reside.</p> <p>If this option is not selected, then a snapshot for all volumes in the backup job is created simultaneously. All volumes must meet the minimum quiet time.</p> <p>This option is only available for Symantec Volume Snapshot Provider (VSP) and Microsoft Volume Shadow Copy Service (VSS) jobs for local volumes.</p> <p>The Shadow Copy Components snapshots are created using VSS, which is reported in the job log.</p>
<b>Enable checkpoint restart</b>	<p>Enables the checkpoint restart option. Checkpoint restart lets you restart jobs that are interrupted. The job restarts from the point where it was interrupted instead of starting over again at the beginning. Files that were already backed up are skipped and only the remaining files are backed up when the job restarts.</p> <p>See <a href="#">“About using checkpoint restart”</a> on page 538.</p>

## Security options

The following table lists the security options that you can select for backup jobs. You can configure default options for security, which your backup jobs inherit when you create them. Or you can override default security settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See “[About backing up data](#)” on page 155.

**Table 5-17** Security options

Item	Description
<b>Run a backup job immediately when an elevated Symantec ThreatCon level is reached</b>	Runs automatic backups when the Symantec ThreatCon reaches the level that you specify in the <b>Symantec ThreatCon level</b> field. You must have Symantec Endpoint Protection 11.0 or later installed on the same computer as Backup Exec to use this feature.
<b>Backup job</b>	Lets you select the type of backup job that you want to run when the Symantec ThreatCon level is raised.
<b>Symantec ThreatCon level</b>	Specifies the ThreatCon level at which you want automatic backups to run.  You can find more information about Symantec ThreatCon levels at the following URL: <a href="http://www.symantec.com">http://www.symantec.com</a>

## Pre/post commands options

You can use pre/post commands to run commands before or after a backup job.

See “[About pre/post commands](#)” on page 542.

You can configure default options for pre- and post-commands, which your backup jobs inherit when you create them. Or you can override the default pre- and post-command settings when you create backup jobs.

See “[Setting default backup job settings](#)” on page 456.

See “[About backing up data](#)” on page 155.

This dialog box includes the following options:

**Table 5-18** Pre- and post-command options

Item	Description
<b>Type a command to run before the backup runs</b>	Runs a command on the specified server before the backup job runs. Use local paths, and make sure that the paths exist on each server and are correct.  Commands that require user interaction, such as prompts, are not supported.

**Table 5-18** Pre- and post-command options (*continued*)

Item	Description
<b>Run job only if pre-command is successful</b>	<p>Runs the backup job only if the pre-command is successful. If the pre-command fails, the job does not run, and is marked as failed.</p> <p>If it is critical that the job does not run if the pre-command fails, then select <b>Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully</b>. If a non-zero code is returned, Backup Exec interprets it to mean that the pre-command did not run successfully. The job does not run and the job status is marked as Failed.</p>
<b>Type a command to run after the backup runs</b>	<p>Runs a command on the specified server after the backup job runs. Use local paths, and make sure that the paths exist on each server and are correct.</p> <p>Commands that require user interaction, such as prompts, are not supported.</p>
<b>Run post-command after job verification completes</b>	<p>Runs the post-command after the verification completes if you selected the <b>Verify after backup completes</b> option on the <b>General backup properties</b> dialog box.</p>
<b>Run post-command only if pre-command is successful</b>	<p>Runs the post-command only if the pre-command is successful.</p> <p>If it is critical that the post-command does not run if the pre-command fails, then select <b>Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully</b>. If a non-zero code is returned for the pre-command, Backup Exec interprets it to mean that the pre-command did not run successfully. The post-command does not run.</p> <p>If you also select <b>Run job only if pre-command is successful</b>, and both the pre-command and the job are successful, but the post-command returns a non-zero code, the job log reports both the job and the post-command as failed.</p>
<b>Run post-command even if job fails</b>	<p>Runs the post-command regardless of whether the job is successful or not.</p> <p>If you also select <b>Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully</b> and the post-command returns a non-zero code, the job log reports the post-command as failed.</p>

**Table 5-18** Pre- and post-command options (*continued*)

Item	Description
<p><b>Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully</b></p>	<p>Lets Backup Exec check the return codes of the pre- and post-commands to determine if they completed successfully.</p> <p>Backup Exec interprets an exit code of zero from either the pre- or post-command to mean that the command completed successfully. Backup Exec interprets a non-zero code to mean that the command ended with an error.</p> <p>After Backup Exec checks the return codes, it continues processing according to the selections you made for running the pre- and post-commands.</p> <p>If this option is not selected, the success of the pre- and post-commands is not determined based on the return code.</p>
<p><b>On this Backup Exec server</b></p>	<p>Runs the pre- and post-commands on this Backup Exec server only.</p>
<p><b>On each server backed up</b></p>	<p>Runs the pre- and post-commands one time on each server that is backed up.</p> <p>The pre- and post-command selections apply to each server independently. If you select this option, the pre- and post-commands are run and completed for each server before Backup Exec begins processing on the next selected server.</p>
<p><b>Cancel command if not completed within x minutes</b></p>	<p>Designates the number of minutes Backup Exec should wait before it cancels a pre- or post-command that did not complete. The default timeout is 30 minutes.</p>

## Files and Folders options

The following table lists the options that you can select for files and folders. You can configure default options for files and folders, which your backup jobs inherit when you create them. Or you can override the default files and folders settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

**Table 5-19** Files and Folders options

Item	Description
<b>Backup method for files</b>	<p>Designates one of the following backup methods:</p> <ul style="list-style-type: none"> <li>■ <b>By modified time</b>                      Backup Exec uses the Windows Change Journal to determine if a file has changed since the last time it was backed up. If the Change Journal is not available, modified time is used.</li> <li>■ <b>Using archive bit</b>                      Backup Exec uses the archive bit from the file system to determine if a file has changed since the last time it was backed up.</li> <li>■ <b>Using catalogs</b>                      Backup Exec uses the Windows Change Journal to determine if a file has changed since the last time it was backed up. Backup Exec compares path names, modified times, deleted and renamed files and folders, and other attributes. If the Change Journal is not available, Backup Exec compares the file information to previous catalogs to determine if it has changed. This method is required for synthetic backups and true image restore. It is the most thorough method, but it takes more time to run.</li> </ul>
<b>Enable single instance backup for NTFS volumes</b>	<p>Lets Backup Exec check the NTFS volume for identical files. If Backup Exec finds multiple copies of a file, it backs up only one instance of that file.</p> <p>This option displays only if you use the Microsoft Windows Single Instance Store (SIS) feature.</p> <p>Single instance backup can considerably reduce the storage space that is required for your backups. Many applications automatically generate some files that have identical content. The actual amount of space that you save depends on the number of duplicate files on the volume.</p> <p><b>Warning:</b> If the backup job does not run to completion, the file data may not be included in the backup set. Rerun the backup job until it is successfully completed. If it was an incremental backup, running the job again does not back up the same files. You must run a full or duplicate backup job to ensure that all files are backed up completely.</p>

**Table 5-19** Files and Folders options (*continued*)

Item	Description
<p><b>Back up files and directories by following junction points and mount points</b></p>	<p>Backs up the information for the junction points and the files and directories to which they are linked. If this check box is not selected, then only the information for the junction points is backed up. The files and directories to which the junction points are linked are not backed up.</p> <p>Backup Exec does not follow junction points that are automatically created by Microsoft Windows Vista/Server 2008 because it can cause the data to be backed up repeatedly.</p> <p>For more information, see the following Symantec Knowledge Base article :  <a href="http://entsupport.symantec.com/umi/V-269-9">http://entsupport.symantec.com/umi/V-269-9</a></p> <p>You cannot select any mounted drives that do not have a drive letter assigned to them. The files and directories to which they are linked are backed up regardless of whether this option is selected.</p> <p>If the files and directories to which the junction points are linked are also included in the backup selections, then they are backed up twice. They are backed up once during the full file and directory backup, and again by the junction point.</p> <p><b>Warning:</b> If a junction point is linked to a location that encompasses it, then recursion (a situation where data is backed up repeatedly) occurs. Recursion results in an error and a job failure. For example, if c:\junctionpoint is linked to c:\, recursion occurs when Backup Exec attempts to back up c:\junctionpoint, and the backup job fails.</p>
<p><b>Back up files and directories by following symbolic links</b></p>	<p>Backs up the information for any symbolic links and the files and directories to which they are linked.</p> <p>If you do not select this option, only the information for the symbolic links is backed up. The files and directories to which they are linked are not backed up.</p> <p>If the symbolic link points to files and directories on a remote computer, the files and directories on the remote computer are not backed up.</p>

**Table 5-19** Files and Folders options (*continued*)

Item	Description
<b>Back up data in Remote Storage</b>	<p>Backs up data that has been migrated from primary storage to secondary storage. The data is not recalled to its original location. It is backed up directly to the backup media.</p> <p>If this option is selected, you should not run a backup of your entire system. Backup Exec has to load the data that has been migrated to secondary storage and additional time is required for migrated data.</p> <p>If this check box is cleared, only the placeholder that stores the location of the data on secondary storage is backed up, not the data itself.</p> <p>This option should not be selected if the device used for secondary storage and backups contains only one drive. If there is only one drive, Remote Storage and Backup Exec compete for use of the drive.</p>

**Table 5-19** Files and Folders options (*continued*)

Item	Description
<p><b>Back up open files</b></p>	<p>Determines how Backup Exec processes any open files for the backup job.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Never</b>            Backup Exec skips any open files that are encountered during the backup job. A list of any files that were skipped appears in the job log.</li> <li>■ <b>If closed within X seconds</b>            Backup Exec waits the specified time interval for files to close before it skips them and continues the backup job.            If the file does not close during the specified interval, it is skipped. A list of skipped files appears in the job log. If multiple files are open, Backup Exec waits the specified time interval for each file. Depending on the number of open files, the wait may significantly increase the backup time.</li> <li>■ <b>With a lock</b>            Backup Exec attempts to open any files that are in use. If Backup Exec is able to open a file, the file is locked while it is backed up. Locking the file prevents other processes from writing to it.            Backing up open files is not as effective as closing applications and allowing the files to be backed up in a consistent state.</li> <li>■ <b>Without a lock</b>            Backup Exec attempts to open any files that are in use. If Backup Exec is able to open the file, the file is not locked while it is backed up. Other applications can write data to the file during the backup operation.</li> </ul> <p><b>Warning:</b> This option allows some files that contain inconsistent data and possibly corrupt data to be backed up.</p>

**Table 5-19** Files and Folders options (*continued*)

Item	Description
<b>Delete selected files and folders after successful backup</b>	<p>Deletes the data you selected to back up after the backup completes successfully.</p> <p>Backup Exec backs up the selected data, verifies the backup sets, and then deletes the data from the server. The logon account credentials that you use to run the job must also have the rights to delete a file. Otherwise, the data is backed up, but it is not deleted.</p> <p>See <a href="#">“About backing up and deleting files”</a> on page 535.</p>
<b>Preserve tree on backup and delete</b>	<p>Retains the file system's directory structure for the files that are backed up in a full backup job. This option is available only when you select the <b>Delete selected files and folders after successful backup</b> option.</p>

## Exclusions options

You can configure Backup Exec to exclude certain files, or certain types of files, from backups. Exclusions can be added to incremental and differential backup jobs, but not full backup jobs.

See [“About including or excluding files for backup jobs”](#) on page 180.

You can configure default options for exclusions, which your backup jobs inherit when you create them. Or you can override the default exclusions settings when you create backup jobs.

See [“Setting default backup job settings”](#) on page 456.

See [“About backing up data”](#) on page 155.

**Table 5-20** Exclusions options

Item	Description
<b>Insert</b>	<p>Lets you create a set of parameters that Backup Exec uses to exclude files, file types, or folders from the backup.</p> <p>See <a href="#">“Exclude Files and Folders options”</a> on page 210.</p>
<b>Delete</b>	<p>Lets you delete a set of parameters that Backup Exec uses to exclude files, file types, or folders from the backup.</p>

**Table 5-20** Exclusions options (*continued*)

Item	Description
<b>Modify</b>	Lets you edit a set of parameters that Backup Exec uses to exclude files, file types, or folders from the backup.  See <a href="#">“Exclude Files and Folders options”</a> on page 210.

## Exclude Files and Folders options

The following options let you create a set of parameters that Backup Exec uses to exclude files, file types, or folders from backups.

See [“About including or excluding files for backup jobs”](#) on page 180.

**Table 5-21** Exclude Files and Folders options

Item	Description
<b>Resource name</b>	Lets you exclude files from a backup of a different drive than the one you selected previously from the backup selections.

**Table 5-21** Exclude Files and Folders options (*continued*)

Item	Description
<b>Path</b>	<p>Specifies the name of the folder and/or subfolder that contains any specific file that you want to exclude.</p> <p>You can use wildcard characters. Use a question mark (?) to represent any single character. Use two asterisks (**) to represent any number of characters.</p> <p>For example, on your C: drive you have a My Documents folder that contains a subfolder called Work Files. There are three Work Files subfolders that are called 2010, 2011, 2012. Each one of these subfolders has a subfolder called Personnel.</p> <p>If you type the path as \My Documents\**\Personnel, the backup excludes the following:</p> <ul style="list-style-type: none"> <li>■ C:\My Documents\Work Files\2010\Personnel</li> <li>■ C:\My Documents\Work Files\2011\Personnel</li> <li>■ C:\My Documents\Work Files\2012\Personnel</li> </ul> <p>In addition, every subfolder below the ** wildcard is excluded. However, the only files from the subfolders that are excluded are those that match the file name that you type in the <b>Name</b> field.</p> <p>So in the example above, every subfolder of C:\My Documents is excluded from the backup. Only any files that match the name in the <b>Name</b> field would be excluded.</p>
<b>Name</b>	<p>Specifies the name of the file that you want to exclude from the backup.</p> <p>You can use wildcard characters. use a question mark (?) to represent any single character. Use two asterisks (**) to represent any number of characters.</p> <p>For example, to include all files with the .exe extension, type **.exe.</p>
<b>Apply to subdirectories</b>	Excludes the contents of all the subfolders when a directory is selected.
<b>Only modified files</b>	Excludes modified files in the path that you specify.
<b>Only read-only files</b>	Excludes the files that cannot be modified.

**Table 5-21** Exclude Files and Folders options (*continued*)

Item	Description
<b>Files dated</b>	Excludes the files that were created or modified during a specific time period. Then select the beginning and ending dates.
<b>Files not accessed in X days</b>	Excludes any files that have not been accessed in a specified number of days. This is useful when you need to migrate older files from your system.

## About backup sets

A backup set is a collection of the data that you back up from a single source of content. A single source of content can be a server or a Microsoft Exchange dataset, for example. If you select multiple sources of content, Backup Exec creates multiple backup sets. When you run a backup job, Backup Exec creates the backup sets and writes them on storage. To restore data, you select the backup sets that contain the data that you want to restore.

When you work with your backed up data, you work with backup sets. Backup Exec offers a number of options for managing the data that is contained in your backup sets.

You can do the following things with backup sets:

- Configure the amount of time that backup sets are stored before Backup Exec expires the backup set and reclaims the disk space.  
See [“About keeping backup sets”](#) on page 213.
- Delete unneeded backup sets.  
See [“Deleting backup sets”](#) on page 214.
- Retain important or time-sensitive backup sets indefinitely.  
See [“Retaining backup sets”](#) on page 215.
- Release any backup sets that are retained to let them expire automatically.  
See [“Releasing retained backup sets”](#) on page 216.
- Catalog backup sets so that you can view the data that is contained in the backup sets and search for files to restore.  
See [“Cataloging backup sets”](#) on page 217.
- View the contents of backup sets and browse the backed up data that is contained in them.  
See [“Viewing the contents of backup sets”](#) on page 217.

- View the system and job properties of backup sets. See [“Viewing backup sets properties”](#) on page 218.
- Copy backup sets from one Backup Exec server to another Backup Exec server. See [“Duplicating backup sets”](#) on page 219.
- Verify the data in backup sets to ensure that Backup Exec can read it. See [“Verifying backup sets”](#) on page 223.

## About keeping backup sets

Backup Exec keeps the backup sets that are stored on disk or on cloud storage for as long as you specify in the backup job properties. By default, the amount of time that backup sets are stored on disk is based on the type of backup job and its schedule.

For example, you can specify to keep the backup sets from a full backup for two weeks. After two weeks, the backup sets expire and Backup Exec can reclaim that disk space. If you later create an incremental backup, Backup Exec keeps the full backup sets for two weeks, plus the amount of time that it keeps the incremental backup sets. If you keep the incremental backup sets for four weeks, then Backup Exec keeps the full backup sets for six weeks. The data from a full backup is kept as long as the data from its associated incremental backups. Backup Exec does not expire backup sets from a job that depends on another job until the data retention expires for all of the associated jobs.

You can keep the backup sets that are on disk from automatically expiring by retaining the backup sets. Backup Exec then retains all dependent backup sets as well.

See [“Retaining backup sets”](#) on page 215.

Backup Exec manages the retention of backup sets differently depending on the type of storage to which you back up the data.

**Table 5-22** Storage types and backup set retention

Type of storage	Backup data retention
Disk and cloud storage	<p>Backup Exec uses data lifecycle management to automatically expire the backup sets when the amount of time that is specified in the backup job expires. If backup sets are dependent on other backup sets, then Backup Exec does not expire the data until all expiration dates are reached.</p> <p>For disk-based storage that you reattach to the Backup Exec server after a specified number of days, you can prevent Backup Exec from reclaiming that disk space. A global setting limits Backup Exec to read-only operations on disk-based storage if it has been detached for a specified number of days. You can also limit Backup Exec to read-only operations per disk storage device by enabling the setting on the device properties.</p> <p>See <a href="#">“Global settings for storage”</a> on page 415.</p> <p>See <a href="#">“Disk storage properties”</a> on page 310.</p> <p>See <a href="#">“About restoring data from a reattached disk-based storage device”</a> on page 308.</p>
Tape and disk cartridge media	<p>Backup Exec uses the Advanced Device and Media Management (ADAMM) feature to manage data retention on tape and disk cartridge media. ADAMM expires the backup sets that are stored on media according to a set of rules that you apply to the media. The set of rules that manage tape and disk cartridge media is called a media set. You create media sets that specify append periods, overwrite protection periods, and vaulting periods.</p> <p>See <a href="#">“About media sets”</a> on page 366.</p>

## Deleting backup sets

You can delete any backup sets that you no longer need to save storage space.

See [“About backup sets”](#) on page 212.

### To delete backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to delete.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:

- To delete a single backup set, right-click the backup set.
  - To delete multiple backup sets, Shift + click or Ctrl + click the backup sets, and then right-click one of the selected backup sets.
- 4 Click **Delete**.
  - 5 Click **Yes** to confirm that you want to delete the backup sets.

## Retaining backup sets

You can prevent backup sets from automatically expiring by retaining the backup sets. Backup Exec retains all dependent backup sets as well. For example, if you choose to retain an incremental backup set, Backup Exec retains all backup sets dating back to, and including, the last full backup. You may need to retain backup sets for legal purposes, such as compliance with data retention laws.

See [“About backup sets”](#) on page 212.

After you retain a backup set, Backup Exec prevents the backup set from expiring indefinitely. If you decide that you no longer need to retain a backup set, you must release it so that it can expire automatically.

See [“Releasing retained backup sets”](#) on page 216.

### To retain backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to retain.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:
  - To retain a single backup set, right-click the backup set.
  - To retain multiple backup sets, Shift + click or Ctrl + click the backup sets, and then right-click one of the selected backup sets.
- 4 Click **Retain**.
- 5 Complete the appropriate options.  
See [“Retain Backup Sets options”](#) on page 215.
- 6 Click **OK**.

### Retain Backup Sets options

You can prevent backup sets from automatically expiring by retaining the backup sets.

See [“Retaining backup sets”](#) on page 215.

**Table 5-23** Retain Backup Sets options

Item	Description
<b>Legal</b>	Specifies that the reason for retaining the backup sets is a legal one. You may have to retain backup sets to comply with data retention policies.
<b>User defined</b>	Specifies that the reason for retaining the backup sets is user-defined .
<b>Explanation</b>	Details any additional information about why you retained the backup sets. Entering an explanation in this field can help remind you why you retained the backup sets or for how long they should be retained.

## Releasing retained backup sets

You can override the retention period for backup sets by manually retaining them. When you choose to retain backup sets, Backup Exec prevents the backup sets from automatically expiring when their retention period is over. You can manually retain backup sets indefinitely.

See [“Retaining backup sets”](#) on page 215.

If you no longer need the retained backup sets, you can allow them to expire. First, you need to remove the backup sets' retained status. Then Backup Exec expires the backup sets automatically according to the backup sets' storage settings.

See [“Storage options”](#) on page 190.

### To release retained backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the retained backup sets that you want to release.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:
  - To release a single backup set, right-click the retained backup set.
  - To release multiple backup sets, Shift + click or Ctrl + click the retained backup sets, and then right-click one of the selected backup sets.
- 4 Clear the **Retain** check box.

## Cataloging backup sets

Before you can restore or verify data, the data must be cataloged.

See “[About catalogs](#)” on page 242.

You can catalog backup sets.

See “[About backup sets](#)” on page 212.

### To catalog backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to catalog.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:
  - To catalog a single backup set, right-click the backup set.
  - To catalog multiple backup sets, Shift + click or Ctrl + click the backup sets, and then right-click one of the selected backup sets.
- 4 Click **Catalog**.

## Viewing the contents of backup sets

After you complete a backup job, you can view the data that is contained in the backup sets that are created. Viewing the contents of backup sets can help you to confirm what data was backed up. You may also want to view the contents of backup sets before you run a restore job to verify the data that they contain.

See “[About backup sets](#)” on page 212.

### To view the contents of backup sets

- 1 On the **Backup and Restore** or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to view.
- 2 In the left pane, click **Backup Sets**.
- 3 Double-click the backup set that you want to view.

---

**Note:** On the **Backup and Restore** tab, you must expand the backup source to see backup sets.

---

- 4 In the left pane, click **Contents**.

The contents of the backup set display in the left pane in a tree view. You can expand folders and drives to view their contents in the right pane.

## Viewing backup sets properties

After you complete a backup job, you can view the properties of the backup sets that are created.

See “[About backup sets](#)” on page 212.

You can view the following properties for backup sets:

- Backup source
- Backup date
- Expiration date
- Backup method
- Size
- Location
- Backup set description
- Data encryption
- True image
- Server name
- Catalog file name
- Snapshot

### To view backup sets properties

- 1 On the **Backup and Restore** or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to view.
- 2 In the left pane, click **Backup Sets**.
- 3 Double-click the backup set that you want to view.

---

**Note:** On the **Backup and Restore** tab, you must expand the backup source to see backup sets.

---

- 4 In the left pane, click **Properties**.

## About duplicating backed up data

You can duplicate backup data automatically by adding a duplicate stage to a backup definition. You can also manually duplicate backup data from completed jobs by selecting the backup set or sets that you want to duplicate.

When you duplicate backup data with a duplicate stage, the stage uses the related, or linked, backup job in the backup definition as the source. You can configure storage, notification, and verify options for the duplicate stage. You can schedule the duplicate job to run at a designated time or you can schedule it to run immediately after the backup job completes. You schedule the duplicate stage to run as a recurring job, so that it duplicates the backup data each time the linked backup job runs.

See [“About backing up data”](#) on page 155.

See [“About stages”](#) on page 183.

When you duplicate backup data from completed jobs, you select the backup sets that you want to duplicate on the **Backup and Restore** tab. The backup sets that you select are read from the source and written to the selected destination, such as a drive, drive pool, or backup folder. You can encrypt the duplicated backup sets. You can schedule when this type of job runs, but it only runs one time.

You can select to duplicate one or more individual backup sets or you can duplicate an entire job history. The job history includes all of a backup definition's dependant backup sets. For example, if you select to duplicate an incremental backup, Backup Exec automatically duplicates all incrementals dating back to, and including, the last full backup.

See [“Duplicating backup sets”](#) on page 219.

See [“Duplicating job history”](#) on page 220.

You can use a duplicate backup job to copy data directly from a virtual device to a physical device. Software encryption cannot be applied to a duplicate backup job when you copy data directly from a virtual device to a physical device. You must either disable DirectCopy or select not to encrypt the job.

See [“How to copy data directly from a virtual tape library to a physical tape device”](#) on page 225.

If you duplicate any Oracle backup sets that were created with multiple data streams, note the following:

- Backup Exec converts the multiple data streams to a sequential data stream during the duplication job.
- A restore job from the duplicated copy may be slower than a restore job from the original media.

## Duplicating backup sets

You can duplicate backup sets after a backup job is complete. You can duplicate backup sets if you want to duplicate only the data that was backed up in a specific

backup job instance. If you want to duplicate a job and all of its dependent backup sets, you can duplicate a job history.

See [“About duplicating backed up data”](#) on page 218.

See [“About backup sets”](#) on page 212.

See [“Duplicating job history”](#) on page 220.

#### To duplicate backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the backup sets that you want to duplicate.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:
  - To duplicate a single backup set, right-click the backup set.
  - To duplicate multiple backup sets, Shift + click or Ctrl + click the backup sets, and then right-click one of the selected backup sets.
- 4 Select **Duplicate**.
- 5 Complete the options on the **Duplicate Job** dialog box.  
See [“Duplicate Job options”](#) on page 221.
- 6 Click **OK** on the **Duplicate Job** dialog box.

## Duplicating job history

You can duplicate an entire job history, which includes all of a job's dependent backup sets. For example, if the backup definition used incremental backups, Backup Exec duplicates all incrementals dating back to, and including, the last full backup. If you want to duplicate only the data that was backed up in a specific backup job instance, you can duplicate backup sets.

See [“About duplicating backed up data”](#) on page 218.

See [“About the Job History”](#) on page 260.

See [“Duplicating backup sets”](#) on page 219.

#### To duplicate job history

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the job history that you want to duplicate.
- 2 In the left pane, click **Job History**.
- 3 Do one of the following:

- To duplicate a single job history, right-click the job history.
  - To duplicate multiple job histories, Shift + click or Ctrl + click the job histories, and then right-click one of the selected job histories.
- 4 Click **Duplicate**.
  - 5 Complete the options on the **Duplicate Job** dialog box for each job history that you want to duplicate.  
See “[Duplicate Job options](#)” on page 221.
  - 6 Click **OK** on the **Duplicate Job** dialog box for each duplicate job that you create.

## Duplicate Job options

You can create a duplicate copy of backup sets or an entire job history after you complete a backup job.

See “[Duplicating backup sets](#)” on page 219.

See “[Duplicating job history](#)” on page 220.

**Table 5-24** Duplicate Job options

Item	Description
<b>Storage</b>	Specifies the storage to which you want to copy the backup sets or job history.
<b>Keep for</b>	Designates the amount of time for which you want to keep the backup sets or job history. The media is protected from being overwritten for the amount of time you specify.
<b>Schedule</b>	Lets you schedule when you want Backup Exec to run the duplicate job. You can select a date and time or you can choose to run the job immediately.
<b>Encryption type</b>	Specifies the encryption type that you want to use, if any.
<b>Encryption key</b>	Specifies the encryption key that you want to use, if you selected an encryption type.
<b>Manage Keys</b>	Lets you create a new encryption key or delete an existing encryption key.  This option is available only if you select an encryption type.
<b>Backup sets being duplicated</b>	Displays any information about the backup sets that you selected to duplicate.

## About test run jobs

Test run jobs attempt to determine if a scheduled backup could possibly fail when you run it. When you run a test job, no data is backed up. Instead, Backup Exec checks your storage capacity, credentials, and media to find potential errors. If there is an error, the job continues to run until it is completed. The error appears in the job log. You can also configure Backup Exec to send a notification to a designated recipient.

You can configure test run jobs to run automatically before your scheduled backup jobs. Or you can run a test run job at any time from the **Jobs** pane on the **Backup and Restore** tab.

During a test run job, the following things may cause a job to fail:

- Logon credentials are incorrect.
- Storage capacity is not sufficient.
- Tape or disk cartridge media is not available.
- Overwritable media is not available for an overwrite job.
- Appendable media is not available for an append job.

A test run job checks the media capacity that is available for the selected job. However, you can check if there is enough available media for multiple test run jobs in the Test Run Results Report.

See [“Test Run Results report”](#) on page 624.

Before you run a test run job, Symantec recommends that you run backup jobs to your storage devices first. Backup Exec does not recognize the capacity of a storage device until an actual backup job sends data to the device. If you create a test run job before any other jobs, Backup Exec cannot check that the device has sufficient capacity to perform the backup job. After at least one backup job has sent data to a device, Backup Exec can determine the capacity.

See [“Running a test job from the Jobs list”](#) on page 259.

See [“Test Run options”](#) on page 196.

## About verifying backed up data

Backup Exec can perform a verify operation to make sure that the media can be read once a backup job has been completed. Symantec recommends that you verify all backups. By default, Backup Exec automatically verifies backups at the end of a job. However, you can also schedule the verify operation to take place at a later

time or disable the verify operation altogether. You can change Backup Exec's verify options as part of the default backup settings or for individual backup jobs.

You can also choose to verify a backup set or a job history at any time.

See [“Verify options”](#) on page 197.

See [“Verifying backup sets”](#) on page 223.

See [“Verifying job history”](#) on page 223.

## Verifying backup sets

You can verify backup sets to ensure the integrity of the collection of data and the media on which it resides. You can verify backup sets if you want to verify only the data that was backed up in a specific backup job instance. If you want to verify a job and all of its dependent backup sets, you can verify a job history.

See [“About backup sets”](#) on page 212.

See [“About verifying backed up data”](#) on page 222.

See [“Verifying job history”](#) on page 223.

### To verify backup sets

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the backup set or backup sets that you want to verify.
- 2 In the left pane, click **Backup Sets**.
- 3 Do one of the following:
  - To verify a single backup set, right-click the backup set.
  - To verify multiple backup sets, Shift + click or Ctrl + click the backup sets, and then right-click one of the selected backup sets.
- 4 Click **Verify**.
- 5 Complete the options on the **Verify Job** dialog box.  
See [“Verify Job options”](#) on page 224.
- 6 Click **OK**.

## Verifying job history

You can verify backup sets to ensure the integrity of the collection of data and the media on which it resides. You can verify an entire job history, which includes all of a job's dependent backup sets. For example, if the backup definition used incremental backups, Backup Exec verifies all incrementals dating back to, and

including, the last full backup. If you want to verify only the data that was backed up in a specific backup job instance, you can verify backup sets.

See [“About backup sets”](#) on page 212.

See [“About verifying backed up data”](#) on page 222.

See [“Verifying backup sets”](#) on page 223.

#### To verify a backup

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device that is related to the job history or job histories that you want to verify.
- 2 In the left pane, click **Job History**.
- 3 Do one of the following:
  - To verify a single job history, right-click the backup set.
  - To verify multiple job histories, Shift + click or Ctrl + click the job histories, and then right-click one of the selected job histories.
- 4 Click **Verify**.
- 5 Complete the options on the **Verify Job** dialog box for each job history that you want to verify.
 

See [“Verify Job options”](#) on page 224.
- 6 Click **OK** on the **Verify Job** dialog box for each job history that you verify.

### Verify Job options

You can verify backup sets to ensure the integrity of the collection of data and the media on which it resides.

See [“Verifying backup sets”](#) on page 223.

See [“Verifying job history”](#) on page 223.

**Table 5-25** Verify Job options

Item	Description
<b>Schedule</b>	Specifies when you want the verify operation to occur. You can schedule the operation or you can choose to run it immediately.
<b>Backup sets being verified</b>	Displays any information about the backup sets that you selected to verify.

# How to copy data directly from a virtual tape library to a physical tape device

Backup Exec's **DirectCopy to tape** option enables data to be copied from a virtual tape library directly to a physical tape device during a duplicate backup job. The Backup Exec server coordinates the duplicate job, but it does not copy the data. Instead, the virtual tape library copies the virtual tape image directly to the physical device. The Backup Exec server records information about the data in the catalog. Because the information about the copied data is in the catalog, you can restore data from either the virtual tape library or the physical device. The job log for the duplicate backup job indicates that **DirectCopy to tape** is enabled.

See [“Copying data from a virtual tape library to a physical tape device”](#) on page 225.

To use **DirectCopy to tape**, both the source device and the destination device must be NDMP-enabled. If the devices are not NDMP-enabled, then Backup Exec performs a regular duplicate backup job.

---

**Note:** If you select disk storage as the destination device for a duplicate job with **DirectCopy to tape** enabled, Backup Exec performs a regular duplicate job.

---

Both hardware encryption and software encryption are supported with **DirectCopy to tape**. For software encryption, both the source backup set and the destination backup set must use software encryption.

See [“About configuring DBA-initiated job templates”](#) on page 483.

## Copying data from a virtual tape library to a physical tape device

You can create a duplicate backup job to copy data directly from a virtual tape library to a physical tape device.

---

**Note:** Both the source device and the destination device must be NDMP-enabled. If the devices are not NDMP-enabled, then Backup Exec performs a regular duplicate backup job.

---

See [“How to copy data directly from a virtual tape library to a physical tape device”](#) on page 225.

**Table 5-26** How to use DirectCopy to tape to copy data from a virtual tape library to a physical device

Step	Notes	For more information
Create a regular backup job.	Select a virtual tape library as the storage destination.	See <a href="#">“Backing up data”</a> on page 163. See <a href="#">“Storage options”</a> on page 190.
Create a duplicate backup job.	In the DBA-initiated job settings: <ul style="list-style-type: none"> <li>■ Select a physical tape device as the destination.</li> <li>■ Select <b>Enable DirectCopy to tape</b>.</li> </ul>	See <a href="#">“Storage options for DBA-initiated jobs”</a> on page 486. See <a href="#">“Duplicate job settings for DBA-initiated jobs”</a> on page 494.

## Viewing all scheduled backup jobs on a calendar

You can view all of your scheduled backup jobs for a month, for a week, or for a day on a calendar. It can be helpful to view your backup jobs in the calendar format to make sure there are no scheduling conflicts. You may want to check the calendar before you create a new job.

### To view all scheduled backup jobs on a calendar

- 1 On the **Backup and Restore** tab, in the **Backups** group, click **Backup Calendar**.  
See [“Backup calendar options”](#) on page 227.
- 2 When you are finished viewing the calendar, click **Close**.

## Excluding dates from the schedule using the backup calendar

You can exclude dates from the backup schedule using the backup calendar. You may want to exclude specific dates, such as holidays, from your backup schedule. Backup Exec skips any backups that are scheduled for excluded dates. You can delete the date from the list later if you want to schedule a backup job on that day.

See [“About excluding dates from the backup schedule”](#) on page 458.

**To exclude dates from the schedule using the backup calendar**

- 1 On the **Backup and Restore** tab, in the **Backups** group, click **Backup Calendar**.  
See “[Backup calendar options](#)” on page 227.
- 2 Right-click the date that you want to exclude from the backup schedule.
- 3 Click **Exclude date**.

---

**Note:** To include the date later, right-click the date and then click **Include date**.

---

## Backup calendar options

You can view any scheduled backups on a calendar. It can be helpful to view your backup jobs in the calendar format to make sure there are no scheduling conflicts.

See “[Viewing all scheduled backup jobs on a calendar](#)” on page 226.

**Table 5-27** Backup calendar options

Item	Description
<b>Day</b>	Displays all scheduled backup jobs for a single day.
<b>Week</b>	Displays all scheduled backup jobs for a week.
<b>Month</b>	Displays all scheduled backup jobs for a month.

**Excluding dates from the schedule using the backup calendar**

# Restores

This chapter includes the following topics:

- [About searching for and restoring data](#)
- [Setting defaults for restore jobs](#)
- [About restoring encrypted data](#)
- [About performing a complete online restore of a Microsoft Windows computer](#)
- [About restoring System State](#)
- [Restoring System State to a domain controller](#)
- [About restoring Backup Exec Shadow Copy Components](#)
- [About restoring utility partitions and UEFI system partitions](#)
- [Installing a new Windows Server domain controller into an existing domain by using a redirected restore](#)
- [About restoring media created with other backup software](#)
- [About canceling a restore job](#)
- [About catalogs](#)

## About searching for and restoring data

Backup Exec provides guided **Search** and **Restore** methods to assist you when you search for or restore backed up data. If you have installed the Archiving Option, you can also search for or restore archived data.

From **Search** or **Restore**, you can do the following:

- Restore data to the location from which it was originally backed up or redirect the restore to another location.
- Start the restore job immediately or schedule it to run at a future time.

You can also specify a network to use as a default network for all restore jobs.

See “[Setting defaults for restore jobs](#)” on page 231.

**Table 6-1** Guided methods to restore and search for data

Method	Description
<b>Search</b>	<p>Lets you select multiple servers to search for backup sets. Then, you can choose to restore the data, or you can copy and save the search criteria and the results to the clipboard. You can then email the results to the person who requested the restore to ensure that you have found the correct data before you restore it.</p> <p>Backup Exec creates separate restore jobs for each server that you restore data to.</p> <p>Search supports only the following types of data:</p> <ul style="list-style-type: none"> <li>■ Files and folders</li> <li>■ Exchange and SharePoint backup sets for which Granular Recovery Technology was enabled</li> <li>■ Archived file system data and archived Exchange mailbox data</li> </ul> <p>The <b>Search</b> option on the <b>Backup and Restore</b> tab launches the Search Wizard.</p>
<b>Restore</b>	<p>Lets you browse the backup sets from a single server. Then, you can restore the data.</p> <p>You can also perform a complete online restore of a Windows computer if the computer was fully selected for a backup. By default, backup jobs include all necessary components that are required for a complete restore.</p> <p>The <b>Restore</b> option on the <b>Backup and Restore</b> tab launches the Restore Wizard .</p>
<b>Simplified Disaster Recovery</b>	<p>Lets you recover Windows computers after a hard drive failure. The Simplified Disaster Recovery wizards guide you in preparing for disaster recovery, and in recovering a local computer or a remote computer to its pre-disaster state.</p> <p>See “<a href="#">About Simplified Disaster Recovery</a>” on page 704.</p>

- See [“About restoring Exchange data”](#) on page 857.
- See [“About restoring SQL databases”](#) on page 825.
- See [“About restoring Oracle resources”](#) on page 904.
- See [“About restoring VMware resources”](#) on page 791.
- See [“About restoring deduplicated data”](#) on page 778.
- See [“About restoring items from the archives”](#) on page 1259.
- See [“About restoring an Archiving Option component”](#) on page 1265.
- See [“About restoring Microsoft SharePoint data”](#) on page 872.
- See [“About restoring Enterprise Vault”](#) on page 929.
- See [“About restoring data to Linux computers”](#) on page 1095.
- See [“About restoring Lotus Domino databases”](#) on page 973.

## Setting defaults for restore jobs

You can specify a default network to use for all restore jobs.

See [“About specifying backup networks”](#) on page 548.

### To set defaults for restore jobs

- 1 Click the Backup Exec button, select **Configuration and Settings**, select **Job Defaults**, and then select **Restore**.
- 2 Edit the options as appropriate.  
See [“Restore job defaults”](#) on page 231.
- 3 Click **OK**.

## Restore job defaults

You can specify defaults for all restore jobs.

See [“Setting defaults for restore jobs”](#) on page 231.

**Table 6-2** Restore job defaults

Item	Description
<b>Network interface</b>	<p>Designates the name of the network interface card that connects the Backup Exec server to the network that you want to use for the restore job. The list includes all available network interface cards on the Backup Exec server.</p> <p>If the Central Admin Server Option (CASO) is installed, select the option <b>Use the default network interface for the managed Backup Exec server</b>. This option enables delegated restore jobs to be processed using the network interface card that is configured as the default on the managed Backup Exec server.</p>
<b>Protocol</b>	<p>Designates the network protocol.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>■ Use any available protocol</li> <li>■ Use IPv4</li> <li>■ Use IPv6</li> </ul> <p>See <a href="#">“About using IPv4 and IPv6 in Backup Exec”</a> on page 550.</p>
<b>Subnet</b>	<p>Displays the 32-bit number that determines the subnet to which the network interface card belongs.</p> <p>This option only appears when the network interface is set to local area connection.</p>

Table 6-2 Restore job defaults (*continued*)

Item	Description
<b>Allow use of any available network interface, subnet, or protocol for Backup Exec agents not bound to the above network interface, subnet, or protocol</b>	<p>Ensures that the data from a remote computer on which a Backup Exec agent is installed is restored over any available network. The remote computer that you selected for restore cannot already be part of a specified restore network.</p> <p>If this option is unchecked and if the remote computer is not part of the specified restore network, then the job fails. Backup Exec cannot restore the data to the remote computer.</p> <p>This option can only be selected when the network interface is set to local area connection.</p>
<b>Interface Details</b>	<p>Displays the Media Access Control (MAC) address, Adapter type, Description, IP addresses, and subnet prefixes of the network interface that you selected for the restore network.</p>

## About restoring encrypted data

Encrypted backup sets are identified in the restore selection list by an icon with a lock on it. When you select encrypted data to restore, Backup Exec automatically validates the encryption key for the data. If the encryption key that was used to back up the data is still in the Backup Exec Database, then Backup Exec selects that encryption key automatically. However, if the encryption key cannot be located, Backup Exec prompts you to provide the pass phrase for the encryption key that was used to back up the data. If you enter the correct pass phrase, Backup Exec recreates the key.

When you use a restricted encryption key to back up data, users other than the key owner must enter the pass phrase to restore data.

See [“About pass phrases in encryption”](#) on page 553.

See [“About encryption key management”](#) on page 477.

See [“Replacing an encryption key”](#) on page 480.

## About performing a complete online restore of a Microsoft Windows computer

You can perform a complete online restore of a Microsoft Windows computer if the computer was fully selected for a backup. You select the backup set time from which you want to recover the computer. All required backup sets are automatically selected. You can select additional backup sets to restore as appropriate. You cannot redirect the restore of the computer.

See [“About backing up critical system components”](#) on page 539.

See [“About searching for and restoring data”](#) on page 229.

## About restoring System State

Depending on the version of Microsoft Windows, service pack levels, and features that are installed, you can restore the following system state data:

- Active Directory
- Automated system recovery
- Background Intelligent Transfer Service
- COM+ Class Registration database
- Dynamic Host Configuration Protocol
- Event logs
- File Server Resource Manager
- Internet Information Service (IIS)
- Microsoft Search Service
- Network Policy Server
- Registry
- Remote Storage
- Removable Storage Manager
- Shadow Copy Optimization Writer
- System files
- Terminal Server Licensing
- Terminal Services Gateway
- Windows Deployment Services

- Windows Management Instrumentation

If the server is a certificate server, then System State includes the Certificate Services database.

If the server is a domain controller, then System State includes the Active Directory services database and SYSVOL directory.

See [“About the Agent for Microsoft Active Directory”](#) on page 985.

You must restart the computer after you restore System State data.

---

**Note:** You should not cancel a System State restore job. Canceling this job can leave the server unusable.

---

See [“About backing up critical system components”](#) on page 539.

See [“About performing a complete online restore of a Microsoft Windows computer”](#) on page 234.

## Restoring System State to a domain controller

To restore System State to a computer that is a domain controller, you must start the computer in safe mode. Then, use the Directory Services Restore Mode to perform the restore.

To replicate Active Directory to the other domain controllers that exist in the domain, you must perform an authoritative restore of the Active Directory. An authoritative restore ensures that the restored data is replicated to all of the servers. Performing an authoritative restore includes running Microsoft's Ntdsutil utility after Backup Exec restores System State, but before you restart the server. For more information about authoritative restore and the Ntdsutil utility, see your Microsoft documentation.

See [“About restoring System State”](#) on page 234.

### To restore System State to a domain controller

- 1 Start the destination server, press <F8> when prompted for Startup Options, and then select the **Directory Services Restore Mode** option.
- 2 Do one of the following:

To open services on Windows 2003

Do the following in the order listed:

- Right-click **My Computer**.
- Click **Manage**.
- Expand **Services and Applications**.

To open services on Windows 2008

Do the following in the order listed:

- Right-click **My Computer**.
- Click **Manage**.
- Expand **Configuration**.

- 3 Click **Services**.
- 4 For each Backup Exec service listed, do the following in the order listed:
  - Click **Properties**.
  - Click the **Log On** tab, click **This account**, enter a user account with local administrator's rights, and then click **OK**.
  - Right-click the service, and then click **Start**.
- 5 After the Backup Exec services have started, run the Restore Wizard to restore System State.  
See "[About searching for and restoring data](#)" on page 229.
- 6 In the Restore Wizard, enable the option **Mark this server as the primary arbitrator for replication when restoring SYSVOL in System State**.
- 7 Restart the server before you restore more data.

## About restoring Backup Exec Shadow Copy Components

The Backup Exec Shadow Copy Components file system uses Microsoft's Volume Shadow Copy Service to protect third-party application and user data on Windows computers. You can restore the items in Backup Exec Shadow Copy Components individually or together.

The following items are contained in Backup Exec Shadow Copy Components:

- Backup Exec Deduplication Disk Storage
- Distributed File System Replication (DFSR)
- OSISoft PI Server

See "[About searching for and restoring data](#)" on page 229.

See "[About restoring System State](#)" on page 234.

## About restoring utility partitions and UEFI system partitions

You can select utility partitions for restore. Utility partitions are small partitions that OEM vendors such as Dell, Hewlett-Packard, and IBM install on the disk. These partitions contain system diagnostic and configuration utilities. You can restore Unified Extensible Firmware Interface (UEFI) partitions, which are the small partitions that the operating system creates. The UEFI system partitions contain the critical system files, such as bootmgr and BOOT\BCD files.

Requirements for restoring utility partitions are as follows:

- You must recreate the utility partitions before you restore any data.
- You must have Administrator rights.
- You cannot redirect the restore of a utility partition to another computer.
- You can only restore the utility partitions that belong to the same vendor. For example, you cannot restore Dell utility partitions to a Compaq utility partition.
- The size of the utility partition to which you restore the data must be equal to or greater in size than the utility partition that was backed up.

See [“About searching for and restoring data”](#) on page 229.

## Installing a new Windows Server domain controller into an existing domain by using a redirected restore

To install a new Windows Server domain controller into an existing domain, the Active Directory and SYSVOL data must be replicated to the new domain controller. If there is a large amount of data to be replicated or if the connection between the domain controllers is slow, the replication time can be lengthy. The amount of data to be replicated and the connection speed also affects the Active Directory Application Mode replication time. To decrease the replication time for Active Directory and Active Directory Application Mode, you can use the Microsoft Windows feature called Install from Media.

For Active Directory, use the Install from Media feature. Restore the system state backup sets of an existing domain controller in the domain in which you want to add a new domain controller. Then, perform a redirected restore of the system state backup sets to the destination domain controller.

For Active Directory Application Mode, you can back up data using the ADAM Writer. Then, you can perform a redirected restore of the data from the ADAM backup to the destination computer.

See [“About the Agent for Microsoft Active Directory”](#) on page 985.

For more information, refer to your Microsoft documentation.

**Table 6-3** How to install a new Windows Server domain controller into an existing domain by using a redirected restore

Step	Description
Step 1	<p>Back up the System State data of an active Windows Server domain controller that is in the target domain. You should back up the data to some type of removable storage, such as a disk cartridge device or a tape.</p> <p>See <a href="#">“Backing up data”</a> on page 163.</p>
Step 2	<p>Attach the storage that contains the System State data to the computer that you want to install into the destination domain.</p> <p><b>Note:</b> Symantec recommends that you encrypt the storage. Use caution when transporting it to the location of the destination domain.</p>
Step 3	<p>Inventory and catalog the storage.</p> <p>See <a href="#">“Cataloging a storage device”</a> on page 424.</p>
Step 4	<p>Redirect the restore of the system state backup sets to a temporary location on a volume or directory on the destination computer.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>

**Table 6-3** How to install a new Windows Server domain controller into an existing domain by using a redirected restore (*continued*)

Step	Description
Step 5	<p>Start the domain controller installation by doing the following in the order listed:</p> <ul style="list-style-type: none"> <li>■ On the destination computer, click <b>Start</b>, and then click <b>Run</b>.</li> <li>■ Type <code>dcpromo /adv</code>, and then click <b>OK</b>.</li> <li>■ Click <b>Next</b> when the Active Directory Installation Wizard appears.</li> <li>■ Select <b>Additional domain controller for an existing domain</b>, and then click <b>Next</b>.</li> <li>■ Select <b>From these restored backup files</b>, enter the temporary location to which you redirected the restore of the System State data, and then click <b>Next</b>.</li> <li>■ Complete the Active Directory Installation Wizard by following the prompts on the screen.</li> </ul>
Step 6	Complete the domain controller installation.
Step 7	Restart the computer that has the new domain controller.
Step 8	Delete any remaining system state backup sets that you redirected to the temporary location.

## About restoring media created with other backup software

Backup Exec supports restoring NetWare SMS volume backups to non-SMS volumes. For example, the data that is backed up with Backup Exec for NetWare Servers or Novell’s SBackup can be restored to the Backup Exec server or to another network share.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

## About restoring data from ARCserve tapes

You can restore data from ARCserve tapes.

The following types of data cannot be restored from ARCserve tapes:

- Databases, such as Microsoft SQL and Exchange Server and NetWare Directory Services
- Windows registry
- Interleaved files
- Compressed files
- Encrypted files
- Long filenames and Extended Attributes for OS/2 files
- Long filenames and resource forks for Macintosh files

Storage that contains ARCserve backups can be overwritten; however, backup append jobs are not supported. All Backup Exec storage utility functions can be performed on ARCserve media.

---

**Note:** If the ARCserve backup spans multiple tapes, you must have all the tapes that were included in the ARCserve backup available. Make sure you start both the catalog job and the restore job with the first tape used in the ARCserve backup.

---

See [“Restoring data from ARCserve tapes”](#) on page 240.

See [“About inventorying a storage device”](#) on page 422.

See [“Cataloging a storage device”](#) on page 424.

## Restoring data from ARCserve tapes

You can restore data from ARCserve tapes.

See [“About restoring data from ARCserve tapes”](#) on page 240.

**Table 6-4** Restoring data from ARCserve tapes

Step	Action
Step 1	<p>Catalog and inventory all of the storage from the ARCserve backup.</p> <p>See <a href="#">“About inventorying a storage device”</a> on page 422.</p> <p>During cataloging, Backup Exec reports file formats that it can read. Files that cannot be read do not appear in the catalogs. The media description that appears in the Backup Exec catalog comes from the session description that ARCserve uses.</p> <p>Storage-based catalogs are not supported on storage that is created by other vendors’ backup products. Therefore, cataloging ARCserve storage takes considerably longer than cataloging Backup Exec storage.</p>
Step 2	<p>Restore the selected data to a computer.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p> <p>Due to the naming conventions that ARCserve uses for some computers, it may be necessary to redirect the data that you want to restore to another computer.</p>

## About canceling a restore job

Canceling a restore job while it is in progress results in unusable data and may leave the disk in an unusable state. To avoid canceling a restore job, you can redirect the restore to a noncritical destination. Then, copy the data to a final destination when the job completes successfully.

You should not cancel a System State restore job. Canceling this job can leave the system unusable.

See [“Canceling an active job”](#) on page 252.

## About catalogs

While backing up data, Backup Exec creates a catalog that contains information about the backup sets and about the storage device on which the backup sets are stored. When you select data to restore, Backup Exec uses the catalog information to find the restore selections and the storage devices on which they reside.

When a storage device is fully cataloged, you can do the following:

- View information on all the directories and files that are contained in each backup set.
- Search for files to restore.

Backup Exec fully catalogs each backup job. However, if the catalogs are truncated, only backup set information is listed. You cannot view files or file attributes. The amount of information in the catalog is determined by whether you choose to truncate the catalogs after a specific amount of time.

Catalogs reside on the Backup Exec server and on the storage device to which you sent the backup job.

To restore the data that was backed up by another installation of Backup Exec, you must first run a catalog operation on the storage device on the local Backup Exec server. The catalog for a backup job that was run on one installation of Backup Exec does not exist on another installation of Backup Exec.

See [“Editing global options for catalogs”](#) on page 242.

See [“Cataloging a storage device”](#) on page 424.

See [“About cataloging media that contains encrypted backup sets”](#) on page 391.

## Editing global options for catalogs

You can edit the global options for catalogs to specify the defaults that are best suited for your environment.

See [“About catalogs”](#) on page 242.

### To edit global options for catalogs

- 1 Click the Backup Exec button, click **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, click **Catalog**.
- 3 Select the appropriate options.

See [“Global options for catalogs”](#) on page 243.

- 4 Click **OK**.

## Global options for catalogs

You can change the global defaults that apply to all catalogs.

See [“Editing global options for catalogs”](#) on page 242.

**Table 6-5** Global options for catalogs

Option	Description
<b>Request all media in the sequence for catalog operations</b>	<p>Catalogs the media in tape drives and disk cartridges by starting with the lowest known tape number in the tape family. For example, if you don't have the first tape, the catalog job starts with the second tape. If you uncheck this option, the catalog job begins on the tape that you specify.</p> <p>If you uncheck <b>Request all media in the sequence for catalog operations</b>, then you cannot select the option <b>Use storage-based catalogs</b>.</p>

**Table 6-5** Global options for catalogs (*continued*)

Option	Description
<p><b>Use storage-based catalogs</b></p>	<p>Lets Backup Exec read the catalog information from the storage device.</p> <p>Storage-based catalogs allow quick cataloging of the backup sets that are not included in the Backup Exec server-based catalog. An example is when you want to catalog backup sets that another installation of Backup Exec creates.</p> <p>Storage-based catalogs enable backup sets to be cataloged in minutes, rather than the hours that are required with traditional file-by-file cataloging methods.</p> <p>To create a new catalog by having Backup Exec read each file block, clear this option. You should clear this option only if normal catalog methods are unsuccessful.</p> <p>If you uncheck <b>Request all media in the sequence for catalog operations</b>, then the option <b>Use storage-based catalogs</b> is unavailable.</p> <p><b>Warning:</b> This option must be enabled if you plan to use Simplified Disaster Recovery as part of your disaster recovery plan. If you disable this option, the backup sets that you create for use with SDR cannot be restored during an SDR recovery operation. As a result, SDR cannot recover the failed computer.</p> <p>See “<a href="#">About preparing computers for use with Simplified Disaster Recovery</a>” on page 707.</p>

**Table 6-5** Global options for catalogs (*continued*)

Option	Description
<b>Truncate catalogs after</b>	<p>Retains only the header information and removes all file details and directory details after the specified amount of time. This option reduces the size of the catalogs considerably. After the catalogs have been truncated, the files and directories cannot be restored until you recatalog the storage. See “<a href="#">Cataloging a storage device</a>” on page 424.</p> <p>The last access date is not reset when catalogs are truncated.</p> <p>You can perform a full restore of backup sets from truncated catalogs.</p> <p>This option does not apply to synthetic backup jobs.</p>
<b>Current path</b>	<p>Designates the path where you want to locate the catalogs. This path is the same as the installation path, which by default is \Program Files\Symantec\Backup Exec\Catalogs.</p>
<b>Catalog drive</b>	<p>Designates the volume on which you want to locate the catalog files if disk space is limited on the Backup Exec server.</p>
<b>Catalog path</b>	<p>Designates a path on the volume for the catalog files. If the path does not exist, you are prompted to create the path.</p>



# Job management and monitoring

This chapter includes the following topics:

- [About managing and monitoring active and scheduled jobs](#)
- [About the Job History](#)
- [About error-handling rules for failed or canceled jobs](#)
- [About job status and recovery](#)

## About managing and monitoring active and scheduled jobs

Backup Exec includes features that enable you to manage backup jobs, restore jobs, and storage operation jobs. Active and scheduled backup and restore jobs appear on the **Jobs** list when you select a server on the **Backup and Restore** tab. Storage operation jobs for storage devices appear on the **Jobs** list when you select the details for a storage device on the **Storage** tab. You can monitor your active jobs and scheduled jobs from the Jobs list, which shows the type of jobs, the state and status of the jobs, the schedule, and other details.

You can manage jobs in the **Jobs** list in the following ways:

- Edit scheduled jobs.
- View the job activity details for an active job.
- Delete scheduled jobs.
- Cancel active jobs.
- Change the priority of scheduled jobs.

- Run a scheduled job immediately.
  - Hold a job or the job queue.
  - Run a test of the backup job.
- See [“Editing a single scheduled job”](#) on page 251.
- See [“Editing multiple scheduled jobs”](#) on page 252.
- See [“Viewing job activity details for active jobs”](#) on page 248.
- See [“Deleting scheduled jobs”](#) on page 259.
- See [“Canceling an active job”](#) on page 252.
- See [“Changing the priority for a scheduled job”](#) on page 258.
- See [“Running a scheduled job immediately”](#) on page 258.
- See [“Placing a job on hold”](#) on page 253.
- See [“Placing the job queue on hold”](#) on page 253.
- See [“Running a test job from the Jobs list”](#) on page 259.

## Viewing job activity details for active jobs

When a job is running, you can view details for the job, such as the percent complete, job rate, and byte count.

### To view details for active jobs

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device on which the job is running.
- 2 In the left pane, click **Jobs**.
- 3 Right-click the job, and then click **View Job Activity**.

See [“Job activity options”](#) on page 248.

### Job activity options

When a job is running, you can view details for the job, such as the percent complete, job rate, and byte count.

See [“Viewing job activity details for active jobs”](#) on page 248.

**Table 7-1** Job activity options

Item	Description
<b>Job name</b>	Shows the job name.

**Table 7-1** Job activity options (*continued*)

<b>Item</b>	<b>Description</b>
<b>Job type</b>	Shows the type of job that was submitted for processing.
<b>Job log</b>	Shows the file name of the job log. The job log cannot be viewed until the job has completed. The job log is located in Program Files\Symantec\Backup Exec\Data.
<b>Status</b>	Shows the status of the operation.  See " <a href="#">Active job statuses</a> " on page 254.
<b>Current Operation</b>	Shows the type of operation that is currently in progress (Backup, Catalog, Restore, Verify, etc.).
<b>Created on</b>	Indicates whether the job was created on the central administration server or on the managed Backup Exec server. This option appears only if the Central Admin Server Option (CASO) is installed.
<b>Server name</b>	Shows the name of the Backup Exec server that is processing the job.
<b>Device name</b>	Shows the name of the storage device that is processing the job.  Only data from the first stream displays for multistream jobs.
<b>Source</b>	Shows the name of the media or the share that is being processed.  The icon field to the left of the field name displays either of the following: <ul style="list-style-type: none"> <li>■ A disk drive icon when a backup operation is running.</li> <li>■ A tape drive icon when a restore operation or a verify operation is running.</li> </ul> Only data from the first stream displays for multistream jobs.
<b>Destination</b>	Lists the location where the data is being written.  The icon field to the left of the field name displays either of the following: <ul style="list-style-type: none"> <li>■ A tape device icon when a backup operation is running.</li> <li>■ A disk drive icon when a restore operation is running.</li> </ul> Only data from the first stream displays for multistream jobs.

**Table 7-1** Job activity options (*continued*)

Item	Description
<b>Current directory</b>	<p>Lists the name of the current directory that is being processed.</p> <p>The icon field to the left of the field displays either of the following:</p> <ul style="list-style-type: none"> <li>■ A folder if the active job is a backup or restore operation.</li> <li>■ No icon, if the active job is not a backup or restore operation, but a job such as an Erase or Format operation.</li> </ul> <p>Only data from the first stream displays for multistream jobs.</p>
<b>Current file</b>	<p>Lists the name of the current file that is being processed.</p> <p>The icon field to the left of the field name displays either of the following:</p> <ul style="list-style-type: none"> <li>■ A page, if the active job is a backup or restore operation.</li> <li>■ No icon, if the active job is not a backup or restore operation, but a job such as an Erase or Format operation.</li> </ul> <p>Only data from the first stream displays for multistream jobs.</p>
<b>Delegation status</b>	<p>Indicates the current status of a job that is being delegated from the central administration server to the managed Backup Exec server. This option appears only if the Central Admin Server Option is installed.</p> <p>The following statuses may appear, where &lt;x&gt; is replaced with the name of the managed Backup Exec server:</p> <ul style="list-style-type: none"> <li>■ Preparing to delegate job to &lt;x&gt;</li> <li>■ Delegating job to &lt;x&gt;</li> <li>■ Job has been delegated to &lt;x&gt;</li> <li>■ Job has been received by &lt;x&gt;</li> <li>■ Job is actively running on &lt;x&gt;</li> <li>■ Job has completed on &lt;x&gt;</li> <li>■ Error in delegating job ... re-submitting job to &lt;x&gt;</li> </ul>
<b>Directories</b>	Indicates the number of directories that have processed.
<b>Files</b>	Indicates the number of files that have processed.
<b>Skipped files</b>	Indicates the number of files that were skipped during the operation.
<b>Corrupt files</b>	Indicates the number of corrupt files that were encountered during the operation.
<b>Files in use</b>	Indicates the number of files that were in use during the operation.

**Table 7-1** Job activity options (*continued*)

Item	Description
<b>Job rate</b>	Indicates the number of megabytes that were processed per minute.
<b>Bytes</b>	Indicates the number of bytes that were processed.
<b>Start time</b>	Indicates the time when the operation started.
<b>Elapsed time</b>	Indicates the length of time that has elapsed since the operation started.
<b>Percent complete</b>	Indicates the percentage of the job that has completed. This option appears only if <b>Display progress indicators for backup jobs</b> is selected as a preference.
<b>Estimated total bytes</b>	Indicates the total number of bytes that is estimated for the backup job during a prescan. This option appears only if <b>Display progress indicators for backup jobs</b> is selected as a preference.
<b>Estimated time remaining</b>	Indicates the estimated time it will take for the job to complete. This option appears only if <b>Display progress indicators for backup jobs</b> is selected as a preference.
<b>Note</b>	Indicates that the option to show job estimates is not selected. This option appears only if <b>Display progress indicators for backup jobs</b> is selected as a preference.

See [“Changing the default preferences”](#) on page 465.

## Editing a single scheduled job

You can edit the properties for a single scheduled job..

### To edit a single scheduled job

- 1** On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device on which the job is scheduled.
- 2** In the left pane, click **Jobs**.
- 3** Right-click the job, and then click **Edit**.
- 4** Change the appropriate settings, and then click **OK**.

See [“Editing multiple scheduled jobs”](#) on page 252.

## Editing multiple scheduled jobs

When you edit multiple scheduled jobs, the changes are applied to all of the selected jobs.

### To edit multiple scheduled jobs

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device on which the job is scheduled.
- 2 In the left pane, click **Jobs**.
- 3 Ctrl + click the jobs that you want to edit.
- 4 Right-click one of the highlighted jobs.
- 5 Click **Edit Backups**.
- 6 On the **Backup Job Selection** dialog box, check the check boxes for the jobs you want to edit, and then click **OK**.
- 7 Do one or both of the following:
  - To change settings, click **Edit**, and then change the appropriate settings.
  - To add a stage, click **Add Stage**, select the type of stage that you want to add, and then select **Edit** to edit the settings for that stage.
- 8 Click **OK**.

See [“Editing a single scheduled job”](#) on page 251.

## Canceling an active job

You can cancel a job that is in progress. If the job is scheduled, it runs again at the next scheduled time.

It may take several minutes for a job to cancel. While Backup Exec processes the cancellation of a job, the Cancel Pending status appears in the Job Status column.

### To cancel an active job

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is running.
- 2 In the left pane, click **Jobs**.
- 3 Right-click the active job that you want to cancel, and then click **Cancel**.
- 4 Click **Yes** to confirm the cancellation of the job.

## Placing a job on hold

Active and scheduled jobs can be placed on hold. When you place an active job on hold, the job continues to run until it is complete. However, the next scheduled occurrence of that job is placed on hold.

### To place a job on hold

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is running or is scheduled to run.

- 2 In the left pane, click **Jobs**.

To select multiple jobs, select a job, and then press the <Ctrl> or <Shift> keys while you click other jobs that you want to select. This allows you to hold more than one job at a time, as long as the states of the jobs are the same.

- 3 Right-click the job that you want to hold, and then click **Hold**.

See [“Removing the hold on a job”](#) on page 253.

## Removing the hold on a job

You can remove the hold on a scheduled job at any time.

### To remove the hold on a scheduled job

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is on hold.

- 2 In the left pane, click **Jobs**.

- 3 Right-click the job that you want to remove from the hold, and then click **Hold**.

See [“Placing a job on hold”](#) on page 253.

## Placing the job queue on hold

You can place the entire job queue on hold to make changes to your environment. The server is paused to place the job queue on hold. When the job queue is on hold, only active jobs continue to run unless you choose to cancel them. No other jobs can run until the job queue is taken off hold.

### To place the job queue on hold

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is running or scheduled to run.

- 2 In the left pane, click **Jobs**.

- 3 In the **Jobs** group, click **Hold**, and then click **Hold Job Queue**.

- 4 Click **Yes**.
- 5 If active jobs are running, select the active jobs that you want to cancel, and then click **OK**.

See [“Removing the hold on the job queue”](#) on page 254.

## Removing the hold on the job queue

When you remove the hold on the job queue, the server is unpaused and jobs then run according to the schedule.

### To remove the hold on the job queue

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job queue is on hold.
- 2 In the left pane, click **Jobs**.
- 3 In the **Jobs** group, click **Hold**, and then click **Hold Job Queue**.

See [“Placing the job queue on hold”](#) on page 253.

## Active job statuses

Possible statuses for an active job include the following:

**Table 7-2** Active job statuses

Item	Description
Running	The operation is underway.
Queued	The job has been initiated, but Backup Exec is actively looking for a suitable drive or media.
Cancel Pending	Backup Exec cannot process the Cancel request immediately. This status is displayed until the job is actually canceled. The job is then displayed in job history with a status of Canceled.
Loading Media	The media is being loaded and positioned on the target device.

**Table 7-2** Active job statuses (*continued*)

Item	Description
Pre-processing	<p>This status can indicate any or all of the following:</p> <ul style="list-style-type: none"> <li>■ Backup Exec is calculating the amount of data that will be backed up, if the <b>Display progress indicators for backup jobs</b> option is enabled in the Preferences section of Backup Exec settings. See <a href="#">“Changing the default preferences”</a> on page 465.</li> <li>■ Backup Exec is waiting for a pre- or post-command to complete.</li> <li>■ Backup Exec is retrieving the set maps and is positioning the tape to the append point location for an append job.</li> </ul>
Snapshot processing	Backup Exec is processing a snapshot operation.
Device Paused	<p>The device that the job was sent to is paused.</p> <p>See <a href="#">“Pausing and unpausing a storage device”</a> on page 425.</p>
Server Paused	<p>The Backup Exec server is paused.</p> <p>See <a href="#">“Pausing a managed Backup Exec server”</a> on page 1037.</p>
Stalled	<p>The Backup Exec services have become unresponsive.</p> <p>See <a href="#">“Setting job status and recovery options”</a> on page 277.</p>
Media Request	You must insert media for the job to continue.
Communication Stalled	<p>Communications between the managed Backup Exec server and the central administration server have not occurred within the configured time threshold.</p> <p>See <a href="#">“Enabling communications between the managed Backup Exec server and the central administration server”</a> on page 1025.</p>
No Communication	<p>No communication about jobs is being received at the central administration server from the managed Backup Exec server. The configured time threshold has been reached.</p> <p>See <a href="#">“Enabling communications between the managed Backup Exec server and the central administration server”</a> on page 1025.</p>
Consistency check	Backup Exec is running a consistency check of the databases before backup.
Updating Catalogs	Backup Exec is updating the catalog information.

See [“Scheduled job statuses”](#) on page 256.

See [“Completed job statuses”](#) on page 263.

## Scheduled job statuses

Possible statuses for scheduled jobs are listed in the following table:

**Table 7-3** Scheduled job statuses

Scheduled job status	Description
Invalid Schedule	The scheduled job will not run because of a scheduling issue.  See <a href="#">“Setting global schedule options”</a> on page 457.
Not in time window	The job was ready to be sent for processing, but the time window for the job closed.  See <a href="#">“Setting global schedule options”</a> on page 457.
On Hold	The job has been placed on hold.
Queued	A temporary state that displays when Backup Exec is applying an error-handling rule that is enabled to retry the job.  See <a href="#">“Custom error-handling rule for recovered jobs”</a> on page 275.

**Table 7-3** Scheduled job statuses (*continued*)

Scheduled job status	Description
Ready	<p>The job is ready to run, but cannot for one of the following reasons:</p> <ul style="list-style-type: none"> <li>■ Internal error. No devices are available, but the cause is unknown.</li> <li>■ Invalid job. The job type is unknown; there may be an internal error or the database is corrupted.</li> <li>■ Invalid target. This type of storage device no longer exists.</li> <li>■ Backup Exec server not available.</li> <li>■ No license for option name. A license must be purchased and installed on the Backup Exec server.</li> <li>■ No Backup Exec servers are available.</li> <li>■ No Backup Exec servers are available in Backup Exec server pool.</li> <li>■ Specified destination storage device pool is empty.</li> <li>■ Specified destination device is not in Backup Exec server pool.</li> <li>■ Specified destination device not on local Backup Exec server.</li> <li>■ Specified destination storage device pool on local Backup Exec server is empty.</li> <li>■ The destination storage device cannot be a storage pool.</li> <li>■ The destination storage device cannot be a Backup Exec server.</li> <li>■ Another job is running in the system that is blocking execution of this job. This job will run after the other job completes.</li> <li>■ Invalid input.</li> <li>■ Incompatible Resumes.</li> <li>■ No server license available.</li> <li>■ No multi-server license available.</li> <li>■ No Windows license.</li> <li>■ No Windows server.</li> <li>■ Need local Backup Exec server.</li> <li>■ Local server is not a Backup Exec server.</li> <li>■ No idle storage devices are available.</li> <li>■ No eligible storage devices within the storage pool are available.</li> <li>■ Blocked by an active, linked duplicate backup sets job.</li> </ul>

**Table 7-3** Scheduled job statuses (*continued*)

Scheduled job status	Description
Scheduled	The job is scheduled to run in the future. The scheduled jobs that are linked to another job, such as a job to duplicate backup sets, will not display a scheduled job status.
Server Paused	The job is ready, but the Backup Exec server has been paused. No jobs are dispatched while the Backup Exec server is paused.  See “ <a href="#">Pausing a managed Backup Exec server</a> ” on page 1037.
To Be Scheduled	A state that the scheduled job transitions through as it is being sent for processing.

See “[Active job statuses](#)” on page 254.

See “[Completed job statuses](#)” on page 263.

## Running a scheduled job immediately

You can run a scheduled job immediately. The job will also run on the next scheduled occurrence.

### To run a scheduled job immediately

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is scheduled to run.
- 2 In the left pane, click **Jobs**.
- 3 Right-click the scheduled job that you want to run, and then click **Run Now**.

## Changing the priority for a scheduled job

The priority determines the order that jobs run. If two jobs are scheduled to run at the same time, the priority you set determines which job runs first. The priority is changed for all occurrences of the scheduled job.

The priority of the job is displayed in the **Priority** column in the **Jobs** list.

### To change the priority for a scheduled job

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is scheduled to run.
- 2 In the left pane, click **Jobs**.

- 3 Right-click the scheduled job, and then click **Change Priority**.
- 4 Select the new priority.

## Deleting scheduled jobs

Deleting a scheduled job removes all scheduled occurrences of the job. To delete only the occurrence of a scheduled job on a specific date, you can edit the schedule to remove that date.

---

**Note:** If a backup definition includes more than one type of job, then the backup definition must be deleted instead of the individual jobs within the definition.

---

### To delete a scheduled job

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job is scheduled to run.
- 2 In the left pane, click **Jobs**.
- 3 Right-click the scheduled job, and then click **Delete**.
- 4 Click **Yes**.

## Running a test job from the Jobs list

Test run jobs attempt to determine if a job could possibly fail when you run it. When you run a test job, no data is backed up. Instead, Backup Exec checks your storage capacity, credentials, and media to find potential errors.

---

**Note:** If a backup definition includes more than one type of job, then the test run job must be run on the backup definition instead of the individual jobs within the definition.

---

### To run a test job from the Jobs list

- 1 On the **Backup and Restore** tab, double-click the server that contains the job you want to test.
- 2 In the left pane, click **Jobs**.
- 3 Right-click the job that you want to test, and then click **Test Run**.
- 4 Click **Yes** to confirm that you want to run the test job now.

See [“About test run jobs”](#) on page 222.

## About the Job History

The Job History displays a list of completed and failed backup, restore, and storage operation jobs. The Job History appears when you select a server on the **Backup and Restore** tab, and when you select a storage device on the **Storage** tab.

From the Job History, you can do any of the following:

- View the job log.
- Delete a job.
- Rerun a job.
- Duplicate the data from a completed backup job.
- Verify a backup job.
- Enable error-handling rules for a failed job.

See [“Running a job from the Job History”](#) on page 263.

See [“Viewing the job log ”](#) on page 264.

See [“Deleting a job from the Job History”](#) on page 262.

See [“Enabling an error-handling rule for a failed job”](#) on page 274.

See [“Duplicating job history”](#) on page 220.

See [“Verifying job history”](#) on page 223.

## Viewing the history of a job

The job history shows statistics for all occurrences of a job.

### To view the history of a job

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, select **Jobs** or **Job History**
- 3 Select the job for which you want to view history.
- 4 In the **Job History** group, click **View Job History**.

See [“Job History options”](#) on page 260.

### Job History options

The job history shows statistics for all occurrences of a job.

See [“Viewing the history of a job”](#) on page 260.

Table 7-4 Job History options

Item	Description
<b>Name</b>	Shows the name of the job.
<b>Device</b>	Shows the name of the storage device where the job ran.
<b>Job Type</b>	Shows the type of job.
<b>Job Status</b>	Indicates the status of the job, such as successful or failed.
<b>Percent Complete</b>	Indicates the amount of the job that completed.
<b>Start Time</b>	Indicates the date and time when the job started.
<b>End Time</b>	Indicates the date and time when the job ended.
<b>Successful</b>	Indicates the number of jobs that completed without errors.
<b>Completed with Exceptions</b>	Indicates the number of jobs that completed, but had exceptions. For example, skipped, corrupted, or in-use files were encountered during the job.
<b>Failed</b>	Indicates the number of jobs that ran, but had one or more significant errors occur. The job log should indicate what caused the errors.
<b>Canceled</b>	Indicates the number of jobs that the administrator canceled.
<b>Missed</b>	Indicates the number of jobs that did not run during the scheduled time window.
<b>Recovered</b>	Indicates the number of jobs that were active when the status of the managed Backup Exec server changed from Communication Stalled to No Communication. The custom error-handling rule for Recovered Jobs was applied to the job.

**Table 7-4** Job History options (*continued*)

Item	Description
<b>Resumed</b>	Indicates the number of jobs that ran in a cluster environment and were active on one computer and then resumed on another computer.
<b>Combined Elapsed Time</b>	Indicates the total amount of time that was required to process all occurrences of the job.
<b>Average Elapsed Time</b>	Indicates the average amount of time that was required to process all occurrences of the job.
<b>Shortest Elapsed Time</b>	Indicates the shortest job processing time.
<b>Longest Elapsed Time</b>	Indicates the longest job processing time.

## Deleting a job from the Job History

You can delete a job from the **Job History**, or have Backup Exec automatically delete the job history using database maintenance.

If you delete a job, it is removed from the computer and cannot be recovered.

### To delete a job from the Job History

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, click **Job History**.
- 3 Right-click the job that you want to delete, and then click **Delete**.

You can select multiple jobs by selecting a job, and then pressing the <Ctrl> or <Shift> keys while you click other jobs that you want to select. This allows you to perform tasks such as Delete on more than one job at a time, as long as the jobs are of similar type.

You can delete up to 2500 jobs from the Job History. If you attempt to delete more than 2500 jobs, you are prompted to continue with the deletion.

- 4 Click **Yes**.

See “[About the Job History](#)” on page 260.

## Running a job from the Job History

After a job runs, the job moves to the Job History. You can run a completed job again from the Job History.

### To run a job from the Job History

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, click **Job History**.
- 3 Right-click the job that you want to run, and then click **Run Now**.

See “[About the Job History](#)” on page 260.

## Completed job statuses

The following job completion statuses may appear for jobs that were completed:

**Table 7-5** Job completion status

Status	Description
Successful	The job was completed without errors.
Completed with exceptions	The job completed, but some files were in use, skipped, or corrupted.
Failed over	The job ran in a cluster environment and was active on one computer, and then the cluster performed a failover and the job was restarted on another computer in the cluster. Two separate sets of job history are available when a job is failed over. The first job history includes the Failed over status and the second job history includes the status that is appropriate for the completed job.
Resumed	The status is the same as the failed over status, however the <b>Enable checkpoint restart</b> option was selected.
Canceled	The administrator terminated the operation as it was running.
Canceled, timed out	The <b>Cancel the job if it is still running x hours after its scheduled start</b> feature in the Frequency - Schedule property was enabled and the job was not completed within the specified timeframe.

**Table 7-5** Job completion status (*continued*)

Status	Description
Failed	<p>The operation took place, but one or more significant errors occurred. The job log should indicate what caused the errors so that you can decide if you want to run the job again. For example, if a job failure occurred due to a lost connection during job processing, you could choose to resubmit the job when the connection is restored.</p> <p>If a drive loses power during a backup operation, you should restart the backup job using a different tape. You can restore the data that was written to the tape up to the point of the power loss, but you should not reuse the tape for subsequent backup operations.</p> <p>A failed job has an error message in the Errors section of the job log with a link to the Symantec Technical Support Web site.</p> <p>A job may fail for the following reasons:</p> <ul style="list-style-type: none"> <li>■ The storage device that was selected the job was not available when the job ran.</li> <li>■ The logon account that was used in the backup job is incorrect. Verify that the logon account information is valid for the resource being backed up.</li> <li>■ A problem occurred with the storage device when the job was run.</li> <li>■ The computer being backed up was shut down before or during the backup job.</li> </ul>
Recovered	<p>The job was active when the status of the managed Backup Exec server was changed from Communication Stalled to No Communication. The custom error-handling rule for Recovered Jobs was applied to the job.</p>
Missed	<p>The job did not run during the scheduled time window. The job is rescheduled to run based on the time window that you configured.</p>

## Viewing the job log

You can view detailed job-related properties for each job that has been processed. You can save a copy of the job log to a location of your choice or you can print the job log.

**To view the job log**

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, click **Job History**.
- 3 Right-click the job, and then select **View Job Log**.  
 See “[Job Log properties for completed jobs](#)” on page 265.

**Job Log properties for completed jobs**

The **Job Log** provides job and file statistics. Most job logs display in HTML format. However, some logs may display in text.

See “[Viewing the job log](#)” on page 264.

**Table 7-6** Job Log properties for completed jobs

Item	Description
<b>Job Information</b>	Displays the job server, job name, the date and time the job started, the type of job, and the job log name.
<b>Device and Media Information</b>	Displays the drive name, media label, the overwrite protection and append periods, and the media set that this job was targeted to.
<b>Storage operation Job Information</b>	Displays information about the slot, barcode, media label, status, and device that the storage operation job was processed on.
<b>Job Operation</b>	Displays information about the type of job operation, such as a backup operation or a verify operation. It also displays information about the backup sets for the job.
<b>Job Completion Status</b>	Displays the job end time, completion status, error codes, error description, and error category. The job completion section is green, orange, or red, depending on the job status.  See “ <a href="#">Completed job statuses</a> ” on page 263.
<b>Errors</b>	Displays a detailed description of the errors that were encountered during job processing. The errors are grouped by set and labeled. The label includes the operation and the destination resource name for that set. The error section is red in the job log.  To locate where the error occurred in the Backup Set Detail Information, click the error text. Then, if additional information on an error is available, click the underlined error code number to go to the Symantec Technical Support Web site.

**Table 7-6** Job Log properties for completed jobs (*continued*)

Item	Description
<b>Exceptions</b>	Displays a detailed description of the minor errors that were encountered during job processing. The exceptions section is orange in the job log.
<b>NDMP Log</b>	Provides details about the NDMP environment variables that were selected for an operation, and about duplicate sets for NDMP.

## Linking from the job log to the Symantec Technical Support Web site

Errors that are reported in the job log each have a unique code, called a Unique Message Identifier (UMI). These codes contain hyperlinks that you can click to go to the Symantec Technical Support Web site. From the Web site, you can access technical notes and troubleshooting tips that are related to a specific message. UMI codes establish unique message codes across all Symantec products.

Some alerts also contain a UMI. For example, if a Warning alert appears when a job fails, the alert includes the UMI code.

You can create or enable an error-handling rule for errors. These rules let you set options to retry or stop a job when the error occurs.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

### To link from the job log to the Symantec Technical Support Web site

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, click **Job History**.
- 3 Right-click a job, and then select **View Job Log**
- 4 Scroll to the Job Completion Status section.
- 5 Click the UMI code, which appears as a blue hyperlink.

## About using job logs with vertical applications

The Backup Exec Administration Console provides a view of the job logs in HTML format. If necessary, you can convert the job logs to a text format for use with vertical applications.

To convert a job log file to a text format, load the Backup Exec Management Command Line Interface, and then type the following at a command prompt:

```
Get-BEJobLog "pathname\job log filename"
```

For example, to display the job log C:\program files\Symantec\Backup Exec\Data\bex00001.xml in text format to the command prompt, you would type:

```
Get-BEJobLog "C:\program files\Symantec\Backup Exec\Data\bex00001.xml"
```

To redirect the job log to a file, you would type one of the following:

```
Get-BEJobLog "C:\program files\Symantec\Backup Exec\Data\bex00001.xml" > bex00001.txt
```

See [“Viewing the job log”](#) on page 264.

## Finding text in the job log

You can search for specific text in the job log.

### To find text in the job log

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the server or the storage device where the job ran.
- 2 In the left pane, click **Job History**.
- 3 Right-click the job, and then click **View Job Log**.
- 4 Click **Find**.
- 5 Enter the text that you want to find.  
See [“Find options”](#) on page 267.
- 6 Click **Next** to find the next occurrence of the text.

### Find options

You can search for specific text in the job history or the job properties log.

See [“Finding text in the job log”](#) on page 267.

**Table 7-7** Find options

Item	Description
<b>Find</b>	Indicates the text that you want to find.

**Table 7-7** Find options (*continued*)

Item	Description
<b>Match whole word only</b>	Indicates that you want to search for the whole word you typed. If you do not select this option, Backup Exec finds the text that includes part of the word. For example, if you search for the word "file" and do not select this option, Backup Exec finds all occurrences of "file", "files", "filed", and any other words that contain "file". If you do select this option, Backup Exec finds only the occurrences of "file".
<b>Match case</b>	Indicates that you want to use the exact capitalization for the word you typed. For example, if you search for the word "File" and select this option, Backup Exec finds all occurrences of "File", but does not find any occurrences of "file".
<b>Highlight all matches</b>	Highlights the text that matches the search criteria.

## Configuring default job log options

You can configure default options for job logs that specify the amount of detail you want to include in the completed job log. For the jobs that produce large job logs, you may want to reduce the amount of detail in the job log. The size of the job log increases proportionally to the level of detail that is configured for the job log.

### To configure default job log options

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, click **Job Logs**.
- 3 Select the appropriate options.

See “[Default job log options](#)” on page 268.

### Default job log options

You can configure default options for job logs that specify the amount of detail you want to include in the completed job log.

See “Configuring default job log options” on page 268.

**Table 7-8** Default job log options

<b>Item</b>	<b>Description</b>
<b>Summary information only</b>	<p>Includes the following information in the job log:</p> <ul style="list-style-type: none"> <li>■ Job name</li> <li>■ Job type</li> <li>■ Job log name</li> <li>■ Backup Exec server name</li> <li>■ Storage device</li> <li>■ Starting date and time</li> <li>■ Errors encountered</li> <li>■ Ending date and time</li> <li>■ Completion statistics</li> </ul> <p>This option also includes the name of files that were skipped, the name of the media set, the backup type and results of the verify operation if one was performed.</p>
<b>Summary information and directories processed</b>	<p>Includes summary information and a list of all processed subdirectories in the job log.</p>
<b>Summary information, directories, and files processed</b>	<p>Includes summary information, processed subdirectories, and a list of all the file names that were processed in the job log.</p>
<b>Summary information, directories, files and file details</b>	<p>Includes Summary information, processed subdirectories, a list of all the file names and their attributes in the job log.</p> <p>This option increases the job log sizes significantly.</p>
<b>Prefix for the job log file name</b>	<p>Indicates a prefix to add to the job logs that are processed. The default prefix is BEX.</p> <p>The job log file name consists of Prefix_ServerName_Count. Prefix is the label that you enter in this field, ServerName is the name of the Backup Exec server that ran the job, and Count is the number of job logs that this job has produced.</p>
<b>Attach job logs as html</b>	<p>Attaches the job logs in an HTML format when an email notification is sent.</p>
<b>Attach job logs as text</b>	<p>Attaches the job logs in a text format when an email notification is sent.</p>
<b>Job log path</b>	<p>Shows the current location of the job log. To change the path you can use BE Utility.</p>

## About error-handling rules for failed or canceled jobs

You can enable default rules or create custom rules to set retry options and final job disposition for failed or canceled jobs. Retry options let you specify how often to retry a job if it fails and the time to wait between retry attempts. The final job disposition lets you either place the job on hold until you can fix the error, or reschedule the job for its next scheduled service.

Each default error-handling rule applies to one category of errors, such as Network Errors or Security Errors. Default error-handling rules are disabled by default, so you must edit a rule and enable the rules that you want to use. You cannot delete default error-handling rules, add specific error codes to a category, or add new error categories. Before the error-handling rules will apply, the final error code must be in an error category that is associated with a rule, and the rule must be enabled.

To apply an error-handling rule for a specific error code that is in an error category, you can create a custom error-handling rule. You can select up to 28 error codes in an error category that a custom error-handling rule can apply to. You can also add an error code to an existing custom rule.

A custom error-handling rule named "Recovered Jobs" is created when Backup Exec is installed and is enabled by default. This rule applies retry options and a final job disposition to jobs that fail and that are not scheduled to run again.

See ["Creating a custom error-handling rule"](#) on page 270.

If both a custom error-handling rule and a default error-handling rule apply to a failed job, the settings in the custom rule are applied to the job.

---

**Note:** If the server on which Backup Exec is installed is in a cluster environment, the Cluster Failover error-handling rule is displayed on the list of error-handling rules. This rule is enabled by default.

---

See ["About the cluster failover error-handling rule"](#) on page 276.

## Creating a custom error-handling rule

You can create custom rules to set retry options and final job disposition for failed or canceled jobs.

See ["About error-handling rules for failed or canceled jobs"](#) on page 270.

**To create a custom error-handling rule**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Error-Handling Rules**.
- 2 Click **New**.
- 3 Complete the items in the **Error-Handling Rule Settings** dialog box, and then click **OK**.

See “” on page 273.

See “[Error-Handling Rule Settings options](#)” on page 271.

See “[Custom error-handling rule for recovered jobs](#)” on page 275.

See “[About the cluster failover error-handling rule](#)” on page 276.

**Error-Handling Rule Settings options**

You can create custom rules to set retry options and final job disposition for failed or canceled jobs. You can also edit existing rules.

See “[Creating a custom error-handling rule](#)” on page 270.

**Table 7-9** Error-Handling Rule Settings options

Item	Description
<b>Enable error-handling rule</b>	Enables or disables the error-handling rule. This check box must be selected before you can set the retry options and the final job disposition options.
<b>Name</b>	Indicates the name for the error-handling rule. To add or update a custom error-handling rule, you must enter a rule name.
<b>Final job status</b>	Indicates the status for the job that will activate the rule. The job status can be viewed, but not modified.  The following statuses are available: <ul style="list-style-type: none"> <li>■ Error</li> <li>■ Canceled</li> <li>■ Failed</li> </ul>

**Table 7-9** Error-Handling Rule Settings options (*continued*)

Item	Description
<b>Error category</b>	<p>Indicates the category of error for which the rule will be applied.</p> <p>If you are editing a default or custom error-handling rule, the error category can be viewed, but not modified.</p> <p>If you are creating a custom error-handling rule, you must select an error category that contains the errors to apply this rule to.</p> <p>Available error categories include the following:</p> <ul style="list-style-type: none"> <li>■ Other</li> <li>■ Network</li> <li>■ Server</li> <li>■ Resource</li> <li>■ Security</li> <li>■ Backup Device</li> <li>■ Backup Media</li> <li>■ Job</li> <li>■ System</li> <li>■ Dispatch</li> </ul>
<b>Available errors</b>	<p>Lists the error codes that are not associated with a custom error-handling rule. This field does not appear if you are editing a default error-handling rule.</p> <p>If you are creating or editing a custom error-handling rule, you must select the check box of the error code that you want this rule to apply to. You can select up to 28 error codes.</p> <p>To change the list of available errors, select a different error category.</p>
<b>Retry job</b>	Allows Backup Exec to retry the job.
<b>Maximum retries</b>	Indicates the number of times you want the job retried. The maximum number of times the job can be retried is 99.
<b>Retry interval</b>	Indicates the number of minutes to wait before the job is retried. The maximum number of minutes is 1440.
<b>Place job on hold until error condition has been manually cleared</b>	Places the job on hold until you can manually clear the error. After you clear the error, you must remove the hold for the job.

**Table 7-9** Error-Handling Rule Settings options (*continued*)

Item	Description
<b>Reschedule for its next scheduled service</b>	Runs the job at the next scheduled occurrence.
<b>Notes</b>	Shows any miscellaneous information for the error-handling rule.

You can enable default rules or create custom rules to set retry options and final job disposition for failed or canceled jobs.

**Table 7-10** Error-Handling Rules options

Item	Description
<b>Name</b>	Indicates the name of the error-handling rule.
<b>Type</b>	Indicates the type of rule, either Default or Custom.  A default rule is a predefined default error-handling rule for a category of errors. You cannot delete default rules and you cannot modify default rules to include specific error codes in a category.  A custom rule is an error-handling rule that you can create for a specific error code or codes in an error category.
<b>Job Status</b>	Indicates the status of the job that activates the rule.  The status can be Error, Canceled, or Failed.
<b>Error Category</b>	Indicates the category of error codes that the rule applies to.
<b>Enabled</b>	Indicates whether the rule is enabled or disabled.
<b>New</b>	Enables you to create a new error-handling rule.
<b>Edit</b>	Enables you to edit an existing error-handling rule.
<b>Delete</b>	Enables you to delete an error-handling rule.

See [“Creating a custom error-handling rule”](#) on page 270.

## Enabling or disabling error-handling rules

Follow these steps to enable or disable specific error-handling rules.

### To enable error-handling rules

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Error-Handling Rules**.
- 2 Select the rule that you want to enable, and then click **Edit**.
- 3 Do one of the following:
  - To enable the rule, check **Enable error-handling rule**.
  - To disable the rule, clear the **Enable error-handling rule** check boxClick **OK**.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

## Deleting a custom error-handling rule

A custom error-handling rule can be deleted at any time. A default error-handling rule cannot be deleted.

### To delete a custom error-handling rule

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Error-Handling Rules**.
- 2 Select the custom rule that you want to delete, and then click **Delete**.
- 3 Click **Yes** to confirm that you want to delete the rule.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

## Enabling an error-handling rule for a failed job

You can create custom rules to set retry options and final job disposition for failed jobs.

### Enabling an error-handling rule for a failed job

- 1 On the **Backup and Restore** tab or the **Storage** tab, on the left, select **Job History**.
- 2 Right-click the failed job, and then select **Error Handling**.

- 3 Check the **Enable error-handling rule** check box.
- 4 Complete the remaining options for this rule.  
 See [“Error-Handling Rule Settings options”](#) on page 271.

## Custom error-handling rule for recovered jobs

Backup Exec includes a custom error-handling rule called "Recovered Jobs" to recover the jobs that failed with specific errors. This rule is created when Backup Exec is installed, and is enabled by default.

The retry options for this rule are to retry the job twice, with an interval of five minutes between the retry attempts. The final job disposition is to place the job on hold until you have manually cleared the error condition.

The following table describes the error codes that are selected by default for the Recovered Jobs custom error-handling rule.

**Table 7-11** Error codes for recovered jobs custom error-handling rule

Error code	Description
0xE00081D9 E_JOB_ENGINE_DEAD	The displayed error message is:  The Backup Exec job engine system service is not responding.
0xE0008820 E_JOB_LOCAL RECOVERNORMAL	The displayed error message is:  The local job has been recovered. No user action is required.
0xE000881F E_JOB_REMOTE RECOVERNORMAL	The displayed error message is:  The remote job has been recovered. No user action is required.
0xE0008821 E_JOB_STARTUP RECOVERY	The displayed error message is:  Job was recovered as a result of Backup Exec RPC service starting. No user action is required.

**Note:** If the Central Admin Server Option is installed, additional error codes are selected.

- See [“About error-handling rules for failed or canceled jobs”](#) on page 270.  
 See [“About the cluster failover error-handling rule”](#) on page 276.

## About the cluster failover error-handling rule

If the server on which Backup Exec is installed is in a cluster environment, the cluster failover error-handling rule is displayed on the list of error-handling rules. This rule is enabled by default.

You cannot configure any options for this rule. You can only enable or disable the cluster failover error-handling rule.

The cluster failover error-handling rule and the **Enable checkpoint restart** option in **Advanced Open File** backup options work together to enable you to resume jobs from the point of failover. The **Enable checkpoint restart** option is dependent on the cluster failover error-handling rule; if you disable the rule, the option is automatically disabled to match the rule's setting.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

## About job status and recovery

If the Backup Exec services become unresponsive or jobs no longer run, you can set the threshold at which Backup Exec changes the status of active jobs to stalled. You can also set the threshold at which Backup Exec fails the jobs that were stalled, and then recovers them.

By lowering the amount of time before Backup Exec reaches the threshold for changing a job's status to stalled, you can receive an earlier notification that jobs have stalled. A shorter time between the stalled and recovered thresholds also allows Backup Exec to fail and then recover the stalled jobs earlier. However, setting the thresholds too low may force a job to be recovered when it is not necessary.

Backup Exec recovers the jobs by using the custom error-handling rule named Recovered Jobs. This custom error-handling rule is created and enabled when Backup Exec is installed, and specifies that stalled, failed, and recovered jobs are retried two times, with an interval of five minutes between the retries.

Jobs that are stalled and then failed and recovered by Backup Exec because of unresponsive Backup Exec services are displayed differently in Backup Exec than the jobs that fail because of errors in normal daily activities. The stalled/failed/recovered jobs are not indicated in red text in the job history as other failed jobs are. Instead, these jobs are displayed in gray text with a job status of **Recovered**.

In the job history, the error category is listed as Job Errors. The job history indicates the type of internal communication error that occurred and that the job was recovered. Based on the type of error that occurred, a log file may or may not be associated with the recovered job.

See “[Setting job status and recovery options](#)” on page 277.

See “[About error-handling rules for failed or canceled jobs](#)” on page 270.

## Setting job status and recovery options

If the Backup Exec services become unresponsive or jobs no longer run, you can set the threshold at which Backup Exec changes the status of active jobs to stalled. You can also set the threshold at which Backup Exec fails the jobs that were stalled, and then recovers them.

See “[About job status and recovery](#)” on page 276.

### To set job status and recovery options

- 1 Click the Backup Exec button, click **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, click **Job Status and Recovery**.
- 3 Set the thresholds for stalled and recovered jobs, and then click **OK**.

See “[Job status and recovery options](#) ” on page 277.

### Job status and recovery options

If the Backup Exec services become unresponsive or jobs no longer run, you can set the threshold at which Backup Exec changes the status of active jobs to **Stalled**. You can also set the threshold at which Backup Exec fails the jobs that were stalled, and then recovers them.

See “[Setting job status and recovery options](#)” on page 277.

**Table 7-12** Job status and recovery options

Item	Description
<b>Stalled</b>	Designates the amount of time you want to wait before Backup Exec changes an unresponsive job's status to Stalled.
<b>Recovered</b>	Designates the amount of time you want to wait before Backup Exec fails jobs that stalled and then recovers them. A custom error-handling rule named Recovered Jobs is applied to recovered jobs. If this rule is disabled, then any other error-handling rules that have been enabled will apply to the recovered jobs. If no error-handling rules apply to the job, then the job fails.



# Alerts and notifications

This chapter includes the following topics:

- [About alerts](#)
- [Viewing active alerts and alert history on the Home tab](#)
- [Viewing the alert history for a server or a storage device](#)
- [Filtering alerts](#)
- [Viewing the job log from an alert](#)
- [Responding to active alerts](#)
- [Clearing all informational alerts manually](#)
- [Configuring alert categories](#)
- [About notifications for alerts](#)
- [About managing recipients for alert notifications](#)
- [Sending a notification when a job completes](#)
- [About SNMP notification](#)

## About alerts

An alert is any event or condition in Backup Exec that is important enough to display a message or require a response from you. Backup Exec includes many alert categories and four alert types. Alert categories are events or conditions that cause alerts. Alert categories encompass many circumstances or problems that affect the system, jobs, media, or storage sources. Each alert category can include one or more events that generate an alert. For example, a Job Failed error may

occur for many reasons. The alert types can help you to determine which alerts need immediate attention and which alerts require a response.

The following alert types are used in Backup Exec:

**Table 8-1** Alert types

Item	Description
Attention required	Indicates the issues that require a response before the job or operation can continue.
Error	Indicates the issues that affect job processing or the integrity of your backup. These alerts cannot be disabled and cannot be configured to be cleared automatically. You must respond to them manually.
Warning	Indicates the conditions that may or may not cause jobs to fail. You should monitor the conditions and take actions to resolve them.
Informational	Provides status messages for the conditions that you might want to know about.

By default, most alerts are enabled, which means that they appear in the **Active Alerts** pane. You can disable attention required alerts, warning alerts, and informational alerts by editing alert category properties. However, alerts for errors cannot be disabled. You can filter the alerts so that only specific types of alerts appear.

See [“Configuring alert categories”](#) on page 286.

From the **Home** tab, you can view all active alerts or filter the alerts to view only specific alert types or alerts that occurred on certain dates. On the **Backup and Restore** tab, when you double-click a server, you can see the active alerts that are specific to that server. Similarly, on the **Storage** tab, when you double-click a type of storage, you can see the active alerts that are specific to that storage device.

Alerts remain in the **Active Alerts** pane until they receive a response. You can respond to an alert manually or you can configure Backup Exec to respond to some alerts automatically after a specified length of time. Depending on the alert type, a response might not be required, such as with informational alerts. After you respond to an alert, Backup Exec moves it to the alert history. Alert history is available on the **Home** tab, the **Backup and Restore** tab, and the **Storage** tab. In addition, an Alert History report is available from the **Reports** tab.

See [“Alert History report”](#) on page 595.

See [“Responding to active alerts”](#) on page 285.

You can configure notifications to inform recipients when alerts occur. For example, you can notify a backup administrator by email or cell phone text message when a critical alert occurs.

See [“Setting up notification for alerts”](#) on page 289.

To assist with hardware troubleshooting, Backup Exec displays alerts for SCSI event ID 9 (storage timeout), ID 11 (controller error), and ID 15 (storage not ready).

## Viewing active alerts and alert history on the Home tab

The **Active Alerts** pane appears on the **Home** tab by default. If it does not appear, follow these steps to show the alert details. Optionally, you can also enable a history of all alerts for the server to appear on the **Home** tab.

### To view active alerts and alert history on the Home tab

- ◆ On the **Home** tab, in the **System Health** group, do any of the following:
  - Check the **Active Alerts** check box to see a list of active alerts.
  - Check the **Alert History** check box to see a list of all alerts that occurred on the server.

See [“Active alerts properties ”](#) on page 281.

## Active alerts properties

Properties for active alerts can be viewed on the **Home** tab or in the details for a backup job, a restore job, or a type of storage.

See [“Viewing active alerts and alert history on the Home tab”](#) on page 281.

**Table 8-2** Properties for active alerts

Item	Description
Type	<p>Indicates the severity of the alert. The type helps you determine how quickly you want to respond.</p> <p>The following alert types may appear:</p> <ul style="list-style-type: none"><li>■ Error</li><li>■ Warning</li><li>■ Information</li><li>■ Attention Required</li></ul>

**Table 8-2** Properties for active alerts (*continued*)

Item	Description
<b>Category</b>	Indicates the condition that caused the alert. Categories include Database Maintenance, General Information, Device Error, or Job Failed.
<b>Message</b>	Indicates the text of the error message.
<b>Date and Time</b>	Shows the date and time when the alert was received.
<b>Job Name</b>	Indicates the name of the job that triggered the alert. This column is blank if the alert was not triggered by a job, such as for general information alerts.
<b>Storage</b>	Shows the name of the storage device on which the alert occurred.
<b>Server</b>	Shows the name of the server on which the alert occurred.
<b>Source</b>	Indicates the cause of the alert. Alerts can originate from one of the following sources: <ul style="list-style-type: none"><li>■ System</li><li>■ Job</li><li>■ Storage</li><li>■ Media</li></ul>

## Viewing the alert history for a server or a storage device

After you respond to an alert, Backup Exec moves it to the alert history.

### To view the alert history for a server or a storage device

- 1 On the **Backup and Restore** tab or the **Storage** tab, double-click the item for which you want to view the alert history.
- 2 In the left pane, click **Active Alerts**.
- 3 In the **Alerts** group, select **Show Alert History**.  
See [“Alert History options”](#) on page 282.

### Alert History options

After you respond to an alert, Backup Exec moves it to the alert history.

See [“Viewing the alert history for a server or a storage device”](#) on page 282.

**Table 8-3** Alert History options

Item	Description
<b>Type</b>	Indicates the severity of the alert. The alert types are Error, Warning, Informational, and Attention Required.
<b>Category</b>	Indicates the condition that caused the alert. Categories include Database Maintenance, General Information, Device Error, Job Cancellation, or Job Failed.
<b>Message</b>	Indicates the text of the error message.
<b>Date and Time</b>	Shows the date and time when the error occurred.
<b>Response Machine</b>	Shows the name of the server from which the alert response was sent.
<b>Response Time</b>	Shows the date and time when the alert response was sent.
<b>Response User</b>	Shows the user name of the person who sent the alert response.
<b>Job Name</b>	Indicates the name of the job that triggered the alert. This column is blank if the alert was not triggered by a job, such as for general information alerts.
<b>Storage</b>	Shows the name of the storage device on which the alert occurred.
<b>Server</b>	Shows the name of the server on which the alert occurred.
<b>Source</b>	Indicates the cause of the alert. Alerts can originate from one of the following sources: <ul style="list-style-type: none"><li>■ System</li><li>■ Job</li><li>■ Storage</li><li>■ Media</li></ul>

## Filtering alerts

You can filter the alerts that appear in the **Active Alerts** pane on the **Home** tab. Filters are useful when you have many alerts and you want to only view specific alert types. Alerts can be filtered by category, time, and type of alert. For example, you can choose to view only the error alerts that occurred during the last 12 hours for jobs.

### To filter alerts

- 1 On the **Home** tab, locate the **Active Alerts** pane.  
If the **Active Alerts** pane does not appear, you must enable the alert details. See [“Viewing active alerts and alert history on the Home tab”](#) on page 281.
- 2 Use any combination of the following options to filter the alerts list:
  - In the **Source** field, select the source of the alerts that you want to view.
  - In the **Time** field, select the time frame for which you want to view alerts.
  - In the **Severity** field, select the types of alerts that you want to view, such as **Error** or **Warning**.

## Viewing the job log from an alert

The job log provides detailed job information, storage and media information, job options, file statistics, and job completion status for completed jobs. You can access the job log from the alerts that were generated for jobs.

### To view the job log from an alert

- 1 Access the **Active Alerts** pane on the **Home** tab, the **Backup and Restore** tab, or the **Storage** tab.
- 2 Right-click the alert for which you want to view the job log, and then select **View Job Log**.
- 3 Do any of the following:
  - To search for a specific word or phrase, click **Find**. Type the text you want to find, and then click **Next**.  
Be sure to expand all sections of the job log. The Find feature searches only the expanded sections of the job log.
  - To print the job log, click **Print**. To print the log, you must have a printer attached to your system and configured.
  - To save the job log as an .html file or a .txt file, click **Save As** and then select the file name, file location, and file type.

See [“Job Log properties for completed jobs”](#) on page 265.

## Responding to active alerts

You can respond to active alerts and continue or cancel the operation, depending on the alert condition. By default, Backup Exec displays all enabled alerts, and all alerts that require a response. If you have set filters, only those alerts that are selected appear in addition to any alerts that require a response.

If you click **Close** on the alert response dialog box, the dialog box closes, but the alert remains active. To clear the alert, you must select a response such as **OK**, **Yes**, **No**, or **Cancel**. You can configure automatic responses for some alert categories.

See [“Configuring alert categories”](#) on page 286.

Some alerts provide a Unique Message Identifier (UMI) code. This code is a hyperlink to the Symantec Technical Support Web site. You can access the technical notes that are related to the alert.

### To respond to an active alert

- 1 Access the **Active Alerts** pane on the **Home** tab, the **Backup and Restore** tab, or the **Storage** tab.
- 2 Right-click the alert that you want to respond to, and then click **Respond** or **Respond OK**.
- 3 Click a response for the alert.

See [“Alert response options”](#) on page 285.

## Alert response options

You can respond to active alerts and depending on the alert condition, you can either continue or cancel the operation.

See [“Responding to active alerts”](#) on page 285.

**Table 8-4** Alert response options

Item	Description
<b>Server</b>	Shows the name of the computer on which the alert occurred.
<b>Storage</b>	Shows the name of the storage device on which the alert occurred.
<b>Job name</b>	Shows the name of the job that is associated with the alert.
<b>Date and Time</b>	Shows the date and time the alert occurred.

**Table 8-4** Alert response options (*continued*)

Item	Description
<b>Message</b>	Shows the detailed information about the alert.
<b>Click here for more information: V-XXX-XXXXX</b>	<p>Appears if a Technote is associated with an error. Click the Unique Message Identifier (UMI), which starts with the letter V, and appears as a blue hyperlink. A new browser window opens to the Symantec Technical Support Web site.</p> <p>If the computer does not have access to the Internet, you can type the following URL in a browser window on another computer:  <a href="http://entsupport.symantec.com/umi/&lt;UMI Code&gt;">http://entsupport.symantec.com/umi/&lt;UMI Code&gt;</a></p>
<b>View job log</b>	Lets you view the job log for the job that triggered the alert.
<b>Respond OK</b>	Lets you clear the alert from the active alerts list.
<b>Respond</b>	Lets you choose a response to the alert.
<b>Close</b>	Closes the dialog box, but does not clear the alert. The alert remains in the list of active alerts. To clear the alert, you must select a response.

## Clearing all informational alerts manually

You can configure individual alert categories to be cleared automatically after a certain period of time. Informational alerts may be generated often, so you may want to clear all informational alerts manually before the system moves them automatically.

### To clear all informational alerts manually

- 1 Access the **Active Alerts** pane on the **Home** tab, the **Backup and Restore** tab, or the **Storage** tab.
- 2 Right-click an informational alert, and then select **Clear All Informational Alerts**.

See “[Configuring alert categories](#)” on page 286.

## Configuring alert categories

You can set up alert categories to enable or disable alerts and to determine what actions should take place when an alert occurs.

Most alerts are enabled by default, however the following alert categories are initially disabled:

- Backup job contains no data
- Job Start
- Job Success

Each time you change the alert configuration, it is recorded in the audit log. You can view the audit log at any time to view the changes that were made to the alert category.

#### To configure alert category properties

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Alert Categories**.
- 3 Under **Alert category**, select the alert that you want to configure.
- 4 Under **Category Properties**, select the appropriate options.  
See “[Configure Alert Categories options](#)” on page 287.
- 5 Repeat steps 2 - 4 to configure additional alert categories.
- 6 Click **OK** to save the properties that you selected.

## Configure Alert Categories options

You can set up alert categories to enable or disable alerts and to determine what actions should take place when an alert occurs.

See “[Configuring alert categories](#)” on page 286.

**Table 8-5**      **Configure Alert Categories** options

Item	Description
<b>Alert category</b>	Lists the categories that are available.
<b>Status</b>	Indicates whether the alert category is enabled or disabled.
<b>Enable alerts for &lt;alert category&gt;</b>	Enables or disables the alert. You cannot disable alert types such as error and attention required.
<b>Include the job log with email notifications</b>	Sends the job log to the recipient that is configured for notification.

**Table 8-5**      **Configure Alert Categories options** (*continued*)

Item	Description
<b>Record event in the Windows Event Log</b>	Enters the alert into the Windows Event Viewer. The Windows Event log displays all the property information for the alert.  If a link appears in the Windows Event log you can search the Symantec Technical Support Web site for information about the Event ID.
<b>Send SNMP notifications</b>	Indicates whether SNMP notifications are enabled or cleared for the alert. SNMP must be installed to use this option.
<b>Automatically clear after <i>x</i> days/hours/minutes</b>	Lets you enter the number of minutes, hours, or days you want the alert to remain active before it is cleared.
<b>Respond with</b>	Indicates the response that you want Backup Exec to send automatically when the alert is cleared. This option is available only for the <b>Media Overwrite</b> and <b>Media Insert</b> alert categories and only when the <b>Automatically clear after <i>x</i> days/hours/minutes</b> option is selected. The choices are <b>Cancel</b> , <b>No</b> , <b>Yes</b> , or <b>OK</b> .
<b>Send notification to the following recipients</b>	Lets you select the name of a recipient to notify when this type of alert occurs. You must have recipients configured to use this option.
<b>Manage Recipients</b>	Lets you edit recipient information.

## About notifications for alerts

Backup Exec provides the ability to notify people by email or text message when alerts occur. You choose which alert categories initiate a notification and which recipients receive the notification.

**Table 8-6**      Email and text message notification details

Item	Description
Email notification	Backup Exec uses SMTP for email notifications and supports authentication and Transport Layer Security (TLS). Notification email messages can be sent to Microsoft Outlook, Lotus Notes, and Web-based email applications, such as Gmail or Yahoo mail.

**Table 8-6** Email and text message notification details (*continued*)

Item	Description
Text message notification	<p>For a text message notification, Backup Exec attempts to format the message to contain fewer than 144 characters to meet text messaging protocol restrictions. By limiting a notification to fewer than 144 characters, the notification is more likely to be sent in a single text message instead of broken up into multiple messages. However, the text messaging service provider determines how the notifications are delivered.</p> <p>Text message notifications are sent in the following formats:</p> <ul style="list-style-type: none"> <li>■ Job-related notification: Backup Exec: &lt;Server Name&gt; : &lt;Job Name&gt; : &lt;Status&gt;</li> <li>■ Alert-related notification: Backup Exec: &lt;Server Name&gt; : &lt;Alert Type&gt;</li> </ul>

After you configure email or text notification, you cannot remove the configuration to disable notifications. However, you can disable notification for individual recipients.

See [“Stopping alert notification for a recipient”](#) on page 298.

See [“Configuring email notification for alerts”](#) on page 290.

See [“Configuring text message notification for alerts”](#) on page 291.

## Setting up notification for alerts

You can configure Backup Exec to notify recipients when alerts occur. Notifications can be sent by email or text message.

**Table 8-7** How to set up notification for alerts

Step	Action
Step 1	<p>Configure the method you want to use to notify the recipient. The notification methods are text message or email.</p> <p>See <a href="#">“Configuring email notification for alerts”</a> on page 290.</p> <p>See <a href="#">“Configuring text message notification for alerts”</a> on page 291.</p>

**Table 8-7** How to set up notification for alerts (*continued*)

Step	Action
Step 2	Configure recipients, either individuals or groups. See <a href="#">“Configuring an individual recipient for alert notifications”</a> on page 293. See <a href="#">“Configuring a group recipient for alert notifications”</a> on page 295.
Step 3	Assign the recipients to alert categories or jobs for notification. See <a href="#">“Configuring alert categories”</a> on page 286. See <a href="#">“Sending a notification when a job completes”</a> on page 299.

## Configuring email notification for alerts

You can set up Backup Exec to send email to specified recipients when an alert occurs. Email notification requires an email account to be used as the sender. For example, you might want to use an email account for the backup administrator or the IT administrator. To configure email notifications, enter the name of the sender's mail server, the port number that the server uses, and the sender's name and email address. You can also set up Backup Exec to authenticate the emails that are sent for alerts.

After the sender's email information has been entered, then information about recipients can be set up.

---

**Note:** An SMTP-compliant email system, such as a POP3 mail server, is required for email notifications.

---



---

**Note:** After you configure email notification, you cannot remove the configuration to disable notifications. However, you can disable notification for individual recipients.

---

### To configure email notification for alerts

- 1 Click the Symantec Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Email and Text Notification**.
- 3 Under **Email configuration**, enter the name of the mail server, the port number, and the sender's name and email address.

See [“Configure Email and Text Messages options”](#) on page 291.

- 4 If you want to provide authentication for the emails that are sent, complete the fields under **Email authentication**.
- 5 Click **OK**.

See [“Configuring text message notification for alerts”](#) on page 291.

## Configuring text message notification for alerts

You can set up Backup Exec to send text messages to specified recipients when an alert occurs. Text message notification requires the fully-qualified domain name of the sender's text messaging service provider. In addition, information about the sender's email account, such as the name of the mail server and the sender's email address, must be entered before you can enter the sender's text message information.

---

**Note:** After you configure text notification, you cannot remove the configuration to disable notifications. However, you can disable notification for individual recipients.

---

### To configure text message notification for alerts

- 1 Click the Symantec Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Email and Text Notification**.
- 3 Under **Email configuration**, enter the name of the mail server, the port number, and the sender's name and email address.  
See [“Configure Email and Text Messages options”](#) on page 291.
- 4 In **Text message service provider address**, enter the fully-qualified domain name of the sender's text messaging service provider.
- 5 Click **OK**.

See [“Configuring email notification for alerts”](#) on page 290.

## Configure Email and Text Messages options

To enable email notifications, you must enter the name of the sender's mail server, the port number that is used, and the sender's name and email address. You can also set up Backup Exec to authenticate the emails that are sent for alert notifications. Text message notification is sent as SMTP mail to an email address that is provided by a text messaging service provider. To enable notification by text message, you must enter the fully-qualified domain name of a default text messaging service provider. For example, if a company called "MyPhone" provides

text messaging services, then enter "MyPhone.com" in the **Text message service provider address** field. You can override this default address for the individuals who do not use this provider.

---

**Note:** An SMTP-compliant email system is required for email notifications.

---

See [“Configuring email notification for alerts”](#) on page 290.

See [“Configuring text message notification for alerts”](#) on page 291.

**Table 8-8**      **Configure Email and Text Messages** options

Item	Description
<b>Email server</b>	Indicates the name of an SMTP mail server on which you have a valid user account.
<b>Port number</b>	Indicates the SMTP port number that is used for your mail server.  Your email service provider can provide the appropriate port number.
<b>Sender name</b>	Indicates the name that should appear as the sender of the notification.
<b>Sender email address</b>	Indicates the email address from which the notification should be sent.
<b>Enable email authentication</b>	Enables Backup Exec to authenticate the emails that are sent for alert notifications.
<b>Sender user name</b>	Indicates the user name for the sender's email account.
<b>Sender password</b>	Indicates the password for the sender's email account.
<b>Text message service provider address</b>	Indicates the fully-qualified domain name for all text message recipients. This address is used as the default for all recipients. However, when you configure individual recipients, you can override the default by entering a different address for that recipient.

## About managing recipients for alert notifications

Individuals or groups can be set up to receive notifications when alerts occur in Backup Exec. When you set up an individual recipient, you indicate whether the person wants to receive notifications by email, text message, or both. A group

recipient contains the individual recipients that you select. Each individual within a group receives notifications by the method that is indicated for the individual; email, text message, or both

See [“Configuring an individual recipient for alert notifications”](#) on page 293.

See [“Configuring a group recipient for alert notifications”](#) on page 295.

From the Manage Recipients dialog box, you can add or delete individual or group recipients, and edit the settings for recipients.

See [“Configuring an individual recipient for alert notifications”](#) on page 293.

See [“Configuring a group recipient for alert notifications”](#) on page 295.

**Table 8-9** Manage Recipients options

Item	Description
<b>Name</b>	Shows the names of the individual and group recipients.
<b>Type</b>	Indicates <b>Recipient</b> for an individual recipient or <b>Group</b> for a group recipient.
<b>Add a recipient</b>	Lets you add an individual recipient.
<b>Add a group</b>	Lets you add a group recipient.
<b>Edit</b>	Lets you change the settings for the selected individual or group recipient.
<b>Delete</b>	Lets you delete the selected individual or group recipient.

## Configuring an individual recipient for alert notifications

You can set up Backup Exec to send an email or a text message to a recipient when an alert occurs.

---

**Note:** Information about the notification sender must be configured before recipients can be configured.

---

See [“Configuring email notification for alerts”](#) on page 290.

See [“Configuring text message notification for alerts”](#) on page 291.

### To configure an individual recipient for alert notifications

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Notification Recipients**.
- 3 On the **Manage Recipients** dialog box, click **Add a recipient**.
- 4 Enter the name of the recipient, and then configure the email or text messaging settings.

See [“Add/Edit Individual Recipient options”](#) on page 294.

- 5 Click **OK**.

### Add/Edit Individual Recipient options

Configure the following options to send email or text message notifications to a recipient when an alert occurs.

See [“Configuring an individual recipient for alert notifications”](#) on page 293.

See [“Editing recipient notification properties”](#) on page 297.

**Table 8-10** Add/Edit Individual Recipient options

Item	Description
<b>Name</b>	Indicates the name of the notification recipient.
<b>Send notifications by email</b>	Indicates that this recipient should receive notifications by email.
<b>Recipient's email address</b>	Indicates the email address of the notification recipient.
<b>Send test email</b>	Enables Backup Exec to send a test email to verify that the email address is correct. The recipient must check his or her email account to verify that the email was received. Backup Exec does not provide confirmation of delivery.
<b>Send no more than <i>x</i> emails within <i>x</i> minutes</b>	Lets you specify the frequency of notification emails to send to this recipient. A maximum of 999 email messages can be sent within a 999-minute time period.
<b>Send notifications by text message</b>	Indicates that this recipient should receive notifications by text message.

**Table 8-10** Add/Edit Individual Recipient options (*continued*)

Item	Description
<b>Recipient's cell phone number</b>	Indicates the cell phone number of the notification recipient. If a country code is required, include the code.  The phone number can include spaces and the following characters: <ul style="list-style-type: none"><li>■ Opening and closing quotes</li><li>■ Period</li><li>■ Plus sign</li><li>■ Dash</li><li>■ Opening and closing parentheses</li><li>■ Forward slash</li></ul>
<b>Send test message</b>	Enables Backup Exec to send a test text message to verify that the phone number is correct. The recipient must check his or her text messages to verify that the message was received. Backup Exec does not provide confirmation of delivery.
<b>Text message service provider address</b>	Indicates the name of the notification recipient's text message service provider.  If a default address was entered on the <b>Configure Email and Text Messages</b> dialog box, then that address displays here. If this recipient does not use the default text message service provider, enter the appropriate address to override the default address.
<b>Send no more than <i>x</i> text messages within <i>x</i> minutes</b>	Lets you specify the frequency of text messages to send to this recipient. A maximum of 999 text messages can be sent within a 999-minute time period.

## Configuring a group recipient for alert notifications

Groups are configured by adding recipients as group members. A group contains one or more recipients and each recipient receives the notification message. A group can only include individuals. A group cannot contain other groups.

### To configure a group recipient for alert notifications

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Notification Recipients**.
- 3 On the **Manage Recipients** dialog box, click **Add a group**.
- 4 In the **Name** field, type a unique name for this notification group.
- 5 To add members to the group, select recipients from the **All recipients** list, and then click **Add** to move them to the **Selected recipients** list.

To remove members from the group, select recipients from the **Group Members** list, and then click **Remove** to move them to the **All Recipients** list.

- 6 When you have completed the group, click **OK**.

The group is added to the list of recipients on the **Manage Recipients** dialog box.

See [“Add/Edit Recipient Group options”](#) on page 296.

See [“Configuring an individual recipient for alert notifications”](#) on page 293.

## Add/Edit Recipient Group options

Groups are configured by adding individual recipients as group members.

See [“Configuring a group recipient for alert notifications”](#) on page 295.

See [“Editing recipient notification properties”](#) on page 297.

**Table 8-11** Add/Edit Recipient Group options

Item	Description
<b>Name</b>	Indicates the name of this group of recipients.
<b>All recipients</b>	Lists all of the recipients that can be added to this group.
<b>Selected recipients</b>	Lists the recipients that are included in this group.
<b>Add all</b>	Adds all recipients that are selected in the <b>All recipients</b> field to the <b>Selected recipients</b> field.

**Table 8-11** Add/Edit Recipient Group options (*continued*)

Item	Description
<b>Add</b>	Adds the individual recipient that is selected in the <b>All recipients</b> field to the <b>Selected recipients</b> field.
<b>Remove</b>	Removes the individual recipient that is selected in the <b>Selected recipients</b> field.
<b>Remove all</b>	Removes all of the recipients that are in the <b>Selected recipients</b> field.

## Removing a recipient from a group

When you remove a recipient from a group, the recipient no longer receives the notifications that the group is configured to receive. The recipient continues to receive notifications for which he or she is configured to receive as an individual recipient.

### To remove a recipient from a group

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Notification Recipients**.
- 3 On the **Manage Recipients** dialog box, double-click the group that contains the recipient.
- 4 Under **Selected recipients**, select the recipient that you want to remove, and then click **Remove**.

See “[About managing recipients for alert notifications](#)” on page 292.

## Editing recipient notification properties

You can edit the recipient notification properties at any time and change the recipient information, such as an email address or cell phone number. For a group, you can add recipients to the group or remove recipients from the group.

### To edit the recipient notification properties

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Notification Recipients**.
- 3 On the **Manage Recipients** dialog box, select the recipient that you want to edit.
- 4 Click **Edit**.

- 5 Edit the properties for the selected recipient.  
See [“Add/Edit Individual Recipient options”](#) on page 294.  
See [“Add\Edit Recipient Group options”](#) on page 296.
- 6 Click **OK**.

## Deleting recipients

You can delete the recipients that do not want to receive notification messages. The recipient is permanently removed upon deletion.

### To delete a recipient

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Notification Recipients**.
- 3 On the **Manage Recipients** dialog box, select the recipient that you want to delete.
- 4 Click **Delete**.
- 5 Click **Yes** to confirm that you want to delete this recipient.
- 6 Click **OK**.

See [“About managing recipients for alert notifications”](#) on page 292.

## Stopping alert notification for a recipient

When a recipient no longer needs to receive notifications for an alert category, you can stop the notification.

### To stop alert notification for a recipient

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Alerts and Notifications**, and then select **Alert Categories**.
- 3 Under **Alert category**, select the category for which a recipient no longer needs to receive notification.
- 4 Under **Send notifications to the following recipients**, clear the check box next to the recipient for whom you want to stop notification.
- 5 Click **OK**.

See [“About managing recipients for alert notifications”](#) on page 292.

# Sending a notification when a job completes

You can assign recipients to be notified when a job completes. Recipients must be set up before you can set up notification.

## To send a notification when a job completes

- 1 Create a new job or edit an existing job.
- 2 On the **Backup Options** dialog box, in the left pane, click **Notification**.
- 3 Select the check box for each recipient that you want to notify when each type of job completes.
- 4 To send the job log with the notification to an email address, check **Include job log in email notifications**.

See “[Notification options for jobs](#)” on page 299.

- 5 You can continue selecting other options from the **Options** dialog box or click **OK**.

## Notification options for jobs

When you set up or edit a job, you can select recipients to receive notification when the job completes.

See “[Sending a notification when a job completes](#)” on page 299.

**Table 8-12** Notification options for jobs

Item	Description
<b>Recipient name</b>	Shows the names of the individual and group recipients.
<b>Recipient type</b>	Indicates <b>Recipient</b> for an individual recipient or <b>Group</b> for a group recipient.
<b>Include job log in email notifications</b>	Enables Backup Exec to include a copy of the job log with the notification. This option applies only to email recipients. The maximum size of an attachment is determined by the settings on your mail server.
<b>Manage Recipients</b>	Lets you add, edit, or delete recipients.
<b>Properties</b>	Lets you view or change the properties of a selected recipient.

# About SNMP notification

SNMP (Simple Network Management Protocol) is a method by which a network can be monitored from a central location. SNMP-enabled network applications (like Backup Exec) report to an SNMP console (a management workstation). The console receives messages (traps) from Backup Exec regarding status and error conditions. An MIB is available in the WINNT\SNMP\language directory on the Backup Exec installation media that you can load into your SNMP console.

The Object Identifier prefix for Symantec is:

1.3.6.1.4.1.1302

Backup Exec SNMP traps (messages) have unique object IDs and may include up to four strings.

The following SNMP trap types are supported:

**Table 8-13** SNMP traps

Trap Type	Object ID	String 1	String 2	String 3	String 4
Product Start	1302.3.1.1.9.1	Backup Exec: Application initializing	machine name	product, version, revision	
Product Stop	1302.3.1.1.9.2	Backup Exec: Application terminating	machine name	product, version, revision	
Job Canceled	1302.3.1.2.8.2	Backup Exec: Job canceled by Operator	machine name	job name	local or remote Operator name
Job Failed	1302.3.1.2.8.1	Backup Exec: Job failed	machine name	job name	detail message
Storage device requires human intervention	1302.3.2.5.3.3	Backup Exec: Storage device requires attention	machine name	job name	detail message
Robotic library requires human intervention	1302.3.2.4.3.3	Backup Exec: robotic library device requires attention	machine name	job name	detail message
Simplified Disaster Recovery Message	1302.3.1.4.2.1.1	SDR copy failed	machine name	job name	detail message

**Table 8-13** SNMP traps (*continued*)

Trap Type	Object ID	String 1	String 2	String 3	String 4
Simplified Disaster Recovery Message	1302.3.1.4.2.1.2	SDR full backup success	machine name	job name	detail message
Backup Exec system error	1302.3.1.1.9.3	The application has encountered an error	machine name	job name	detail message
Backup Exec general information	1302.3.1.1.9.4	Information on normal events	machine name	job name	detail message
Job Success	1302.3.1.2.8.3	The job succeeded	machine name	job name	detail message
Job Success with exceptions	1302.3.1.2.8.4	The job succeeded, but there was a problem	machine name	job name	detail message
Job Started	1302.3.1.2.8.5	The job has started	machine name	job name	detail message
Job Completed with no data	1302.3.1.2.8.6	The job succeeded, but there was no data	machine name	job name	detail message
Job Warning	1302.3.1.2.8.7	The job has a warning	machine name	job name	detail message
PVL Device Error	1302.3.1.5.1.1.1	The device has encountered an error	machine name	job name	detail message
PVL Device Warning	1302.3.1.5.1.1.2	The device has encountered a warning	machine name	job name	detail message
PVL Device Information	1302.3.1.5.1.1.3	Normal device information	machine name	job name	detail message
PVL Device Intervention	1302.3.1.5.1.1.4	Device requires attention	machine name	job name	detail message
PVL Media Error	1302.3.1.5.2.1.1	There is an error with the media	machine name	job name	detail message

**Table 8-13** SNMP traps (*continued*)

Trap Type	Object ID	String 1	String 2	String 3	String 4
PVL Media Warning	1302.3.1.5.2.1.2	There may be a problem with the media	machine name	job name	detail message
PVL Media Information	1302.3.1.5.2.1.3	Normal media information	machine name	job name	detail message
PVL Media Intervention	1302.3.1.5.2.1.4	Media requires attention	machine name	job name	detail message
Catalog Error	1302.3.1.5.3.1.1	There is an error with the catalog	machine name	job name	detail message
Tape Alert Error	1302.3.1.5.4.1.1	There is a TapeAlert error	machine name	job name	detail message
Tape Alert Warning	1302.3.1.5.4.1.2	There is a TapeAlert warning	machine name	job name	detail message
Tape Alert Information	1302.3.1.5.4.1.3	Normal TapeAlert information	machine name	job name	detail message
Database Maintenance Error	1302.3.1.5.5.1.1	There is a database maintenance error	machine name	job name	detail message
Database Maintenance Information	1302.3.1.5.5.1.2	Normal database maintenance information	machine name	job name	detail message
LiveUpdate Error	1302.3.1.5.6.1.1	There is a software update error	machine name	job name	detail message
LiveUpdate Warning	1302.3.1.5.6.1.2	There is a software update warning	machine name	job name	detail message
LiveUpdate Information	1302.3.1.5.6.1.3	Normal software update information	machine name	job name	detail message
Install Update Warning	1302.3.1.5.7.1.1	There is an install warning	machine name	job name	detail message

Table 8-13 SNMP traps (continued)

Trap Type	Object ID	String 1	String 2	String 3	String 4
Install Update Information	1302.3.1.5.7.1.2	Normal Install information	machine name	job name	detail message

See “[Installing and configuring the SNMP system service](#)” on page 303.

## Installing and configuring the SNMP system service

To receive Backup Exec traps at the SNMP console, you must configure the SNMP system service with the SNMP console's IP address.

SNMP starts automatically after installation. You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.

**To install the SNMP system service and configure it to send traps to the SNMP console for Windows Server 2003**

- 1 From the Windows Control Panel, select **Add/Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 In Add/Remove Windows Components, select **Management and Monitoring Tools**, and then click **Details**.

When selecting the component, do not select or clear its check box.

- 4 Select **Simple Network Management Protocol**, and then click **OK**.
- 5 Click **Next**.

## Installing the Windows Management Instrumentation performance counter provider

Windows Management Instrumentation (WMI) is an infrastructure through which you can monitor and control system resources. Backup Exec includes performance counter and SNMP providers that can be manually installed and used with WMI.

**To install the WMI performance counter provider**

- 1 Insert the Backup Exec Installation media.
- 2 At the command prompt, type the following:

```
mofcomp <CD Drive Letter>:\winnt\wmi\backupexecperfmon.mof
```

## Installing the Windows Management Instrumentation provider for SNMP

Windows Management Instrumentation (WMI) is an infrastructure through which you can monitor and control system resources. Backup Exec includes performance counter and SNMP providers that can be manually installed and used with WMI.

To use the WMI SNMP provider you must set up SNMP notification.

### To install the WMI SNMP provider

- 1 Before you install the SNMP provider that is included with Backup Exec, you must have the Microsoft SNMP provider installed on your system.

For more information, refer to your Microsoft documentation.

- 2 Insert the Backup Exec Installation media.
- 3 At the command prompt, type the following:

```
mofcomp <CD Drive Letter>:\winnt\wmi\snmp\eng\bkupexecmib.mof
```

## Uninstalling the Windows Management Instrumentation performance counter provider

You must uninstall the Windows Management Instrumentation (WMI) performance counter provider and the WMI SNMP provider separately.

### To uninstall the WMI performance counter provider

- ◆ At the command line, type:

```
mofcomp <CD Drive  
Letter>:\winnt\wmi\deletebackupexecperfmon.mof
```

## Uninstalling the Windows Management Instrumentation provider for SNMP

You must uninstall the Windows Management Instrumentation (WMI) performance counter provider and the WMI SNMP provider separately.

### To uninstall the WMI SNMP provider

- ◆ At the command line, type:

```
Smi2smir /d Backup_Exec_MIB
```

# Disk-based storage

This chapter includes the following topics:

- [About disk-based storage](#)
- [About storage trending for disk storage and virtual disks](#)
- [About disk storage](#)
- [About disk cartridge storage](#)

## About disk-based storage

Features of disk-based storage include the following:

- Automatic discovery of locally accessible disk volumes.
- Disk space monitoring. Alerts are sent when the disk space thresholds that you set are reached.
- Storage trending analysis that provides predictions of low disk space for disk storage and virtual disks.

Disk-based storage includes the following types of storage:

- Disk storage  
See [“About disk storage”](#) on page 307.
- Disk cartridge devices  
See [“About disk cartridge storage”](#) on page 317.
- Deduplication storage  
See [“About the Deduplication Option”](#) on page 752.
- Storage arrays and virtual disks  
See [“About the Storage Provisioning Option”](#) on page 1160.
- Vault stores

See [“About vault stores in the Archiving Option”](#) on page 1235.

See [“About storage trending for disk storage and virtual disks”](#) on page 306.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## About storage trending for disk storage and virtual disks

Backup Exec gathers disk usage information for disk storage and virtual disks. Backup Exec then performs statistical analysis of used disk space and free disk space. The analysis provides an estimate of how many days remain before the disk storage or virtual disk is full.

Alerts provide information about whether the current disk space resources are sufficient, and can help you plan when to increase disk space.

**Table 9-1** Storage trending statuses

Storage trending status	Description
<b>Remaining storage: x days</b>	An estimate of the remaining number of days of storage space, based on the current usage of disk space.
<b>History of used space is still being gathered</b>	This status may appear for any of the following reasons: <ul style="list-style-type: none"> <li>■ The disk storage device has not been configured long enough to get a statistical estimate.</li> <li>■ This storage may be on a managed Backup Exec server that is currently in a rolling upgrade.</li> </ul>
<b>Current storage is sufficient</b>	The environment contains enough disk space to meet storage requirements for the next 30 days.
<b>No estimate due to an inconclusive history of used space</b>	A storage trend cannot be obtained. Unusual increases or decreases in the amount of free disk space in the last 30 days can cause this status.
<b>Not enough statistical information is available</b>	Backup Exec has not collected enough sample data for statistical analysis.

See [“About disk storage”](#) on page 307.

See [“About the Storage Provisioning Option”](#) on page 1160.

## About disk storage

Disk storage is a location on a locally attached internal hard drive, a USB device, a FireWire device, or a network-attached storage device to which you can back up data. You do not need to manage media when you keep backup data on disk storage. You specify how long you want to keep the data that you back up to disk storage when you create a backup job. Backup Exec automatically reclaims the disk space as the backup data expires. If you want to keep the backup data longer than the period that you specify when you create the backup job, you should create a duplicate backup job. A duplicate backup job copies the backup data from the original storage device to tape or to disk cartridge, which you can then send for long-term or off-site storage.

You must use the Configure Storage wizard to create disk storage. In the Configure Storage wizard, Backup Exec provides a list of disks on which you can create disk storage. The disks do not appear in the list in the alphabetical order of the drive letter. Instead, the disk that appears first in the list has the most amount of disk space. You can select any disk that you want, but the disk that Backup Exec recommends for use appears at the top of the list. The disk that you use as the system drive always appears last in the list. Symantec recommends that you do not configure disk storage on the system drive.

To be eligible for configuration as disk storage, a disk must have at least 1 GB of disk space and cannot be configured as deduplication disk storage. Although you can configure disk storage and deduplication disk storage on the same disk, it is not recommended.

When you create disk storage on a disk that is attached to the network, you must specify the path to an existing share. The Backup Exec service account must have read and write permissions on the remote computer on which the network share is located.

---

**Note:** Before you create the disk storage on a network share, you must give read and write permissions to the Backup Exec service account. The Backup Exec service account is on the Backup Exec server that you want to access the network share.

---

When you create disk storage, Backup Exec lets you specify any of the following locations on a local disk:

- Volumes with or without drive letters.  
You can create only one disk storage on a volume.

- Unformatted partitions.  
Backup Exec formats and partitions the drive for you, if necessary.
- Drives that do not have partitions.

Backup Exec creates a folder named BEControl on the root of the volume. Do not delete or edit the contents of the BEControl folder, and do not copy it to other volumes or drive letters.

In Windows Explorer, the backup files that the disk storage device contains display with a .bkf file extension. Each disk storage device also contains a file named changer.cfg and a file named folder.cfg, which store information about the backup files. Do not delete or edit the changer.cfg or folder.cfg files.

A subfolder with a prefix of IMG in the name may display in a disk storage device. This subfolder appears if the option to enable Granular Recovery Technology (GRT) was selected for backup, or if you select the disk storage device as storage for backup data.

See [“About the Deduplication Option”](#) on page 752.

See [“About the Configure Storage wizard”](#) on page 145.

See [“Changing the location of a disk storage device”](#) on page 309.

See [“Editing disk storage properties”](#) on page 309.

See [“About keeping backup sets”](#) on page 213.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“About restoring data from a reattached disk-based storage device”](#) on page 308.

## About restoring data from a reattached disk-based storage device

If the backup sets on a disk-based storage device expire while that device is detached, the catalogs for those backup sets are deleted. To restore from any backup sets, you must run an inventory and catalog operation on the device when you reattach it. When you run the inventory and catalog operation, Backup Exec sets a new expiration date for each backup set by using the backup set's original retention setting, calculated from the current date. The expiration date is also reset for any backup set on the storage device that expires within seven days of the current date.

If you want the backup sets to expire, you can disable the storage device property **Limit Backup Exec to read-only operations**. Do not run an inventory and catalog operation. Backup Exec reclaims the disk space on that storage device during data lifecycle management. You can also delete the backup sets.

See [“Inventorying and cataloging a storage device”](#) on page 423.

See [“Disk storage properties”](#) on page 310.

See [“About keeping backup sets”](#) on page 213.

See [“Deleting backup sets”](#) on page 214.

## Changing the location of a disk storage device

You can change the location of an existing disk storage device.

See [“About disk storage”](#) on page 307.

---

**Note:** When you copy files from the original disk storage device to the new location, do not copy .cfg files.

---

### To change the location of a disk storage device

- 1 Use the **Configure Storage** wizard to create a new disk storage device with a different name and drive letter than the original disk storage device.  
See [“About the Configure Storage wizard”](#) on page 145.
- 2 In Windows Explorer, copy and paste the following files from the \BEData folder on the original disk storage device to the \BEData folder on the new location:
  - .Bkf files
  - Any subfolders with a prefix of IMG in the name
- 3 In Windows Explorer, delete all of the files from the original disk storage device.
- 4 Delete the original disk storage device.  
See [“Deleting a storage device”](#) on page 421.
- 5 Rename the new disk storage device with the name of the original disk storage device.
- 6 On the Backup Exec Administration Console, right-click the new disk storage device, and then click **Inventory and Catalog**.  
See [“Inventorying and cataloging a storage device”](#) on page 423.

## Editing disk storage properties

You can edit disk space management settings for the disk storage device.

See [“About disk storage”](#) on page 307.

**To edit disk storage properties**

- 1 On the **Storage** tab, double-click the storage for which you want to edit properties.
- 2 In the left pane, click **Properties**.
- 3 Edit the appropriate options.  
 See “[Disk storage properties](#)” on page 310.
- 4 Click **Apply**.

## Disk storage properties

Properties for disk storage enable you to perform the following actions:

- Change disk space management settings.
- View usage and error statistics.

See “[Editing disk storage properties](#)” on page 309.

**Table 9-2** Disk storage properties

Item	Description
<b>Name</b>	Displays the name of the disk storage. You can edit this field.
<b>Description</b>	Displays a description of the disk storage. You can edit this field.
<b>State</b>	Indicates the status of the disk storage device.  See “ <a href="#">Backup Exec server and storage device states</a> ” on page 434.

**Table 9-2** Disk storage properties (*continued*)

Item	Description
<b>Limit Backup Exec to read-only operations</b>	<p>Indicates whether or not you want Backup Exec to reclaim disk space from this disk-based storage, such as a USB drive. If you reattach a storage device to Backup Exec, and if any data has expired, then Backup Exec may attempt to reclaim the disk space. To prevent this situation, limit Backup Exec to read-only operations so that you can restore data from this storage device without overwriting the existing data.</p> <p>If you enable this option, you can change the global setting that specifies the number of days that the storage device must be detached from Backup Exec before this option takes effect. However, when the specified number of days has passed for a detached disk storage device, Backup Exec automatically limits Backup Exec to read-only operations for this device.</p> <p>The default value is <b>No</b>.</p> <p>See “<a href="#">Global settings for storage</a>” on page 415.</p> <p>See “<a href="#">About keeping backup sets</a>” on page 213.</p> <p>See “<a href="#">About restoring data from a reattached disk-based storage device</a>” on page 308.</p>
<b>Maximum file size</b>	<p>Displays the maximum file size on the disk storage. The data from the backup job is contained in a file on the disk.</p> <p>The default value is 50 GB or the capacity of the disk storage.</p>

**Table 9-2** Disk storage properties (*continued*)

Item	Description
<p><b>Preallocate disk space incrementally up to the maximum file size</b></p>	<p>Creates the file when the backup job starts by preallocating space incrementally, according to the size of the increment that you set in <b>Preallocation increment</b>. As the job uses the disk space, more disk space is preallocated up to the maximum file size. When the job completes, the file size is then reduced to the amount of disk space that the job actually used.</p> <p>For example, if you enable preallocation and set the preallocation increment to 4 GB, then 4 GB of disk space is preallocated when the job starts. After the job uses 4 GB, then Backup Exec allocates another 4 GB. Disk space continues to be preallocated by 4 GB until the job completes. If the job only uses 13 GB of the 16 GB that was allocated, then the file size is reduced to 13 GB.</p> <p>The default value is <b>Disabled</b>.</p>
<p><b>Preallocation increment</b></p>	<p>Displays the amount of disk space by which to increase the file size. The file size is increased by this increment as the job requires disk space, up to the maximum file size.</p> <p>The default value is 1 GB.</p>
<p><b>Auto detect block and buffer size</b></p>	<p>Indicates if Backup Exec automatically detects the preferred settings for the block and buffer size for the disk storage.</p> <p>The default value is <b>Enabled</b>.</p>

Table 9-2 Disk storage properties (*continued*)

Item	Description
<b>Block size</b>	<p>Displays the size of the blocks of data that are written to new media in this disk storage device if the option <b>Auto detect block and buffer size</b> is disabled. The default is the preferred block size.</p> <p>Some storage devices provide better performance when larger block sizes are used. The preferred block size can range from 512 bytes to 64 kilobytes or larger. If you use a storage device that supports larger block sizes, you can change the block size. However, if the option to change the block size is unavailable, you must configure the device to use a larger size.</p> <p>See the manufacturer's documentation for help in configuring the device.</p> <p>Backup Exec does not ensure that the requested block size is supported by the storage device. If the requested block size is not supported, it defaults to its standard block size.</p> <p>If the device does not support block size configuration, this option is unavailable.</p>
<b>Buffer size</b>	<p>Displays the amount of the data that is sent to the disk storage device on each read or write request if the option <b>Auto detect block and buffer size</b> is disabled. The buffer size must be an even multiple of the block size.</p> <p>Depending on the amount of memory in your system, increasing this value may improve storage performance. Each type of storage device requires a different buffer size to achieve maximum throughput.</p> <p>If the preferred block size is greater than 64 KB, the default buffer size is the same as the default block size. If the preferred block size is less than 64 KB, then the default buffer size is 64 KB.</p>

**Table 9-2** Disk storage properties (*continued*)

Item	Description
<p><b>Low disk space - Critical</b></p>	<p>Displays the critically low disk space threshold at which you want Backup Exec to send an alert. Backup Exec sends alerts when the amount of free disk space drops below the low disk space threshold, and again if it drops below the warning threshold. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the warning threshold.</p> <p>The default value is 5%.</p>
<p><b>Low disk space - Warning</b></p>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the low disk space threshold.</p> <p>The default value is 15%.</p>

Table 9-2 Disk storage properties (*continued*)

Item	Description
<b>Low disk space</b>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below this threshold to the amount specified in the warning threshold, another alert is sent. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes.</p> <p>The default value is 25%.</p>
<b>Disk space to reserve for non-Backup Exec operations</b>	<p>Displays the amount of disk space to set aside for applications other than Backup Exec.</p> <p>The default value is 10 MB.</p>
<b>Total capacity</b>	<p>Displays the size of the volume on which the disk storage is located.</p>
<b>Total backup storage</b>	<p>Displays the difference between <b>Total capacity</b> and the amount of disk space that is reserved for non-Backup Exec operations.</p>
<b>Used capacity</b>	<p>Displays the amount of space on the volume that is used by Backup Exec and other applications.</p>
<b>Amount of data written</b>	<p>Displays the total amount of backup data that is on the disk storage device.</p>
<b>Available capacity</b>	<p>Displays the difference between <b>Total backup storage</b> and <b>Used capacity</b>.</p>
<b>Compression ratio</b>	<p>Displays the ratio of <b>Amount of data written</b> to <b>Used capacity</b>. <b>Compression ratio</b> shows the overall effect that data compression and media flaws have on the amount of data that is stored.</p>

**Table 9-2** Disk storage properties (*continued*)

Item	Description
<b>Path</b>	Displays the location of the disk storage device on the Backup Exec server.
<b>Connection type</b>	Indicates if the disk storage is located on a disk that is local to the Backup Exec server or if it is on a remote disk.
<b>Backup Exec service restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.
<b>Auto detect settings</b>	Indicates if Backup Exec automatically detects the preferred settings for read and write buffers for the disk storage.
<b>Buffered read</b>	Indicates the following when the setting is enabled: <ul style="list-style-type: none"> <li>■ You do not want Backup Exec to automatically detect settings for this disk storage device.</li> <li>■ You want this disk storage to allow buffered reads, which is the reading of large blocks of data.</li> </ul> <p>Enabling buffered reads may provide increased performance.</p>
<b>Buffered write</b>	Indicates the following when the setting is enabled: <ul style="list-style-type: none"> <li>■ You do not want Backup Exec to automatically detect settings for this disk storage device.</li> <li>■ You want this disk storage to allow buffered writes, which is the writing of large blocks of data.</li> </ul>
<b>Concurrent write operations</b>	Displays the number of concurrent write operations that you want to allow to this disk storage device.

## About disk cartridge storage

Disk cartridges are a type of storage that usually remains attached to the Backup Exec server while you remove the media, such as RDX. If you are not sure if the storage has removable media, you can open the Computer folder on your Windows computer. The devices that contain removable media are listed.

You can manage how long Backup Exec keeps data that is stored on disk cartridge media by associating the media with media sets. You create media sets that specify append periods, overwrite protection periods, and vaulting periods.

You must use the **Configure Storage** wizard to configure a disk cartridge device and to create new media sets. When you install Backup Exec, system-defined media sets are created by default.

See [“Creating media sets for tape and disk cartridge media”](#) on page 373.

See [“About the Configure Storage wizard”](#) on page 145.

See [“Editing disk cartridge properties”](#) on page 317.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Editing disk cartridge properties

You can edit disk space management settings and settings for the Backup Exec server to which the storage is attached.

See [“About disk cartridge storage”](#) on page 317.

### To edit disk cartridge properties

- 1 On the **Storage** tab, double-click the disk cartridge for which you want to edit properties.
- 2 In the left pane, click **Properties**.
- 3 Edit the appropriate options.  
See [“Disk cartridge properties”](#) on page 317.
- 4 Click **Apply**.

## Disk cartridge properties

Properties provide information about the disk cartridge, and the Backup Exec server that it is attached to.

See [“Editing disk cartridge properties”](#) on page 317.

**Table 9-3** Disk cartridge properties

Item	Description
<b>Name</b>	<p>Displays the name of the disk cartridge. Disk cartridge names cannot exceed 128 characters.</p> <p>You can rename the disk cartridge.</p>
<b>Description</b>	<p>Displays a description of the disk cartridge.</p>
<b>State</b>	<p>Indicates the state of the disk cartridge.</p>
<b>Maximum file size</b>	<p>Displays the maximum file size on the disk cartridge. The data from the job is contained in a file on the disk cartridge.</p> <p>The default value is 50 GB or the capacity of the disk cartridge media.</p>
<b>Preallocate disk space incrementally up to the maximum file size</b>	<p>Creates the file when the job starts by preallocating space incrementally, according to the size of the increment that you set in <b>Preallocation increment</b>. As the job uses the disk space, more disk space is preallocated up to the maximum file size. When the job completes, the file size is then reduced to the amount of disk space that the job used.</p> <p>For example, if you enable preallocation and set the preallocation increment to 4 GB, then 4 GB of disk space is preallocated when the job starts. After the job uses 4 GB, then Backup Exec allocates another 4 GB. Disk space continues to be preallocated by 4 GB until the job completes. If the job only uses 13 GB of the 16 GB that was allocated, then the file size is reduced to 13 GB.</p> <p>The default value is <b>Disabled</b>.</p>
<b>Preallocation increment</b>	<p>Displays the amount of disk space by which to increase the file size. The file size increases by this increment as the job requires disk space, up to the maximum file size.</p> <p>The default value is 1 GB.</p>

**Table 9-3** Disk cartridge properties (*continued*)

Item	Description
<b>Auto detect block and buffer size</b>	<p>Indicates if Backup Exec automatically detects the preferred settings for the block size and buffer size for the disk storage.</p> <p>The default value is <b>Enabled</b>.</p>
<b>Block size</b>	<p>Displays the size of the blocks of data that are written to new media in this disk cartridge if the option <b>Auto detect block and buffer size</b> is disabled. The default is the preferred block size.</p> <p>Some storage provide better performance when larger block sizes are used. The preferred block size can range from 512 bytes to 64 kilobytes or larger. If you use the storage that supports larger block sizes, you can change the block size. However, if the option to change the block size is unavailable, you must configure the device to use a larger size.</p> <p>See the manufacturer’s documentation for help in configuring the storage.</p> <p>Backup Exec does not ensure that the requested block size is supported by that storage. If the requested block size is not supported, it defaults to its standard block size.</p> <p>If the storage does not support block size configuration, this option is unavailable.</p>

**Table 9-3** Disk cartridge properties (*continued*)

Item	Description
<b>Buffer size</b>	<p>Displays the amount of the data that is sent to the disk cartridge on each read or write request if the option <b>Auto detect block and buffer size</b> is disabled. The buffer size must be an even multiple of the block size.</p> <p>Depending on the amount of memory in your system, increasing this value may improve storage performance. Each type of storage requires a different buffer size to achieve maximum throughput.</p> <p>If the preferred block size is greater than 64 KB, the default buffer size is the same as the default block size. If the preferred block size is less than 64 KB, then the default buffer size is 64 KB.</p>
<b>Total capacity</b>	<p>Displays the size of the volume on which the disk cartridge is located.</p>
<b>Total backup storage</b>	<p>Displays the difference between <b>Total capacity</b> and the amount of disk space that is reserved for non-Backup Exec operations.</p>
<b>Used capacity</b>	<p>Displays the amount of space on the volume that is used by Backup Exec and other applications.</p>
<b>Amount of data written</b>	<p>Displays the total amount of backup data that is on the disk cartridge.</p>
<b>Available capacity</b>	<p>Displays the difference between <b>Total backup storage</b> and <b>Used capacity</b>.</p>
<b>Compression ratio</b>	<p>Displays the ratio of <b>Amount of data written</b> to <b>Used capacity</b>. <b>Compression ratio</b> shows the overall effect that data compression and media flaws have on the amount of data that is stored on the disk cartridge media.</p>
<b>Path</b>	<p>Displays the location of the disk cartridge on the Backup Exec server.</p>

**Table 9-3** Disk cartridge properties (*continued*)

Item	Description
<b>Connection type</b>	Indicates if the disk cartridge is located on a disk that is local to the Backup Exec server, or if it is on a remote disk.
<b>Backup Exec service restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.
<b>Auto detect settings</b>	Indicates if Backup Exec automatically detects the preferred settings for read and write buffers for the disk cartridge.  The default value is <b>Enabled</b> .
<b>Buffered read</b>	Indicates the following when the setting is enabled: <ul style="list-style-type: none"> <li>■ You do not want Backup Exec to automatically detect settings for this disk cartridge.</li> <li>■ You want this disk cartridge to allow buffered reads, which is the reading of large blocks of data.</li> </ul> <p>Enabling buffered read operations may provide increased performance.</p> <p>The default value is <b>Enabled</b>. If you disable <b>Auto detect settings</b>, this setting also changes to <b>Disabled</b>.</p>
<b>Buffered write</b>	Indicates the following when the setting is enabled: <ul style="list-style-type: none"> <li>■ You do not want Backup Exec to automatically detect settings for this disk cartridge.</li> <li>■ You want this disk cartridge to allow buffered writes, which is the writing of large blocks of data.</li> </ul> <p>The default value is <b>Enabled</b>. If you disable <b>Auto detect settings</b>, this setting also changes to <b>Disabled</b>.</p>

**Table 9-3** Disk cartridge properties (*continued*)

Item	Description
<b>Concurrent write operations</b>	Displays the number of concurrent write operations that you want to allow to this disk cartridge.

# Network-based storage

This chapter includes the following topics:

- [About network-based storage](#)
- [About cloud storage devices](#)

## About network-based storage

Network-based storage includes NDMP servers, OpenStorage devices, cloud storage, and the Remote Media Agent for Linux.

See “[About cloud storage devices](#)” on page 323.

See “[About the NDMP Option](#)” on page 1062.

See “[About OpenStorage devices](#)” on page 757.

See “[About the Remote Media Agent for Linux](#)” on page 1132.

## About cloud storage devices

You can send your backup data to a cloud storage device. To use a cloud storage device, you must have an account with a public cloud storage device vendor. You must also download the associated OST plug-in for this device and install it on the Backup Exec server. Backup Exec OST Cloud Storage plug-ins enable Symantec data protection applications to access Cloud Storage Solutions. Either the storage vendor or Symantec provides a software plug-in, which you install on each Backup Exec server that is connected to the cloud solution.

You can find a list of compatible types of cloud storage, as well as direct links to available plug-ins at the following URL, in the OpenStorage section:

<http://entsupport.symantec.com/umi/V-269-2>

You can add a cloud storage device from the **Configure Storage** wizard. After you add cloud storage, a cloud storage device appears on the **Storage** tab. A cloud storage device cannot belong to any storage pools. This limitation prevents a deduplication job from being sent to a non-deduplication device in a storage pool if the cloud storage device is busy.

If you use Backup Exec Central Admin Server Option, a cloud storage device can be shared between multiple Backup Exec servers. Sharing can be enabled when you add a cloud storage device. You can select new Backup Exec servers to share a cloud storage device. You can remove the sharing ability for Backup Exec servers at any time.

See [“About the Configure Storage wizard”](#) on page 145.

## Editing the properties of a cloud storage device

You can view all of the properties of a cloud storage device and you can change some of the properties.

See [“About network-based storage”](#) on page 323.

### To edit the properties for a cloud storage device

- 1 On the **Storage** tab, double-click the name of the cloud storage device.
- 2 In the left pane, select **Properties**.
- 3 Change the properties as needed.  
See [“Cloud storage device properties”](#) on page 324.
- 4 Click **Apply** to save the changes.

## Cloud storage device properties

You can view all of the properties of a cloud storage device and you can change some of the properties.

See [“Editing the properties of a cloud storage device”](#) on page 324.

**Table 10-1** Cloud storage device properties

Item	Description
<b>Name</b>	Indicates the user-defined name for this cloud storage device.
<b>Description</b>	Indicates the user-defined description of this cloud storage device.

**Table 10-1** Cloud storage device properties (*continued*)

Item	Description
<b>State</b>	Indicates the current state of the device. You cannot change this property.
<b>Host server</b>	Indicates the fully qualified name of the server on which the device exists.
<b>Server location</b>	Indicates the location of the server on which the device exists.
<b>Server type</b>	Indicates the type of cloud storage device.
<b>Storage location</b>	Indicates the name of the storage location on the cloud storage device.
<b>Logon account</b>	Indicates the name of the logon account that is required to access the device.
<b>Concurrent operations</b>	Indicates the maximum number of jobs that you want to run at the same time on this device.
<b>Split data stream every</b>	Indicates the size at which you want Backup Exec to span to a new image. The default size is 50 GB.
<b>Data stream size</b>	Indicates the size of a single write operation that Backup Exec issues. The default size varies based on the type of device that is used.
<b>Stream handler</b>	Indicates whether stream handler is used. Backup Exec sets this option automatically when you select a server type. For some types of devices, this option does not appear at all. If Backup Exec does not set this option, contact the device's vendor for the recommended setting.

**Table 10-1** Cloud storage device properties (*continued*)

Item	Description
<b>Client-side deduplication</b>	<p>Indicates whether client-side deduplication is enabled for this cloud storage device.</p> <p>Client-side deduplication enables a remote computer to send data directly to a cloud storage device. The use of client-side deduplication bypasses the Backup Exec server, which leaves the Backup Exec server free to perform other operations.</p>
<b>Disk space to reserve for non-Backup Exec operations</b>	<p>Displays the amount of disk space to set aside for applications other than Backup Exec. The default amount is 5%.</p>
<b>Total capacity</b>	<p>Shows the total amount of storage space that is available on this device.</p>
<b>Used capacity</b>	<p>Shows the total amount of storage space that is used on this device.</p>
<b>Deduplication ratio</b>	<p>Deduplication is not supported for this device.</p>
<b>Connection type</b>	<p>Indicates the type of connection between the Backup Exec server and the cloud storage device. The connection type is Network.</p>
<b>Backup Exec service restart needed</b>	<p>Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.</p>

# Legacy backup-to-disk folders

This chapter includes the following topics:

- [About legacy backup-to-disk folders](#)

## About legacy backup-to-disk folders

In previous versions of Backup Exec, the backup-to-disk feature let you back up data to a folder on a hard disk. These legacy backup-to-disk folders are now read-only. You can continue to inventory, catalog, and restore data from a backup-to-disk folder. You can use remote Simplified Disaster Recovery to perform a disaster recovery from backup-to-disk folders.

You cannot send backup data to a backup-to-disk folder. Symantec recommends that you use disk storage to back up data to a disk.

See [“About disk-based storage”](#) on page 305.

In Windows Explorer, the backup-to-disk folders display in the path you specified when you added the folders. The backup-to-disk files display with a .bkf file extension. Each backup-to-disk folder also contains a file named changer.cfg and a file named folder.cfg, which store information about the backup-to-disk files.

---

**Note:** Do not delete or edit the changer.cfg or folder.cfg files.

---

A subfolder with a prefix of IMG in the name may display under a backup-to-disk folder.

In previous versions, Backup Exec created this subfolder when the following conditions were met in a backup job:

- The option to enable Granular Recovery Technology (GRT) was selected.
  - A backup-to-disk folder was selected as storage for the backup data.
- See [“Importing a legacy backup-to-disk folder”](#) on page 328.
- See [“Editing backup-to-disk folder properties”](#) on page 328.
- See [“Changing the location of a legacy backup-to-disk folder”](#) on page 330.
- See [“Recreating a legacy backup-to-disk folder and its contents”](#) on page 331.

## Importing a legacy backup-to-disk folder

You must import an existing backup-to-disk folder into Backup Exec 2012 to restore data from it. When you import a backup-to-disk folder, you cannot use the root of a volume or an administrative UNC share as the path. The administrative shares are ADMIN\$, IPC\$, and one for each local disk drive letter, such as C\$, D\$, and so on.

For example, you cannot use D:\ or \\OtherServer\C\$\B2D7, but you can use D:\B2D. If you create a share named B2DOnMyDriveC on OtherServer, then you can use \\OtherServer\B2DOnMyDriveC or \\OtherServer\B2DOnMyDriveC\Dir1.

Use the **Configure Storage** wizard to import a legacy backup-to-disk folder.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About legacy backup-to-disk folders ”](#) on page 327.

## Editing backup-to-disk folder properties

You can edit the name and description of a backup-to-disk folder. You can also change the settings for buffered reads and writes.

See [“About legacy backup-to-disk folders ”](#) on page 327.

### To edit backup-to-disk folder properties

- 1 On the **Storage** tab, double-click the backup-to-disk folder for which you want to edit the properties.
- 2 In the left pane, click **Properties**.
- 3 Edit the appropriate options.  
See [“Backup-to-disk folder properties ”](#) on page 329.
- 4 Click **Apply**.

## Backup-to-disk folder properties

Properties for legacy backup-to-disk folders provide information about the folders.

See [“Editing backup-to-disk folder properties”](#) on page 328.

**Table 11-1** Backup-to-disk folder properties

Item	Description
<b>Name</b>	Displays the name of the backup-to-disk folder. Backup-to-disk folder names must not exceed 128 characters. You can edit this field.  See <a href="#">“Renaming a storage device”</a> on page 421.
<b>Description</b>	Displays the description of the backup-to-disk folder. You can edit this field.
<b>State</b>	Indicates the status of the backup-to-disk folder.  If the folder is offline, no operations are allowed on the folder until it is online again.  The folder appears as offline if the following occurs: <ul style="list-style-type: none"><li>■ The backup-to-disk folder is on a remote computer and connectivity is not available.</li><li>■ The access rights to the folder or to the remote computer are incorrect.</li></ul> See <a href="#">“Changing the state of a storage device to online”</a> on page 425.  See <a href="#">“Backup Exec server and storage device states”</a> on page 434.
<b>Path</b>	Displays the location of the backup-to-disk folder on the Backup Exec server.
<b>Connection type</b>	Indicates if the backup-to-disk folder is located on a disk that is local to the Backup Exec server or if it is on a remote disk.
<b>Restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this backup-to-disk folder.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.

**Table 11-1** Backup-to-disk folder properties (*continued*)

Item	Description
<b>Auto detect buffers</b>	Indicates if Backup Exec automatically detects the preferred settings for read buffers for the backup-to-disk folder.
<b>Buffered reads</b>	Indicates the following when the setting is Enabled: <ul style="list-style-type: none"><li>■ You do not want Backup Exec to automatically detect settings for this backup-to-disk folder.</li><li>■ You want this backup-to-disk folder to allow buffered reads, which is the reading of large blocks of data.</li></ul> Enabling the buffered reads setting may provide increased performance.

## Changing the location of a legacy backup-to-disk folder

You can change the location of a legacy backup-to-disk folder.

See “[About legacy backup-to-disk folders](#)” on page 327.

### To change the location of a legacy backup-to-disk folder

- 1 Delete the original legacy backup-to-disk from Backup Exec.  
See “[Deleting a storage device](#)” on page 421.
- 2 Create a folder that has a different name and location than the existing legacy backup-to-disk folder.
- 3 In Windows Explorer, copy and paste all of the following files and folders to the new folder:
  - .Bkf files
  - .Cfg files
  - Any subfolders with a prefix of IMG in the name
- 4 In Windows Explorer, delete all of the files from the original backup-to-disk folder.
- 5 On the Backup Exec Administration Console, on the **Storage** tab, in the **Configure** operation group, click **Configure Storage**.

- 6 Follow the prompts to import the legacy backup-to-disk folder from the new location.
- 7 Right-click the backup-to-disk folder, and then click **Inventory and Catalog**.  
See [“Inventorying and cataloging a storage device”](#) on page 423.

## Recreating a legacy backup-to-disk folder and its contents

If you have deleted a backup-to-disk folder from Backup Exec, but not from the disk, you can recreate the backup-to-disk folder and the files in it. You must know the name and path of the original backup-to-disk folder to retrieve it. If you deleted a backup-to-disk folder from the disk, you cannot recreate it.

See [“About legacy backup-to-disk folders”](#) on page 327.

### To recreate a legacy backup-to-disk folder and its contents

- 1 On the **Storage** tab, in the **Configure** operation group, click **Configure Storage**.
- 2 Follow the prompts to import the legacy backup-to-disk folder that you want to recreate.
- 3 Right-click the backup-to-disk folder, and then click **Inventory and Catalog**.  
See [“Inventorying and cataloging a storage device”](#) on page 423.



# Tape drives and robotic libraries

This chapter includes the following topics:

- [About tape drives and robotic libraries](#)
- [About the Virtual Tape Library Unlimited Drive Option](#)
- [About the Library Expansion Option](#)
- [About using the Hot-swappable Device Wizard to add or replace devices](#)
- [About installing Symantec tape device drivers](#)
- [Editing tape drive properties](#)
- [Enabling or disabling hardware compression for tape drives](#)
- [Changing the block size, buffer size, buffer count, and high water count for tape drives](#)
- [Changing the settings to read and write in single block mode for tape drives](#)
- [Changing the settings to read and write in SCSI pass-through mode for tape drives](#)
- [Viewing tape drive statistics](#)
- [About robotic libraries in Backup Exec](#)
- [About robotic library partitions](#)

## About tape drives and robotic libraries

When you install Backup Exec, it automatically recognizes all tape storage that is attached to the Backup Exec server. Tape storage includes tape drives, robotic libraries, virtual tape libraries, and simulated tape libraries.

When you install Backup Exec, support for the following items is included:

- The first robotic library drive per robotic library.
- Every single-drive virtual tape library.

Support for additional drives is available with the Library Expansion Option and the Virtual Tape Library Unlimited Drive Option.

You can use the **Configure Storage** wizard to perform the following actions for tape storage:

- Partition robotic library slots.
- Install Symantec tape device drivers.
- Replace or add hot-swappable storage on a Backup Exec server without having to restart the server.
- Create media sets to manage the backup data on tapes.

See “[About the Configure Storage wizard](#)” on page 145.

See “[About the Virtual Tape Library Unlimited Drive Option](#)” on page 334.

See “[About the Library Expansion Option](#)” on page 335.

See “[About media sets](#)” on page 366.

See “[Viewing jobs, job histories, backup sets, and active alerts for storage devices](#)” on page 422.

## About the Virtual Tape Library Unlimited Drive Option

When you install Backup Exec, support for every single-drive virtual tape library is included. The Virtual Tape Library Unlimited Drive Option enables support for all additional drives in each virtual tape library. To install the Virtual Tape Library Unlimited Drive Option, add a license.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/v-269-2>

You can find license information for the Virtual Tape Library Unlimited Drive Option at the following URL:

<http://entsupport.symantec.com/umi/V-269-21>

See “[Installing additional Backup Exec options to the local Backup Exec server](#)” on page 75.

## About the Library Expansion Option

When you install Backup Exec, support for the first drive in every robotic library is included. The Library Expansion Option enables support for each additional drive in a robotic library.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/v-269-2>

You can find license information for the Library Expansion Option at the following URL:

<http://entsupport.symantec.com/umi/V-269-21>

To install the Library Expansion Option, add a license.

See “[Installing additional Backup Exec options to the local Backup Exec server](#)” on page 75.

## About using the Hot-swappable Device Wizard to add or replace devices

Use the **Hot-swappable Device Wizard** to replace or add hot-swappable storage on a Backup Exec server without having to restart the server.

If you remove and then reconnect Universal Serial Bus (USB) tape devices to the USB port, you must run the **Hot-swappable Device Wizard** to allow Backup Exec to rediscover the devices.

For iSCSI-attached devices, you must list the device as a **Persistent Target** in the iSCSI control panel applet, and then run the **Hot-swappable Device Wizard**.

Listing the device as a **Persistent Target** lets Backup Exec rediscover the device whenever you restart the Backup Exec server.

After you start the **Hot-swappable Device Wizard**, you are prompted to close the Backup Exec Administration Console. The **Hot-swappable Device Wizard** waits until any jobs that were processing are completed. The wizard pauses the Backup Exec server and stops the Backup Exec services. You can then add or replace any storage devices. The wizard detects the new device or replaced device, and adds information about the device to the Backup Exec Database. The wizard is then completed, and you can reopen the Backup Exec Administration Console.

Any new storage appears in the **Storage** tab, and usage statistics for the storage begin accumulating. You can enable the new storage in a storage device pool.

Any replaced storage appears in the **Storage** tab, in the **All Storage** view with a status of Offline.

See [“Using the Hot-swappable Device Wizard to add or replace devices”](#) on page 336.

## Using the Hot-swappable Device Wizard to add or replace devices

Use the **Hot-swappable Device Wizard** to add or replace hot-swappable storage on a Backup Exec server. You do not need to restart the server.

See [“About using the Hot-swappable Device Wizard to add or replace devices”](#) on page 335.

---

**Note:** Start the **Symantec Hot-swappable Device Wizard** before you add or replace storage.

---

### Using the Hot-swappable Device Wizard to add or replace devices

**1** Do one of the following:

For iSCSI-attached storage:

In the iSCSI control panel applet, add the storage to the **Persistent Targets** list.

Continue with the next step.

For any other hot-swappable storage:

Continue with the next step.

**2** On the **Storage** tab, in the **Configure** group, click **Configure Storage**.

**3** When you are prompted for the type of storage that you want to configure, select **Tape Storage**, and then click **Next**.

**4** Select **Run the Hot-swappable Device Wizard**, click **Next**, and then follow the on-screen prompts.

## About installing Symantec tape device drivers

Use the **Symantec Device Driver Installation Wizard** to install Symantec tape device drivers.

Before you install Symantec tape device drivers, do the following:

- Ensure that Backup Exec supports the tape device.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

- Run the Windows Device Manager to ensure that it lists the tape device.

See “[Installing Symantec tape device drivers by running tapeinst.exe](#)” on page 337.

See “[Using the Symantec Device Driver Installation Wizard to install tape device drivers](#)” on page 337.

## Installing Symantec tape device drivers by running tapeinst.exe

You can install Symantec tape device drivers by running `tapeinst.exe`, which is located in the Backup Exec installation directory. Updates for `tapeinst.exe` are available in the **Device Driver Installer** package.

You can download the **Device Driver Installer** package from the following URL:

<http://go.symantec.com/support/BEWS-downloads-drivers>

See “[About installing Symantec tape device drivers](#)” on page 336.

---

**Note:** You must run `tapeinst.exe` locally on the Backup Exec server where you want to install tape device drivers. You cannot use `tapeinst.exe` to push-install tape device drivers to remote Backup Exec servers.

---

### To install Symantec tape device drivers by running tapeinst.exe

- 1 From the Backup Exec installation directory, double-click the `tapeinst.exe` file.

The default installation directory is `C:\Program Files\Symantec\Backup Exec`.

- 2 On the **Symantec Device Driver Installation Wizard**, follow the on-screen prompts.

## Using the Symantec Device Driver Installation Wizard to install tape device drivers

You can install Symantec tape device drivers by using the **Symantec Device Driver Installation Wizard**.

See “[About installing Symantec tape device drivers](#)” on page 336.

### To use the Symantec Device Driver Installation Wizard to install tape device drivers

- 1 On the **Storage** tab, in the **Configure** group, click **Configure Storage**.
- 2 On the wizard panel, select **Tape Storage**, and then click **Next**.

- 3 Select **Install tape device drivers**, and then click **Next**.
- 4 On the **Symantec Device Driver Installation Wizard**, follow the on-screen prompts.

## Editing tape drive properties

You can edit the following tape drive properties:

- Hardware compression, if the drive supports compression.
- The preferred block size, buffer size, buffer count, and high water count.
- The read and write settings for single block mode.
- The read and write settings for SCSI pass-through mode.

See [“About tape drives and robotic libraries”](#) on page 334.

### To view tape drive properties

- 1 On the **Storage** tab, double-click the tape drive for which you want to view properties.
- 2 In the left pane, click **Properties**.
- 3 Make changes as appropriate.  
See [“Tape drive properties”](#) on page 338.
- 4 Click **Apply**.

## Tape drive properties

Properties provide detailed information about tape drives.

---

**Caution:** Preferred configuration settings are used to tune the performance of backup and restore operations. Changing preferred configuration settings is not generally recommended and may have a negative effect on your backup performance and system performance. Any changes should be thoroughly tested to make sure that system performance does not deteriorate.

---

See [“Editing tape drive properties”](#) on page 338.

Table 12-1 Tape drive properties

Item	Description
<b>Name</b>	Displays the name of the tape drive. You can edit this field.
<b>Description</b>	Displays the description of the tape drive. You can edit this field.
<b>State</b>	Indicates the status of the tape drive.  See <a href="#">“Backup Exec server and storage device states”</a> on page 434.
<b>Provider</b>	Indicates the type of driver that is in use for the tape drive, such as user mode driver or kernel mode driver.
<b>Reserved by</b>	Indicates the name of the Backup Exec server that is using the tape drive.
<b>Vendor</b>	Displays the name of the vendor of the tape drive.
<b>Product ID</b>	Displays the product ID from the SCSI Inquiry string.
<b>Firmware</b>	Displays the version of the firmware that is used in the tape drive.
<b>Drive type</b>	Displays the type of drive that is detected.
<b>Media type</b>	Displays the type of media that is in this tape drive.
<b>Date in service</b>	Displays the date that this installation of Backup Exec detected this tape drive.
<b>Serial number</b>	Displays the serial number of the tape drive.
<b>Primary inquiry string</b>	Displays information that is read from the tape drive firmware.
<b>Compression</b>	Indicates if hardware compression is enabled.  If this option is available, this drive is capable of supporting hardware compression.  If you configure a job to use hardware compression, and hardware compression is disabled on the device, then hardware compression is unavailable and is not used.

**Table 12-1**      Tape drive properties (*continued*)

Item	Description
<p><b>Block size</b></p>	<p>Displays the size of the blocks of data that are written to new media in this tape drive. The default is the preferred block size.</p> <p>Some devices (for example, LTO devices) provide better performance when larger block sizes are used. The preferred block size can range from 512 bytes to 64 kilobytes or larger. If you use a tape drive that supports larger block sizes, you can change the tape drive's block size. However, if the tape drive does not allow a block size as large as you want, reconfigure the host bus adapter or the tape drive. After you reconfigure the hardware and restart the Backup Exec services, check if the block size that you want to use is available.</p> <p>See the tape drive manufacturer's documentation for help in configuring the device.</p> <p>Backup Exec does not ensure that the requested block size is supported by that tape drive. You should check the tape drive specifications to make sure that the block size is supported. If the tape drive does not support a block size, it defaults to its standard block size.</p> <p>If the tape drive does not support block size configuration, this option is unavailable.</p>
<p><b>Buffer size</b></p>	<p>Displays the amount of data that is sent to the tape drive on each read or write request. The buffer size must be equal to the block size or an even multiple of the block size.</p> <p>Depending on the amount of memory in your system, increasing this value may improve tape drive performance. Each type of tape drive requires a different buffer size to achieve maximum throughput.</p>

**Table 12-1** Tape drive properties (*continued*)

Item	Description
<b>Buffer count</b>	<p>Displays the number of buffers that are allocated for this tape drive.</p> <p>Depending on the amount of memory in your system, increasing this value may improve device performance. Each type of tape drive requires a different number of buffers to achieve maximum throughput.</p> <p>If you change the buffer count, you may need to adjust the high water count accordingly.</p>
<b>High water count</b>	<p>Displays the number of buffers to be filled before data is first sent to the tape drive, and any time that the tape drive underruns.</p> <p>The high water count cannot exceed the buffer count. A value of 0 disables the use of high water logic; that is, each buffer is sent to the device as it is filled.</p> <p>The default setting provides satisfactory performance in most instances; in some configurations, throughput performance may be increased when other values are specified in this field. If you increase or decrease the buffer count, the high water count should be adjusted accordingly. If a tape drive has a high water count default of 0, it should be left at 0.</p>
<b>Default Settings</b>	Returns all of the preferred configuration settings to their defaults.
<b>Read single block mode</b>	<p>Indicates if this tape drive reads only one block of data at a time, regardless of the size of the buffer block.</p> <p>This option is disabled by default.</p>
<b>Write single block mode</b>	<p>Indicates if this tape drive writes only one block of data at a time. This option provides greater control over the handling of data write errors.</p> <p>Symantec recommends that you select this option if the tape drive is shared.</p> <p>This option is enabled by default.</p>

**Table 12-1** Tape drive properties (*continued*)

Item	Description
<b>Read SCSI pass-through mode</b>	<p>Indicates if this tape drive reads data without going through a Microsoft tape device API. This option allows the data to pass directly through the tape drive and allows more detailed information if device errors occur.</p> <p>This option is disabled by default.</p>
<b>Write SCSI pass-through mode</b>	<p>Indicates if this tape drive writes data without going through the Microsoft tape device API. This option allows data to pass directly through the device driver and allows more detailed information if device errors occur.</p> <p>Symantec recommends that you select this option if the tape drive is shared.</p> <p>This option is enabled by default.</p>
<b>Connection type</b>	<p>Indicates if the tape drive is locally attached to the Backup Exec server, or if it is on a remote server.</p> <p>A connection type of SCSI does not imply that a parallel SCSI interface is in use. Connection type refers to the SCSI protocol. The interface may be SCSI, SAS, FC, and so on.</p>
<b>Restart needed</b>	<p>Indicates if the Backup Exec services must be restarted to apply any changes that are made to this tape drive.</p> <p>See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.</p>
<b>Port</b>	<p>Displays the identifying number of the port on the server to which the tape drive is attached.</p>
<b>Bus</b>	<p>Displays the identifying number of the bus to which the tape drive is attached.</p>
<b>Target ID</b>	<p>Displays the unique SCSI ID number (physical unit number).</p>
<b>LUN</b>	<p>Displays the logical unit number of the tape drive.</p>

# Enabling or disabling hardware compression for tape drives

You can enable or disable hardware compression for a tape drive if the drive supports compression.

See [“Tape drive properties”](#) on page 338.

## To enable or disable hardware compression for tape drives

- 1 On the **Storage** tab, double-click the tape drive for which you want to enable or disable hardware compression.
- 2 In the left pane, click **Properties**.
- 3 In the **Hardware compression** field, on the drop-down menu, click **Enabled** or **Disabled**.
- 4 Click **Apply**.

# Changing the block size, buffer size, buffer count, and high water count for tape drives

---

**Caution:** Use the preferred configuration settings to tune the performance of tape drives during backup and restore operations. Changing preferred configuration settings is not generally recommended and may have a negative effect on backup performance and system performance. Thoroughly test any changes before you put them into general use to ensure that system performance does not deteriorate.

---

## To change the preferred block size, buffer size, buffer count, and high water count for tape drives

- 1 On the **Storage** tab, double-click the tape drive for which you want to change settings.
- 2 In the left pane, click **Properties**.
- 3 Change the appropriate settings.  
See [“Tape drive properties”](#) on page 338.
- 4 To reset the values to the default settings, click **Default settings**.
- 5 Click **Apply**.

## Changing the settings to read and write in single block mode for tape drives

For a tape drive, you can enable or disable the reading and writing of one block of data at a time.

See [“Tape drive properties”](#) on page 338.

**To change the settings to read and write in single block mode**

- 1 On the **Storage** tab, double-click the tape drive for which you want to enable reading or writing in single block mode.
- 2 In the left pane, click **Properties**.
- 3 In the **Read single block mode** or **Write single block mode** fields, on the drop-down menu, click **Enabled** or **Disabled**.
- 4 Click **Apply**.

## Changing the settings to read and write in SCSI pass-through mode for tape drives

For a tape drive, you can enable or disable the reading and writing in SCSI pass-through mode.

See [“Tape drive properties”](#) on page 338.

**To change the settings to read and write in SCSI pass-through mode**

- 1 On the **Storage** tab, double-click the tape drive for which you want to enable reading or writing in SCSI pass-through mode.
- 2 In the left pane, click **Properties**.
- 3 In the **Read SCSI pass-through mode** or **Write SCSI pass-through mode** fields, on the drop-down menu, click **Enabled** or **Disabled**.
- 4 Click **Apply**.

## Viewing tape drive statistics

You can view statistics about tape drives.

See [“About tape drives and robotic libraries”](#) on page 334.

**To view tape drive statistics**

- 1 On the **Storage** tab, double-click the tape drive for which you want to view statistics.
- 2 In the left pane, click **Statistics**.  
See “[Tape drive statistics](#)” on page 345.

## Tape drive statistics

Statistics include the date the device was last mounted, device totals such as the total number of bytes written and read, and device errors. Media, head cleaning, and head wear affect error rates. Information includes only the statistics that are gathered after Backup Exec first discovers the tape drive.

The documentation that is included with your tape drive should list the acceptable limits for hard and soft errors; if not, check with the hardware manufacturer.

See “[Viewing tape drive statistics](#)” on page 344.

**Table 12-2** Tape drive statistics

<b>Item</b>	<b>Description</b>
<b>Last mount date</b>	Displays the last date that the device mounted a media.
<b>Total bytes written</b>	Displays the number of bytes that this device has written.
<b>Total bytes read</b>	Displays the number of bytes that this device has read.
<b>Total mounts</b>	Displays the number of times that this device has mounted a media.
<b>Total seeks</b>	Displays the total number of seek operations that this device has performed. Seek operations are run to locate a specific piece of information.
<b>Total hours in use</b>	Displays the total number of hours that this device has been in use performing read, write, mount, and seek operations.

**Table 12-2**      Tape drive statistics (*continued*)

<b>Item</b>	<b>Description</b>
<b>Seek error</b>	Displays the number of errors that were encountered while locating data.
<b>Soft read errors</b>	Displays the number of recoverable read errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the device and perform maintenance on it, and check the media for damage.
<b>Hard read errors</b>	Displays the number of unrecoverable read errors that were encountered. If you receive hard errors, check the device and perform maintenance on it, and check the media for damage.
<b>Soft write errors</b>	Displays the number of recoverable write errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the device and perform maintenance on it, and check the media for damage.
<b>Hard write errors</b>	Displays the number of unrecoverable write errors that were encountered. If you receive hard errors, check the device and perform maintenance on it, and check the media for damage.

**Table 12-2** Tape drive statistics (*continued*)

<b>Item</b>	<b>Description</b>
<b>Last cleaning date</b>	Displays the last date a cleaning operation was performed on the device.
<b>Hours since last cleaning</b>	Displays the number of hours that the device has been in use since the last cleaning.
<b>Reset cleaning statistics</b>	Resets all cleaning statistics to zero. You cannot undo this operation.
<b>Bytes written</b>	Displays the number of bytes that this device has written since the last cleaning.
<b>Bytes read</b>	Displays the number of bytes that this device has read since the last cleaning.
<b>Total mounts</b>	Displays the number of times that this device has mounted media since the last cleaning.
<b>Total seeks</b>	Displays the total number of seek operations that this device has performed since the last cleaning. Seek operations are run to locate a specific piece of information.
<b>Hours in use</b>	Displays the total number of hours that this device has been in use since the last cleaning.
<b>Seek errors</b>	Displays the number of seek errors that were encountered since the last cleaning.

**Table 12-2**      Tape drive statistics (*continued*)

<b>Item</b>	<b>Description</b>
<b>Soft read errors</b>	Displays the number of recoverable read errors that were encountered since the last cleaning. Soft errors may indicate the beginning of a problem. If excessive errors are reported for your environment, check the device and perform maintenance on it, and check the media for damage.
<b>Hard read errors</b>	Displays the number of unrecoverable read errors that were encountered since the last cleaning. If you receive hard errors, check the device and perform maintenance on it, and check the media for damage.
<b>Soft write errors</b>	Displays the number of recoverable write errors that were encountered since the last cleaning. Soft errors may indicate the beginning of a problem. If excessive errors are reported for your environment, check the device and perform maintenance on it, and check the media for damage.
<b>Hard write errors</b>	Displays the number of unrecoverable write errors that were encountered since the last cleaning. If you receive hard errors, check the device and perform maintenance on it, and check the media for damage.

## About robotic libraries in Backup Exec

Backup Exec's Advanced Device and Media Management (ADAMM) feature solves the problems that are associated with typical robotic library modules. Backup Exec accesses all of the media in the robotic library and uses the media that belongs to the specified media set. If the backup job exceeds the capacity of a media, Backup Exec searches all of the media that is contained in the robotic library and finds a suitable media to use.

For example, an operator has a robotic library with six slots. The operator inserts six blank tapes and targets backup jobs to various media sets within the robotic library. Backup Exec automatically allocates available tapes in the robotic library. If a job exceeds the capacity of one tape and another overwritable tape is available in the robotic library, the job automatically continues on that tape. When Backup Exec runs out of tapes, it prompts the operator to import overwritable media.

In a robotic library, Backup Exec selects the oldest recyclable media in the library to use first. If more than one media that meets the requirements is found, Backup Exec selects the media in the lowest-numbered slot. For example, Backup Exec selects media in slot 2 before it selects equivalent media in slot 4.

For restore jobs that use robotic libraries, Backup Exec accesses the source media regardless of its sequential placement in the magazine. For example, if the data for a restore job resides on two media in the magazine, the media do not have to be placed in adjacent slots for Backup Exec to restore the data. If Backup Exec does not find the media that is required for the restore job in the robotic library, an alert is generated that requests the media that is necessary to complete the job.

See [“Requirements for setting up robotic library hardware”](#) on page 349.

See [“About the Virtual Tape Library Unlimited Drive Option ”](#) on page 334.

See [“About the Library Expansion Option ”](#) on page 335.

See [“Configuring robotic library partitions”](#) on page 356.

See [“Removing robotic library partitions”](#) on page 357.

See [“About robotic library partitions”](#) on page 355.

## Requirements for setting up robotic library hardware

You can configure Backup Exec to work with robotic library drives by making associations between the robotic library's drives, robotic arm, and Backup Exec. Backup Exec supports serialized drives. Manual configuration of serialized drives is not required.

You can find a list of supported types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

Ensure that the robotic library hardware is configured as follows:

- Ensure that the robotic arm is set to Random mode. Refer to your robotic library documentation for more information.
- Ensure the following for a multi-LUN robotic library:
  - The controller card is set to support multiple LUNs (if supported).
  - The target LUN for the tape drive is lower than the target LUN for the robotic library.
- Determine which drive is the first drive in the robotic library, and then arrange the SCSI IDs to match the sequence of the drive element addresses. Refer to your robotic library documentation to determine the drive element address for each storage device.
- Ensure that the SCSI ID of the robotic arm precedes the SCSI IDs of the drives in the robotic library. Do not use 0 or 1 because these SCSI IDs are typically reserved for boot devices.

In the following example, if your robotic library has two drives, the drive with the lowest drive element address should be assigned the lower SCSI ID.

**Table 12-3** Example configuration for a multi-drive robotic library

Data transfer element (storage devices )	SCSI ID	Drive element address
Robotic arm	4	N/A
Storage device 0	5	00008000
Storage device 1	6	00008001

See “[About robotic libraries in Backup Exec](#)” on page 349.

## Inventorying robotic libraries when Backup Exec services start

You can set a default so that all robotic libraries are included in the inventory job whenever Backup Exec services are started. Symantec recommends that you enable this default if media is often moved between robotic libraries. Backup Exec may take longer to start.

See “[About inventorying a storage device](#)” on page 422.

### To inventory robotic libraries when Backup Exec services start

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Storage**.  
See [“Global settings for storage”](#) on page 415.
- 3 Click **Inventory robotic libraries when Backup Exec services start**.
- 4 Click **OK**.

## Initializing a robotic library when the Backup Exec service starts

You can initialize a robotic library whenever the Backup Exec services start.

During startup, if media is in the drives in the robotic library, Backup Exec attempts to return the media to its original drive. If the media cannot be returned to the drive, an error message appears that prompts you to eject the media from the drive.

You can also create a job to initialize a robotic library.

See [“Initializing a robotic library”](#) on page 426.

See [“About robotic libraries in Backup Exec”](#) on page 349.

### To initialize a robotic library when the Backup Exec services start

- 1 On the **Storage** tab, double-click the robotic library that you want to initialize.
- 2 In the left pane, click **Properties**.
- 3 In the **Startup initialization** field, in the drop-down menu, click **Enabled**.
- 4 Click **Apply**.

## Defining a cleaning slot

Before submitting a cleaning job, you must define a cleaning slot that contains the cleaning tape.

Make sure that the cleaning tape is located in the slot that you defined as the cleaning slot. After defining the cleaning slot, you can set up a cleaning job for the robotic library drive.

See [“Cleaning a robotic library drive”](#) on page 429.

Defined cleaning slots are not inventoried when an inventory job runs.

**To define a cleaning slot**

- 1 On the **Storage** tab, expand the robotic library, and then double-click **Slots**.
- 2 Double-click the slot that contains the cleaning tape.
- 3 In the **Cleaning slot** field, click the drop-down menu, and then click **Yes**.
- 4 Click **Apply**.

## Viewing robotic library properties

You can view robotic library properties.

See [“About robotic libraries in Backup Exec”](#) on page 349.

**To view robotic library properties**

- 1 On the **Storage** tab, double-click the robotic library for which you want to view properties.
- 2 In the left pane, click **Properties**.

See [“Robotic library properties”](#) on page 352.

## Robotic library properties

Properties for robotic libraries include information about the status, type, and vendor of the device.

See [“Viewing robotic library properties”](#) on page 352.

**Table 12-4**      Robotic library properties

Item	Description
<b>Name</b>	Displays the name of the robotic library. You can edit this field.
<b>Description</b>	Displays the description of the robotic library. You can edit this field.  By default, Backup Exec displays the device's inquiry string, which is the vendor name and product ID.
<b>Status</b>	Displays the status of the robotic library.  See <a href="#">“Changing the state of a storage device to online”</a> on page 425.  See <a href="#">“Troubleshooting hardware-related issues”</a> on page 650.

**Table 12-4**      Robotic library properties (*continued*)

Item	Description
<b>Vendor</b>	Displays the name of the vendor of the drive or robotic library.
<b>Product ID</b>	Displays the product ID from the SCSI Inquiry string.
<b>Firmware</b>	Displays the version of the firmware that is used in the device.
<b>Library type</b>	<p>Displays the default first slot of the robotic library.</p> <p>The string <b>VTL</b> identifies virtual tape libraries. The string <b>TLS</b> identifies simulated tape libraries that the Tape Library Simulator Utility creates. See “<a href="#">About the Tape Library Simulator Utility</a>” on page 1149.</p>
<b>Date in service</b>	Displays the date that this installation of Backup Exec first detected this device.
<b>Serial number</b>	Displays the serial number of the library.
<b>Primary inquiry string</b>	Displays information that is read from the library firmware.
<b>Startup initialization</b>	<p>Indicates if Backup Exec initializes the robotic library when the Backup Exec service is started. Depending upon the type of robotic library, initialization can determine which slots have media and can read all barcode labels on media.</p> <p>You may want to enable this option if the library does not initialize itself when it starts. However, if multiple servers share the library, you should not enable this option since each server must initialize the library. Other servers cannot access the library until all of the initialization processes are complete. If you do not want to initialize the library at startup, you can run an initialization job at any time.</p> <p>The default setting is <b>Disabled</b>.</p>

**Table 12-4**      Robotic library properties (*continued*)

Item	Description
<b>First slot number</b>	Depicts the starting slot for this robotic library. Backup Exec determines what the starting slot should be for this type of library. Some robotic libraries have slots that start at 0. Other libraries start at 1. You can change the starting slot if necessary.
<b>Connection type</b>	Indicates if the robotic library is locally attached to the Backup Exec server or if it is on a remote server.  A connection type of SCSI does not imply that a parallel SCSI interface is in use. Connection type refers to the SCSI protocol. The interface may be SCSI, SAS, FC, and so on.
<b>Restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this robotic library.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.
<b>Port</b>	Displays the identifying number of the port on the server to which the robotic library is attached.
<b>Bus</b>	Displays the identifying number of the bus to which the robotic library is attached.
<b>Target ID</b>	Displays the unique SCSI ID number (physical unit number).
<b>LUN</b>	Displays the logical unit number of the robotic library.

## Viewing jobs, job histories, and active alerts for a robotic library

For each robotic library, you can view the following details:

- Jobs that run on the robotic library
- Job histories
- Active alerts

See [“About robotic libraries in Backup Exec”](#) on page 349.

**To view jobs, job histories, and active alerts for a robotic library**

- 1 On the **Storage** tab, right-click the robotic library, and then click **Details**.
- 2 In the left pane, click the appropriate tab.  
See [“About managing and monitoring active and scheduled jobs”](#) on page 247.  
See [“About alerts”](#) on page 279.

## About robotic library partitions

You can group one or more robotic library slots into partitions. Partitioning robotic library slots provides you with more control over which tape is used for backup jobs. When you create robotic library partitions, Backup Exec creates a storage device pool for each partition. Jobs that you send to a partition's storage device pool run on the media that is located in the partition's slots. For example, if you set up a partition that contains slots 1 and 2 and you want to run a weekly backup only on the media in these slots, you would submit the job to the storage device pool for the partition that contains slots 1 and 2. The storage device pools for robotic library partitions appear in the drop-down menu for the **Storage** field when you edit the backup job. All storage device pools for a robotic library partition have the same name and display the slot ranges for the partition in parentheses within the name.

Partitions can include any number of robotic library slots. However, you cannot move or delete the first partition when other partitions exist.

Depending on the robotic library configuration, the first slot may be numbered 1 or 0. If the robotic library uses a zero-based slot configuration and you assign the first partition to begin with slot 1, the Partition Utility will actually use slot 0 as the first slot for partition 1 and adjust the starting slot accordingly for all other partitions.

When the robotic library is partitioned, Backup Exec searches for the oldest recyclable media in the targeted partition only. If more than one media is found that meets the requirements, Backup Exec then selects the media in the lowest-numbered slot; for example, media in slot 2 is selected before equivalent media in slot 4.

You can create a partitioning scheme that best suits your environment. For example, some administrators may create partitions based on users and groups, while others may create partitions according to operation types.

See [“Editing the properties of a robotic library partition”](#) on page 356.

See [“Configuring robotic library partitions”](#) on page 356.

## Editing the properties of a robotic library partition

You can edit the properties of a robotic library partition.

See [“About robotic library partitions”](#) on page 355.

### To edit the properties of a robotic library partition

- 1 On the **Storage** tab, double-click the robotic library partition.
- 2 In the left pane, click **Properties**.
- 3 View or edit the properties as appropriate.

See [“Robotic library partition properties”](#) on page 356.

## Robotic library partition properties

You can select the tape drives that you want to add to the robotic library partition.

See [“Editing the properties of a robotic library partition”](#) on page 356.

**Table 12-5** Robotic library partition properties

Item	Description
<b>Name</b>	Displays the name of the robotic library partition. You can edit this field.
<b>Description</b>	Displays the description of the robotic library partition. You can edit this field.
<b>Tape drive</b>	Indicates if the tape drive is added to the robotic library partition.

## Configuring robotic library partitions

You can configure partitions for robotic library slots.

See [“About robotic library partitions”](#) on page 355.

### To configure robotic library partitions

- 1 On the **Storage** tab, right-click the robotic library for which you want to create partitions.
- 2 Click **Configure partitions**.
- 3 Follow the on-screen prompts.

## Removing robotic library partitions

You can remove one or all partitions from a robotic library.

See [“About robotic library partitions”](#) on page 355.

### To remove robotic library partitions

- 1 On the **Storage** tab, right-click the robotic library from which you want to remove a partition.
- 2 Click **Configure partitions**.
- 3 Follow the on-screen prompts.

## Reassigning a slot base number for robotic libraries

Backup Exec automatically assigns slot base numbers for robotic libraries. If necessary, you can reassign how robotic library slots are displayed in Backup Exec. Slot base numbers in some robotic libraries start at 0, while slots in other robotic libraries start at 1. If the robotic library uses a zero-based slot configuration, you can reassign how the slots are displayed.

See [“About robotic libraries in Backup Exec”](#) on page 349.

### To reassign a slot base number for robotic libraries

- 1 On the **Storage** tab, double-click the robotic library for which you want to reassign a slot base number.
- 2 In the **First slot number** field, click the drop-down menu to change the base number.
- 3 Click **Apply**.

## Viewing robotic library slot properties or backup sets

You can view the properties of a robotic library slot and any backup sets that are stored on the media in that slot.

See [“About robotic libraries in Backup Exec”](#) on page 349.

### To view robotic library slot properties or backup sets

- 1 On the **Storage** tab, double-click the robotic library.
- 2 In the left pane, click **Slots**.
- 3 Double-click the slot for which you want to view properties.



**Table 12-6** Robotic library slot properties (*continued*)

Item	Description
<b>Media label</b>	<p>Displays the media label as one of the following:</p> <ul style="list-style-type: none"><li>■ A label that Backup Exec automatically assigns.</li><li>■ A label that the administrator assigns.</li><li>■ A pre-assigned barcode label.</li></ul> <p>You can edit the media label, which is limited to 32 characters. Editing the label changes the name of the media in the display, but does not write the new label to the media until an overwrite operation occurs. When you edit a media label, try to make it a concise identifier that remains constant even when the media is reused. You should write this media label on a label that is fixed to the outside of the physical media.</p> <p>Duplicate labels can be automatically generated. For example, reinstalling Backup Exec or bringing media from another Backup Exec installation can cause duplication in labels. Duplicate labels are allowed, but not recommended.</p> <p>If a barcode is available, and a barcode-equipped device is used, then the media label automatically defaults to that barcode .</p> <p><b>Note:</b> Information from this item down only applies to a slot that contains media.</p>

**Table 12-6**      Robotic library slot properties (*continued*)

Item	Description
<b>Media description</b>	<p>Displays the original media label if the media was imported from another installation of Backup Exec, or from another product.</p> <p>You can edit the media description, which is limited to 128 characters, to make it a more descriptive label.</p>
<b>Media ID</b>	<p>Displays the unique internal label that Backup Exec assigns to each media used in Backup Exec. The ID keeps statistics for each media. You cannot change or erase the media ID.</p>
<b>Media type</b>	<p>Displays the media type and subtype (if available). Click the button next to the field to change the media type or subtype.</p>
<b>Export pending</b>	<p>Displays Yes if there is an associated operation to export this media.</p> <p>See <a href="#">“Robotic library slot properties”</a> on page 432 on page 432.</p>
<b>Media set</b>	<p>Displays the name of the media set that this media belongs to.</p> <p>See <a href="#">“About media sets”</a> on page 366.</p>
<b>Media location</b>	<p>Displays the name of the device or vault where this media is located.</p> <p>See <a href="#">“About media vaults”</a> on page 384.</p>
<b>Creation date</b>	<p>Displays the date and time when the media was first entered into Backup Exec.</p>
<b>Allocated date</b>	<p>Displays the date and time when the media was added to a media set as a result of an overwrite operation.</p>

Table 12-6 Robotic library slot properties (*continued*)

Item	Description
<b>Modified date</b>	Displays the date and time when data was last written to the media.
<b>Overwrite protection until</b>	Displays the date and time after which the media can be overwritten.
<b>Appendable until</b>	Displays the date and time after which the media can no longer be appended to.
<b>Supports HW encryption</b>	Displays <b>Yes</b> if this media supports hardware encryption.
<b>Total capacity</b>	Displays the amount of expected total raw capacity of the media. Some tape devices support the ability to read the amount of total capacity of the media that is currently loaded in the device. If a tape device supports reading of the total capacity amount, then <b>Total capacity</b> is derived from the <b>Total capacity</b> amount. Otherwise, <b>Total capacity</b> is estimated based on past usage of the media.
<b>Total backup storage</b>	Displays the expected amount of total raw capacity of the media.
<b>Used capacity</b>	Displays the amount of raw capacity on the media that has been used. <b>Used capacity</b> is calculated when <b>Available capacity</b> is subtracted from <b>Total capacity</b> . <b>Used capacity</b> may or may not equal <b>Bytes written</b> .
<b>Amount of data written</b>	Displays the amount of data written to the media in this slot.

**Table 12-6**      Robotic library slot properties (*continued*)

Item	Description
<b>Available capacity</b>	<p>Displays the amount of expected raw capacity on the media that remains unused. Some tape devices support the ability to read the amount of remaining capacity of the media that is currently loaded in the device. If a tape device supports reading of the remaining capacity amount, then <b>Available capacity</b> is derived from the remaining capacity amount. Otherwise, <b>Available capacity</b> is calculated when <b>Bytes written</b> is subtracted from <b>Total capacity</b>.</p> <p>Because free space is reported in terms of unused raw capacity, review <b>Bytes written</b> and <b>Compression ratio</b> to estimate if there is enough free space for a specific job.</p>
<b>Compression ratio</b>	<p>Displays the ratio of <b>Bytes written</b> to <b>Used capacity</b>. <b>Compression ratio</b> shows the overall effect that data compression and media flaws have on the amount of data that is stored on the media.</p>
<b>Mounts</b>	<p>Displays the number of times this media has been mounted.</p>
<b>Seeks</b>	<p>Displays the total number of seek operations that have been performed on this media. Seek operations are run to locate a specific piece of information on the media.</p>
<b>Seek errors</b>	<p>Displays the number of errors that are encountered while locating data.</p>

**Table 12-6**      Robotic library slot properties (*continued*)

<b>Item</b>	<b>Description</b>
<b>Soft write errors</b>	Displays the number of recoverable write errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the media for damage.
<b>Hard write errors</b>	Displays the number of unrecoverable write errors that were encountered. If you receive hard errors, check the media for damage.
<b>Soft read errors</b>	Displays the number of recoverable read errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the media for damage.
<b>Hard read errors</b>	Displays the number of unrecoverable read errors that were encountered. If you receive hard errors, check the media for damage.



# Tape and disk cartridge media

This chapter includes the following topics:

- [About tape and disk cartridge media](#)
- [Viewing audit log entries for tape and disk cartridge media operations](#)
- [About labeling tape and disk cartridge media](#)
- [About WORM media](#)
- [About media vaults](#)
- [About retiring damaged media](#)
- [About deleting media](#)
- [About erasing media](#)
- [About cataloging media that contains encrypted backup sets](#)
- [Associating media with a media set](#)
- [Editing media properties](#)
- [Media rotation strategies](#)

## About tape and disk cartridge media

For tape and disk cartridge media, you can perform the following actions:

- Protect data from being overwritten.
- Set up media rotation strategies.

- Track the location of media.
- Label media automatically.
- Read and track the media labels that have barcodes.
- Collect and report media statistics.

The Advanced Device and Media Management (ADAMM) feature in Backup Exec automatically selects the tape cartridge media and the disk cartridge media for jobs. Backup Exec keeps track of all tape cartridge media and disk cartridge media that is loaded into the attached storage. Backup Exec also keeps track of the media that is offline and the media that has been placed in media vaults.

For data that is kept on disk and cloud storage, Backup Exec uses data lifecycle management to automatically expire backup sets.

See [“About media sets”](#) on page 366.

See [“Media rotation strategies”](#) on page 398.

See [“About keeping backup sets”](#) on page 213.

## About media sets

A media set consists of the following rules that apply to the media in tape and disk cartridges:

- How long to protect the data on the media from overwrite. This is called the overwrite protection period.
- How long to append data to a media. This is called the append period.
- When and where to send media for vaulting.

Media that are associated with a media set are allocated media. Allocated media have current append and overwrite protection periods. Media that are associated with a media set but have expired overwrite protection periods are recyclable media.

Some media sets are created automatically when you install Backup Exec. Backup Exec creates system media sets that you cannot modify. System media sets are described in the following table.

**Table 13-1** System media sets

Name	Description
<b>Backup Exec and Windows NT Backup Media</b>	Lists all media that is imported from another installation of Backup Exec.  See <a href="#">“Cataloging a storage device”</a> on page 424.

Table 13-1 System media sets (continued)

Name	Description
<b>Cleaning Media</b>	Lists all cleaning media. See <a href="#">“Cleaning a robotic library drive”</a> on page 429.
<b>Foreign Media</b>	Lists all media that is imported from a product other than Backup Exec. See <a href="#">“About restoring media created with other backup software”</a> on page 239. See <a href="#">“Cataloging a storage device”</a> on page 424.
<b>Retired Media</b>	Lists all media that you have taken out of service, usually because of an excessive number of errors. After you associate a media with the retired media set, Backup Exec does not select it for backup jobs. The media is still available for restore operations, if it has not been damaged. <b>Retired Media</b> protects media from being used (overwritten). You can delete the media that is in <b>Retired Media</b> to remove it from Backup Exec. You may want to delete media if you have a lot of off-site media that you do not want to recycle. You can also delete media if you throw away the media. See <a href="#">“About retiring damaged media”</a> on page 388.
<b>Scratch Media</b>	Lists all media that can be overwritten. New, blank, and erased media are automatically associated with the <b>Scratch Media</b> set. See <a href="#">“About media overwrite protection and append periods”</a> on page 369.

Backup Exec creates the following default media sets:

**Table 13-2** Default user media sets

Name	Description
<p><b>Keep Data for 4 Weeks</b></p>	<p>Lists all media that you associate with this media set. If you use the backup job defaults that are set when you install Backup Exec, the media set <b>Keep Data for 4 Weeks</b> is the default media set for all backup jobs. This media set protects data from being overwritten for four weeks and allows the media to be appended to for six days.</p> <p>You can edit and rename <b>Keep Data for 4 Weeks</b> after installation. Therefore, it may not continue to appear in the <b>Media</b> view or in the backup job defaults as <b>Keep Data for 4 Weeks</b>.</p> <p>See <a href="#">“About the default media set Keep Data for 4 Weeks”</a> on page 373.</p>
<p><b>Keep Data Infinitely - Do Not Allow Overwrite</b></p>	<p>Lists all media that you associate with this media set.</p> <p>When you associate media with this media set, data is not overwritten unless you perform any of the following actions on the media:</p> <ul style="list-style-type: none"> <li>■ Erase</li> <li>■ Label</li> <li>■ Format.</li> <li>■ Associate the media with the scratch media set</li> </ul> <p>You can append data to this media for an infinite period (until the media is full).</p> <p>You can edit and rename <b>Keep Data Infinitely - Do Not Allow Overwrite</b> after installation. Therefore, it may not continue to appear in the <b>Media</b> view or in the backup job defaults as <b>Keep Data Infinitely - Do Not Allow Overwrite</b>.</p>

See [“Viewing all media sets”](#) on page 368.

See [“About media overwrite protection and append periods”](#) on page 369.

See [“Creating media sets for tape and disk cartridge media”](#) on page 373.

See [“Creating media vault rules to move media to and from media vaults”](#) on page 386.

## Viewing all media sets

You can view the system media sets and the user media sets, which are the media sets that you create.

See [“About media sets”](#) on page 366.

To view all media sets

- ◆ On the **Storage** tab, double-click **All Media Sets**.

## About media overwrite protection and append periods

Each media is associated with a media set, which is a set of rules that manage media.

These rules include overwrite protection and append periods.

**Table 13-3** Overwrite protection and append periods

Rule	Description
Append period	The amount of time that data can be appended to media. It is measured from the time the media was first allocated. It can be specified in hours, days, weeks, or years.

**Table 13-3** Overwrite protection and append periods (*continued*)

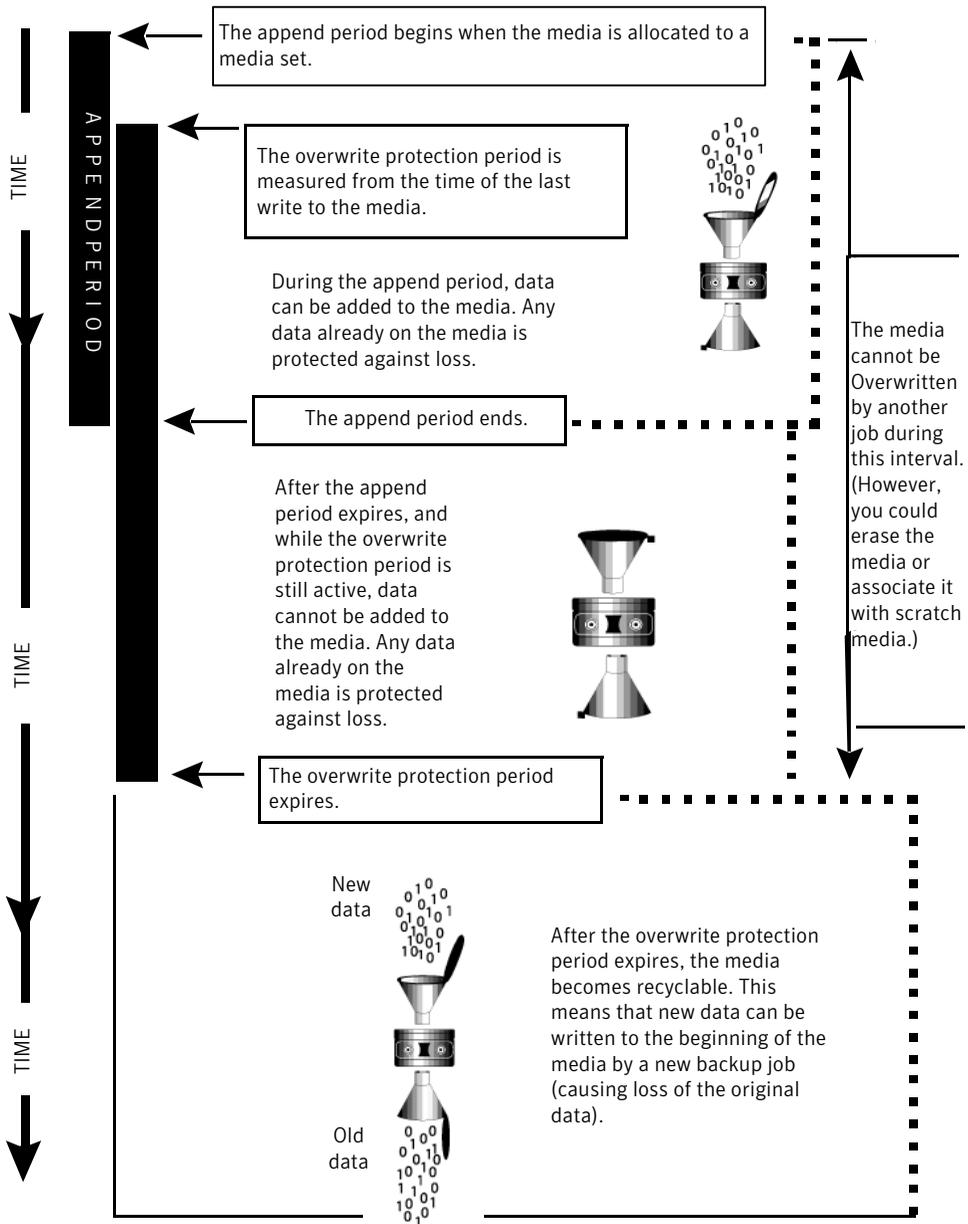
Rule	Description
<p>Overwrite protection period</p>	<p>The amount of time that media is protected from being overwritten. The period is measured from the time of the last write to the media, that is, at the end of the last append or overwrite job. It can be specified in hours, days, weeks, or years. When the overwrite protection period is over, the media becomes recyclable and can be overwritten.</p> <p>The overwrite protection period begins when the backup job is completed. If there is an append period, the overwrite protection period begins again each time an append job completes. Because the overwrite protection period does not begin until the job completes, the amount of time that is required to complete the job takes affects when the media can be overwritten. You may shorten the overwrite protection period to take into account the amount of time a job may run.</p> <p>For example, you set the overwrite protection period for seven days. You also set the append period for four days to ensure that data is not overwritten for at least seven days. The data can be appended to the media for the next four days. The last data that is appended to this media is retained for at least seven days.</p> <p><b>Note:</b> Any media can be overwritten if the overwrite protection level is set to None.</p> <p>See <a href="#">“About media overwrite protection levels for tape and disk cartridge media”</a> on page 377.</p>

Your media rotation strategy must balance between the need to save data as long as possible, and the fact that media are not in infinite supply. The media set rules allow Backup Exec to identify which media can be written to and which media are overwrite-protected. You should consider the use of disk storage for backup data.

See [“About disk storage”](#) on page 307.

The following graphic shows the relationship between the append period and the overwrite protection period.

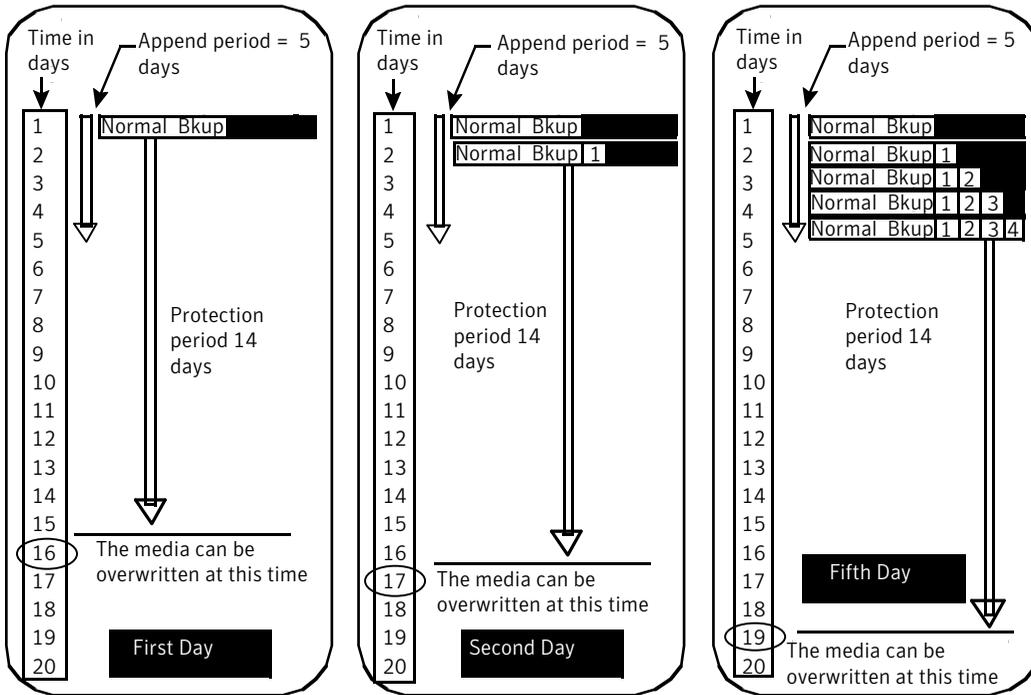
Figure 13-1 Append periods and overwrite protection periods



The append and overwrite protection periods that you specify apply to all the data on the media.

Each time data is written to a media, the time remaining in the overwrite protection period is reset, and the countdown is restarted.

**Figure 13-2** How overwrite protection periods are reset



The amount of time that is required to complete the job takes affects when the media can be overwritten.

For example, suppose that you create a media set named Weekly with an overwrite protection period of seven days. You also specify an append period of zero days, and you schedule a full backup job to run each Friday at 20:00. When it is time for the full backup to run at 20:00 the following Friday, the job cannot run. The first backup job that ran the previous Friday did not complete until 21:10. The overwrite protection period for the Weekly media set still has 70 minutes remaining.

To prevent this situation, you can shorten the overwrite protection period to account for the amount of time a job may run. For this example, the scheduled job recurring at 20:00 can run if the overwrite protection period is set to six days instead of seven days.

## About the default media set Keep Data for 4 Weeks

When you install Backup Exec, a default media set named **Keep Data for 4 Weeks** is created. By default, all of the media that you use for the backup jobs that you create are automatically associated with the media set **Keep Data for 4 Weeks**. The backup data is protected from overwrite for four weeks. The media can be appended to for six days.

You can change the default media set for backup jobs by doing one of the following:

- Create new media sets that have the append and overwrite protection periods set to the time intervals that accommodate your data retention strategy. Then, specify the media set that is most appropriate when you create a backup job. For example, you can create a media set that keeps data for 60 days, and a media set that keeps data for 90 days.
- Select the other default media set **Keep Data Infinitely - Do Not Allow Overwrite** when you create a backup job. The risk that is associated with the media set **Keep Data Infinitely - Do Not Allow Overwrite** is that you can use all of your scratch media. You must continually add new tape or disk cartridge media to Backup Exec.

---

**Note:** Symantec recommends that if you need to keep data longer than four weeks, you should create a duplicate backup job. A duplicate backup job can copy the backup data from the original storage device to tape, which you can then send for long-term or off-site storage.

---

See [“About duplicating backed up data”](#) on page 218.

See [“Creating media sets for tape and disk cartridge media”](#) on page 373.

See [“Associating media with a media set”](#) on page 391.

## Creating media sets for tape and disk cartridge media

A media set consists of the rules that specify the following:

- Append periods
- Overwrite protection periods
- Media vaults
- Amount of time to move media to and from the media vault

The media set rules apply to all of the media that you associate with the media set.

---

**Note:** You must have already created a media vault before you are prompted to add media vault rules in a media set.

---

See [“About media sets”](#) on page 366.

#### To create a media set for tape and disk cartridge media

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**.
- 2 Double-click **All Media Sets**.
- 3 Under **User Media Sets**, right-click a media set, and then click **Create media set**.
- 4 Follow the on-screen prompts.

See [“Media set properties”](#) on page 374.

### Editing media set properties

You can edit the following properties for media sets:

- Name of a media set.
- Overwrite protection and append periods for a media set.
- Media vault and the vaulting periods associated with a media set.

See [“About media sets”](#) on page 366.

#### To edit media set properties

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**.
- 2 Double-click **All Media Sets**.
- 3 Double-click the media set for which you want to view properties.
- 4 In the left pane, click **Properties**, and then make changes as appropriate.

See [“Media set properties”](#) on page 374.

- 5 Click **Apply**.

### Media set properties

Properties for media sets provide information about the overwrite protection period, the append period, and media vaults.

See [“Editing media set properties”](#) on page 374.

Table 13-4 Properties for media sets

Item	Description
<b>Name</b>	Displays the name of the media set.
<b>Description</b>	Displays the description of the media set.
<b>Overwrite protection period</b>	<p>Displays the length of time in hours, days, weeks, or years to retain the data on the media before the media can be overwritten.</p> <p>Regardless of the overwrite protection period that is set, media can be overwritten if you perform the following operations on it:</p> <ul style="list-style-type: none"> <li>■ Erase</li> <li>■ Label</li> <li>■ Associate it with the <b>Scratch Media Set</b></li> <li>■ Set the <b>Media Overwrite Protection Level</b> to <b>None</b></li> <li>■ Format</li> </ul> <p>Because of the method Backup Exec uses to compute time, the unit of time that you enter may be converted. For example, if you enter 14 days, the next time you view this property, it may be displayed as two weeks.</p> <p>The default period is <b>Infinite - Don't Allow Overwrite</b>, which protects the media from being overwritten for 1,000 years.</p> <p>See <a href="#">“About media overwrite protection and append periods”</a> on page 369.</p>
<b>Append period</b>	<p>Displays the length of time in hours, days, or weeks, that data can be added to media. Because of the method Backup Exec uses to compute time, the unit of time that you enter may be converted. For example, if you enter 14 days, the next time you view this property, it may be displayed as two weeks.</p> <p>The append period starts when the first backup job is written to this media.</p> <p>The default period is <b>Infinite - Allow Append</b>, which allows data to be appended until the media capacity is reached.</p>
<b>Media vault to use with this media set</b>	<p>Displays the media vault that stores the media that is associated with this media set.</p> <p>See <a href="#">“About media vaults”</a> on page 384.</p>

**Table 13-4** Properties for media sets (*continued*)

Item	Description
<b>Move media to this vault after</b>	Displays the time period after which this media is reported as ready to be moved to this vault.
<b>Return media from this vault after</b>	Displays the time period after which this media is reported as ready to be returned from this vault.

## Deleting a media set

If you delete a media set that has scheduled jobs associated with it, you are prompted to associate the jobs to another media set.

---

**Caution:** Ensure that the media set that you associate the jobs with has the appropriate overwrite protection and append periods.

---

See [“About media sets”](#) on page 366.

### To delete a media set

- 1 On the **Storage** tab, expand **All Media Sets**.
- 2 Right-click the media set that you want to delete, and then click **Delete**.
- 3 When you are prompted to delete the media set, click **OK**.

## Renaming a media set

When you rename a media set, any jobs that use that media set display the new media set name.

See [“About media sets”](#) on page 366.

### To rename a media set

- 1 On the **Storage** tab, expand **All Media Sets**.
- 2 Right-click the media set that you want to rename, and then click **Details**.
- 3 In the left pane, click **Properties**.
- 4 In the **Name** field, type the new name that you want to assign to this media set, and then click **Apply**.

## About media overwrite protection levels for tape and disk cartridge media

The media overwrite protection level is a global setting that supersedes the media set's overwrite protection period. Although the terms are similar, the media overwrite protection level and the media overwrite protection period are different. The media overwrite protection period is a time interval that changes from one media set to another. The media overwrite protection level specifies whether to overwrite scratch, imported, or allocated media, regardless of the media's overwrite protection period.

Use the media overwrite protection level to specify the type of media that you want to be available for overwrite backup jobs.

See [“Global settings for storage”](#) on page 415.

See [“About media overwrite protection and append periods”](#) on page 369.

## About overwriting allocated or imported media for tape and disk cartridge media

Media that are associated with a media set are called allocated media. Media that are imported from another installation of Backup Exec, or from another product are called imported media. Backup Exec protects allocated and imported media from being overwritten when full or partial overwrite protection is used. However, you can let Backup Exec overwrite allocated and imported media before the data overwrite protection period expires, and without setting the media overwrite protection level to None.

The following methods are available:

- Associate the media with the **Scratch Media Set**. The media is overwritten when it is selected for an overwrite job.
- Erase the media. Erased media is automatically recognized as scratch media and is overwritten immediately.
- Label the media. The **Label Media** operation immediately writes a new media label on the media, which destroys any data that is contained on the media.
- Format the media. Formatting destroys any data that is contained on the media.
- Change the overwrite protection period for the media set so that it is expired.

See [“About tape and disk cartridge media”](#) on page 365.

See [“About deleting media”](#) on page 389.

See [“Editing global settings for storage”](#) on page 415.

## How Backup Exec searches for overwritable media in tape drives and disk cartridges

Media overwrite options set the order in which Backup Exec searches for overwritable media in tape drives and disk cartridges. When Backup Exec searches for overwritable media for a backup job, it searches for either scratch media or media that has an expired overwrite protection period.

You are prompted to select one of the following options that you want Backup Exec to use first:

- **Overwrite scratch media before overwriting recyclable media that is contained in the destination media set.**  
 If you choose to overwrite scratch media before recyclable media, more media may be required for the same number of jobs. However, the recyclable media may be preserved longer for possible recovery.
- **Overwrite recyclable media that is contained in the destination media set before overwriting scratch media.**  
 If you choose to overwrite recyclable media before scratch media, the same media is re-used more frequently than if you overwrite scratch media before recyclable media.

In a storage device pool for tape drives or disk cartridges, Backup Exec selects the oldest recyclable media in the storage device pool to use first.

In a robotic library, Backup Exec selects the oldest recyclable media in the library to use first. If the robotic library is partitioned, Backup Exec searches for the oldest recyclable media in the targeted partition only.

---

**Caution:** Symantec recommends that you physically write-protect media containing critical data. Use the write-protect tab on the media cartridge to protect against unintentional move or erase operations, or expired overwrite protection periods.

---

The following table describes the order in which Backup Exec searches for media to use for an overwrite job.

**Table 13-5** How Backup Exec searches for overwritable media

Overwrite protection level and overwrite option:	Media is overwritten in tape drives and disk cartridges in this order:
Full + Overwrite scratch media first <b>Note:</b> This combination provides the most protection against overwriting media.	<ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Recyclable media in the destination media set</li> <li>■ Recyclable media in any media set</li> </ul>

**Table 13-5** How Backup Exec searches for overwritable media (*continued*)

Overwrite protection level and overwrite option:	Media is overwritten in tape drives and disk cartridges in this order:
Full + Overwrite recyclable media first	<ul style="list-style-type: none"> <li>■ Recyclable media in the destination media set</li> <li>■ Scratch media</li> <li>■ Recyclable media in any media set</li> </ul>
Partial + Overwrite scratch media first	<ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Recyclable media in the destination media set</li> <li>■ Recyclable media in any media set</li> <li>■ Media that is imported from another installation of Backup Exec, or from another product</li> </ul>
Partial + Overwrite recyclable media first	<ul style="list-style-type: none"> <li>■ Recyclable media in the destination media set</li> <li>■ Scratch media</li> <li>■ Recyclable media in any media set</li> <li>■ Media that is imported from another installation of Backup Exec, or from another product</li> </ul>
None - No overwrite protection + overwrite scratch media first <b>Warning:</b> This options is not recommended because it does not protect data from being overwritten.	<ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Recyclable media in the destination media set</li> <li>■ Recyclable media in any media set</li> <li>■ Media that is imported from another installation of Backup Exec, or from another product</li> <li>■ Allocated media in any media set</li> </ul>
None - No overwrite protection + overwrite recyclable media first <b>Warning:</b> This options is not recommended because it does not protect data from being overwritten.	<ul style="list-style-type: none"> <li>■ Recyclable media in the destination media set</li> <li>■ Scratch media</li> <li>■ Recyclable media in any media set</li> <li>■ Media that is imported from another installation of Backup Exec, or from another product</li> <li>■ Allocated media in any media set</li> </ul>

In addition to setting overwrite protection levels, you must set overwrite options, which set the order in which Backup Exec searches for overwritable media.

The most obvious candidates for backup jobs that require overwritable media in tape and disk cartridges are scratch media and recyclable media. Recyclable media have expired overwrite protection periods. Backup Exec searches for these types of media first when a backup requires tape or disk cartridge media to overwrite. The search pattern is different according to whether you have selected Full, Partial, or None. The media indicate that a type of media set is examined for availability.

See [“Editing global settings for storage”](#) on page 415.

See [“About media vaults”](#) on page 384.

## Viewing audit log entries for tape and disk cartridge media operations

The audit log provides information about media operations, such as when media are overwritten or appended to. This information can help you find all of the media that is required for a restore job.

The following options for media operations are enabled by default in the audit log:

- Delete media
- Delete media set
- Erase media
- Format media
- Format media (WORM)
- Label media
- Move media
- Overwrite media

See [“About audit logs”](#) on page 516.

See [“Configuring tape and disk cartridge media operations to appear in the audit log”](#) on page 380.

**To view the audit log entries for tape and disk cartridge media operations**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 In the **Select category to view** field, click **Devices and Media** .
- 3 View the entries in the **Audit Log** window.

## Configuring tape and disk cartridge media operations to appear in the audit log

You can enable some or all media operations to appear in the audit log.

See [“About audit logs”](#) on page 516.

**To configure tape and disk cartridge media operations to appear in the audit log**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 On the **Audit Logs** dialog box, click **Configure Logging**.
- 3 Expand the **Devices and Media** category.
- 4 Select the operations that you want to log, or clear the check box of any item or operation that you do not want to log.
- 5 Click **OK**.

## About labeling tape and disk cartridge media

Media labels identify the tape and disk cartridge media that you use in Backup Exec. When new, blank, or unlabeled tape or disk cartridge media is used during a backup operation, Backup Exec automatically labels the media. This label consists of a prefix that identifies the cartridge type, and an incrementing number. For example, if the media is a 4mm tape, then the prefix is 4M, followed by 000001. The next media label generated for an unlabeled 4mm tape would be 4M000002, and so on.

Another type of media label used by Backup Exec is the media ID, which is a unique label assigned by Backup Exec to the individual media used in Backup Exec. The media ID is used internally by Backup Exec to keep statistics on each media. Because the media label or barcode label for media can be changed, Backup Exec must use the media ID to preserve continuity in record keeping for each individual media. You cannot change or erase the media ID. The media ID has no effect on the media label, or on your ability to rename, label, or erase media.

At times, you may need to use the media ID to distinguish the media that have duplicate media labels. Duplicate labels can be automatically generated in instances when Backup Exec is reinstalled or media from another Backup Exec installation is used. Use the media ID to distinguish between duplicate labels. You can view the media ID in a media's property page.

Write the media label on an external label that is fixed to the outside of the physical media. Whenever you change the media label, you should also change the external label to match.

The following methods are available in Backup Exec to change a media label:

- Write a new media label on the media. The Label operation destroys any data on the media.

- Rename the media. Renaming the media changes the name of the media in the display, but does not write the new label to the media until an overwrite operation occurs. The data on the media is viable until the media is overwritten.
- Edit the label. Editing the label changes the name of the media in the display, but does not write the new label to the media until an overwrite operation occurs. The data on the media is viable until the media is overwritten.

See [“Labeling media”](#) on page 427.

See [“Renaming a media label ”](#) on page 383.

See [“About barcode labeling”](#) on page 382.

## About labeling imported media

Media that is imported from another installation of Backup Exec, or from another product is called imported media. Backup Exec does not automatically relabel imported media. The imported media’s existing label is read and displayed in either the **Backup Exec and Windows NT Backup Media** media set or the **Foreign Media** media set. The original media label of the imported media is displayed in the media’s properties. You can edit the media description in the media’s property page to make it a more descriptive label.

If the media overwrite protection level is set to Partial or None, the imported media may be selected for a job and be overwritten. The imported media is automatically labeled when it is overwritten during a job.

If you want to label a specific imported media while maintaining full media overwrite protection for other imported media, erase the specific media and then label it.

See [“Erasing media”](#) on page 390.

## About barcode labeling

If there is a barcode label on the physical cartridge, and if the robotic library has a barcode reader, the barcode label automatically becomes the media label.

You can change the media label in Backup Exec. However, as long as the media has a barcode label that can be read, the barcode label takes precedence over the media label. To use the media label that you entered using Backup Exec, you must remove the physical barcode label from the media cartridge. Or, you can use the media in a device that does not have a barcode reader.

For example, robotic library 1 has barcode support. During a backup operation, Backup Exec requests a new media or an overwritable media for the operation. A new media with the barcode label 'ABCD' is inserted in the robotic library magazine

and the barcode reader scans the barcode ID. Backup Exec selects this media for the operation and detects that a barcode label has been assigned to the media. Backup Exec automatically uses the barcode label and continues the operation.

When you change magazines or insert new media in a magazine, you can use the **Scan** operation to quickly update slot information.

See [“About labeling tape and disk cartridge media”](#) on page 381.

See [“Scanning a storage device”](#) on page 424.

## Renaming a media label

You can rename a media's label and description. The new label is not written to the media until an overwrite operation occurs. All of the data that is on the media is preserved until the next overwrite job. However, the new media label is stored in the database and is displayed for that media. To write a new media label to the media immediately, use the **Label** operation. The media's contents are erased.

If you rename a media, and then use it in another installation of Backup Exec, that media is imported to the **Backup Exec and Windows NT Media** media set. The media's original media label is displayed. The renamed label is not transferred to other installations of Backup Exec.

See [“About labeling tape and disk cartridge media”](#) on page 381.

### To rename a media label

- 1 On the **Storage** tab, right-click the tape drive or slot that contains the media that you want to relabel, and then click **Details**.
- 2 In the left pane, click **Media Properties**.
- 3 In the **Media label** field, enter a new label name.
- 4 To change the description, enter a new description in the **Media description** field.
- 5 Click **Apply**.

## About WORM media

Write once, read many (WORM) data storage is used to keep the data that has a long retention period. Data can be written to WORM media one time only. After it is written to, the media can be appended to, but it cannot be overwritten, erased, or reformatted.

When WORM media is used in a media set, the overwrite protection period is not applied to it, but the append period is applied.

New WORM media is WORM media that has not been written to. When new WORM media is introduced into Backup Exec, it is placed in the **Scratch Media** set. After the WORM media has been written to one time, you cannot move it to the Scratch media set. You can move WORM media to the **Retired Media** set to delete it from Backup Exec, but you cannot erase it or reformat it.

When you select the option to use WORM media, Backup Exec confirms that the destination device is or contains a WORM-compatible drive. Backup Exec also confirms that the WORM media is available in the drive. If WORM media or a WORM-compatible drive is not found, an alert is sent.

See “[Storage options](#)” on page 190.

## About media vaults

A media vault is a logical representation of the actual physical location of specified media. You can create media vaults to keep track of where media is physically stored, such as a scratch bin, or an off-site location. Backup Exec creates default media vaults to let you view all media that are online, offline, or in a media vault.

You must run the **Configure Storage** wizard to update the location of media in media vaults. From the **Configure Storage** wizard, you can print reports that detail which media are ready to move to and return from the vault. You can also update the location of the media if you choose to move them. However, you must physically collect the media, and move the media to and from the vault. The location of the media is updated in the Backup Exec Database, but the media is not ejected or exported. If Backup Exec detects that the media is in a robotic library, you are prompted to export media. If you choose to export the media, an export media job runs. If your environment includes remote sites, you should create separate media sets for each remote site. Then, the reports contain details on which media are ready to be moved for a specific site.

**Table 13-6**      Default media vaults

Default media vault	Description
<b>Online Tape/Disk Cartridge Media</b>	Displays the media that are available in tape drives or robotic libraries. You cannot add or move media to the online media vault. Backup Exec does that automatically. If you move media from the online media vault to another media vault, the media's overwrite protection period and append period remain in effect.

Table 13-6 Default media vaults (continued)

Default media vault	Description
<b>Offline Tape/Disk Cartridge Media</b>	Displays the media that are on-site but are not in tape drives or robotic libraries, and are not in media vaults. Media appear in the offline media vault if you use Backup Exec to remove media from a tape drive or robotic library. You can add media to the offline media vault from another media vault. An inventory operation or a catalog operation moves the offline media back to the online media vault. You cannot delete or rename the offline media vault.
<b>Vaulted Tape/Disk Cartridge Media</b>	Displays the media that are not in tape drives or robotic libraries, and have been moved to a media vault. <b>Vaulted Tape/Disk Cartridge Media</b> displays in <b>All Media Vaults</b> details only after you create a media vault.
<b>All Media Vaults</b>	Displays the media that are in media vaults that you create. <b>All Media Vaults</b> displays on the <b>Storage</b> tab only after you create a media vault. You can associate media vaults with media sets that you create. You specify when to move the media from a media set to the media vault. You also specify when the media is to return to the media set from the media vault. See <a href="#">“Creating media vault rules to move media to and from media vaults”</a> on page 386.

See [“Editing media vault properties”](#) on page 385.

## Editing media vault properties

You can view and edit the name and description of a media vault.

See [“About media vaults”](#) on page 384.

To view and edit media vaults and media vault rules, edit the properties of the media set that is associated with the media vault.

See [“Editing media set properties”](#) on page 374.

#### To edit media vault properties

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**, and then expand **All Media Vaults**.
- 2 Right-click the media vault for which you want to edit properties, and then click **Details**.
- 3 In the left pane, click **Media Vault Properties**.
- 4 Change the properties as appropriate.

See [“Media vault properties”](#) on page 386.

### Media vault properties

Properties for media vaults include the name and a description of the media vault.

See [“Editing media vault properties”](#) on page 385.

**Table 13-7** Properties for media vaults

Item	Description
<b>Name</b>	Displays the name of the media vault.
<b>Description</b>	Displays a description of the media vault.

## Creating media vault rules to move media to and from media vaults

Create media vault rules to do the following:

- Associate a media vault to which you want to send media with a media set.
- Specify the amount of time to wait between when the media is allocated and when it is sent to the vault.
- Specify the amount of time to wait between returning the media from the vault and when it was last written to.

See [“About media vaults”](#) on page 384.

Backup Exec does not update the vault automatically. You must use the **Configure Storage** wizard to update the location of the media. You can also print or view the reports that contain details on which media are ready to be moved to and from the vault.

See [“Updating the media location in media vaults”](#) on page 387.

### To create media vault rules to move media to and from media vaults

- 1 On the **Storage** tab, expand **All Media Sets**.
- 2 Right-click **Keep Data for 4 Weeks, Keep Data Infinitely - Do Not Allow Overwrite**, or a media set that you created, and then click **Details**.
- 3 In the left pane, click **Properties**.
- 4 Select the media vault that you want to use with the media set.
- 5 Specify when to move the media to the vault and when to return the media to the media set.

See [“Media set properties”](#) on page 374.

## Updating the media location in media vaults

You can update the location of media that are in vaults. You can also print the reports that detail which media are ready to move to and return from the vault. However, you must physically collect the media, and move the media to and from the vault.

See [“About media vaults”](#) on page 384.

### To update the media location in media vaults

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**, and then double-click **All Media Vaults**.
- 2 Right-click the media vault for which you want to update the media location, and then click **Update vault using wizard**.
- 3 Follow the on-screen prompts.

## Moving media to a vault

You can use a barcode scanner to enter the media labels of media that you want to move to a vault. You can also type a media label into the dialog box.

See [“About media vaults”](#) on page 384.

### To move media to a vault

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**, and then double-click **All Media Vaults**.
- 2 Right-click the media vault that you want to move media to, and then click **Move media to vault**.
- 3 Follow the on-screen prompts.

## Deleting a media vault

You can only delete an empty media vault. If there is any media in the vault, you must move it before you can delete the vault. You cannot delete the online media vaults or the offline media vaults.

See [“About media vaults”](#) on page 384.

### To delete a media vault

- 1 On the **Storage** tab, expand **All Media Vaults**.
- 2 Right-click the media vault that you want to delete, and then click **Delete**.
- 3 Click **Yes** when you are prompted to delete the media vault.

## About retiring damaged media

You should associate media that meets or exceeds the discard thresholds that are determined by the media manufacturer with the **Retired Media** media set. Backup Exec tracks the soft errors that are generated by the storage device firmware. Media that exceed acceptable levels of these errors are reported as potential candidates to be discarded.

To decide which media to retire, run a Media Errors report for the total number of errors for media, or view the properties for a specific media.

Associate any media with an unacceptable level of errors to **Retired Media** so that you are protected against using defective media before critical backup operations begin. After you associate media with the **Retired Media** set, it is not used by Backup Exec for future backup jobs. The media is still available to be restored from if it is not damaged.

See [“About deleting media”](#) on page 389.

See [“Media properties”](#) on page 392.

See [“Media Errors report”](#) on page 610.

## Retiring damaged media

You can retire damaged media so that Backup Exec does not use it for backup jobs.

See [“About retiring damaged media”](#) on page 388.

### To retire damaged media

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**.
- 2 Right-click **Online Tape/Disk Cartdrige Media**, and then click **Details**.

- 3 Right-click the media that you want to retire, and then click **Retire**.
- 4 Click **Yes** when you are prompted to retire the media.

## About deleting media

When you delete media from Backup Exec, all records of the media are removed from the Backup Exec Database. These records include catalog information, media statistics, and other information that is associated with the media. You can only delete media when it belongs to the **Retired Media** set.

You may want to delete media when the following occurs:

- You have a lot of off-site media that you do not want to recycle.
- You throw away damaged or old media.

If you import deleted media back into Backup Exec, it is added to either the **Backup Exec and Windows NT Media** media set or the **Foreign Media** media set. Before you can restore from the media, you must catalog it.

See “[Deleting media](#)” on page 389.

See “[About retiring damaged media](#)” on page 388.

## Deleting media

You can delete media from the Backup Exec Database after you associate the media with the **Retired Media** set.

See “[About deleting media](#)” on page 389.

### To delete media

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**.
- 2 Expand **All Media Sets**, right-click **Retired Media**, and then click **Details**.
- 3 Right-click the media that you want to delete, and then click **Delete**.
- 4 Click **Yes** when you are prompted to delete the media.

## About erasing media

You can erase media by using either of the following erase operations:

**Table 13-8** Erase operations

Erase operation	Description
<b>Erase media now</b>	Writes an indicator at the beginning of the media that makes the data that is contained on the media inaccessible. For most uses, the <b>Erase media now</b> operation is sufficient.
<b>Long erase media now</b>	Instructs the drive to physically erase the entire media. If you have sensitive information on the media and you want to dispose of it, use the <b>Long erase media now</b> operation. A long erase operation on a media can take several minutes to several hours to complete depending on the drive and the media capacity.  Some devices do not support a long erase operation.

The erase operation does not change the media label. To change a media label, run a Label operation or rename the media before you run an Erase operation.

You cannot cancel an Erase operation after it has started. You can cancel an Erase operation that is queued.

See [“Erasing media”](#) on page 390.

## Erasing media

You can erase media.

See [“About erasing media”](#) on page 389.

### To erase media

- 1 On the **Storage** tab, right-click the drive that contains the media that you want to erase.
- 2 Click **Erase media now**, and then select an erase operation.
- 3 Click **Yes** when you are prompted to erase the media.

## About cataloging media that contains encrypted backup sets

When you catalog media that contains encrypted backup sets, Backup Exec attempts to find valid encryption keys for the sets in the Backup Exec Database. If Backup Exec does not find a valid key, it issues an alert that instructs you to create one. After you create a valid key, you can respond to the alert to retry cataloging the encrypted set. Alternatively, you can skip the encrypted set and continue to catalog the rest of the media, or cancel the catalog job.

See [“About encryption key management”](#) on page 477.

See [“Creating an encryption key”](#) on page 478.

## Associating media with a media set

When you associate media with a media set, the media uses the append and overwrite protection period properties of that media set.

---

**Note:** Associating scratch or imported media with a media set is not recommended. Backup Exec automatically associates scratch or imported media with a media set when a backup job requires it.

---

See [“Creating media sets for tape and disk cartridge media”](#) on page 373.

### To associate media with a media set

- 1 On the **Storage** tab, expand **Tape/Disk Cartridge Media Sets and Vaults**.
- 2 Double-click **All Media** to display a list of media.
- 3 Right-click the media that you want to associate with a media set, and then click **Associate with media set**.
- 4 Select a media set from the drop-down list, and then click **OK**.

See [“About media sets”](#) on page 366.

## Editing media properties

You can view media properties and edit some media properties.

See [“About tape and disk cartridge media”](#) on page 365.

### To edit media properties

- 1 On the **Storage** tab, double-click the tape drive that contains the media.
- 2 In the left pane, click **Media Properties**.
- 3 Change the appropriate information.  
See “[Media properties](#)” on page 392.

## Media properties

You can view information about the media.  
See “[Editing media properties](#)” on page 391.

Table 13-9 Media properties

Item	Description
<b>Media label</b>	<p>Displays the media label that Backup Exec assigns automatically, or that the administrator assigned, or that is a pre-assigned barcode label.</p> <p>You can edit the media label, which is limited to 32 characters. Editing the label changes the name of the media in the display, but does not write the new label to the media until an overwrite operation occurs. When you edit a media label, try to make it a concise identifier that remains constant even when the media is reused. You should write this media label on a label that is fixed to the outside of the physical media.</p> <p>Duplicate labels can be automatically generated. For example, reinstalling Backup Exec or bringing media from another Backup Exec installation can cause duplication in labels. Duplicate labels are allowed, but not recommended.</p> <p>If a barcode is available, and a bar code-equipped device is used, then the media label automatically defaults to that barcode.</p>

**Table 13-9** Media properties (*continued*)

Item	Description
<b>Media description</b>	<p>Displays the original media label if the media is imported media.</p> <p>You can edit the media description, which is limited to 128 characters, to make it a more descriptive label.</p>
<b>Media ID</b>	<p>Displays the unique internal label that Backup Exec assigns to each media. The ID keeps statistics for each media. You cannot change or erase the media ID.</p>
<b>Media type</b>	<p>Displays the media type and subtype, if the subtype is available. Click the button next to the field to change the media type or subtype.</p>
<b>Export pending</b>	<p>Displays <b>Yes</b> when a job runs that has an associated Export Media operation to export this media.</p>
<b>Media set</b>	<p>Displays the name of the media set this media belongs to.</p>
<b>Media location</b>	<p>Displays the name of the device or vault where this media is located.</p>
<b>Creation date</b>	<p>Displays the date and time when the media was first entered into Backup Exec.</p>
<b>Allocated date</b>	<p>Displays the date and time when the media was added to a media set as a result of an overwrite operation.</p>

Table 13-9 Media properties (continued)

Item	Description
<b>Modified date</b>	Displays the date and time when data was last written to the media.
<b>Overwrite protection until</b>	Displays the date and time after which the media can be overwritten.
<b>Appendable until</b>	Displays the date and time after which the media can no longer be appended to.
<b>Supports hardware encryption</b>	Displays <b>Yes</b> if this media supports hardware encryption.
<b>Total capacity</b>	Displays the amount of expected total raw capacity of the media. Some tape devices support the ability to read the amount of total capacity of the media that is currently loaded in the device. If a tape device supports reading of the total capacity amount, then <b>Total capacity</b> is derived from the <b>Total capacity</b> amount. Otherwise, <b>Total capacity</b> is estimated based on past usage of the media.
<b>Total backup storage</b>	Displays the expected amount of total raw capacity of the media.
<b>Used capacity</b>	Displays the amount of raw capacity on the media that has been used. <b>Available capacity</b> is subtracted from <b>Total capacity</b> to calculate <b>Used capacity</b> . <b>Used capacity</b> may or may not equal <b>Bytes written</b> .

**Table 13-9** Media properties (*continued*)

Item	Description
<b>Amount of data written</b>	<p>Displays the amount of data that has been written to the media. The amount of data that is written may differ from the used capacity due to the effects of data compression. Data compression tends to increase the amount of data that is written when compared to used capacity.</p>
<b>Available capacity</b>	<p>Displays the amount of expected raw capacity on the media that remains unused. Some tape devices support the ability to read the amount of remaining capacity of the media that is currently loaded in the device. If a tape device supports reading of the remaining capacity amount, then <b>Available capacity</b> is derived from the remaining capacity amount. Otherwise, <b>Bytes written</b> is subtracted from <b>Total capacity</b> to calculate <b>Available capacity</b>.</p> <p>Because free space is reported in terms of unused raw capacity, review <b>bytes written</b> and <b>compression ratio</b> to estimate if there is enough free space for a specific job.</p>
<b>Compression ratio</b>	<p>Displays the ratio of <b>Bytes written</b> to <b>Used capacity</b>. <b>Compression ratio</b> shows the overall effect that data compression and media flaws have on the amount of data that is stored on the media.</p>

**Table 13-9** Media properties (*continued*)

<b>Item</b>	<b>Description</b>
<b>Mounts</b>	Displays the number of times this media has been mounted.
<b>Seeks</b>	Displays the total number of seek operations that have been performed on this media. Seek operations are run to locate a specific piece of information on the media.
<b>Seek errors</b>	Displays the number of errors that are encountered while locating data.
<b>Soft write errors</b>	Displays the number of recoverable write errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the media for damage.
<b>Hard write errors</b>	Displays the number of unrecoverable write errors that were encountered. If you receive hard errors, check the media for damage.
<b>Soft read errors</b>	Displays the number of recoverable read errors that were encountered. If you receive soft errors, it may indicate the beginning of a problem. If you receive excessive errors for your environment, check the media for damage.

**Table 13-9** Media properties (*continued*)

Item	Description
<b>Hard read errors</b>	Displays the number of unrecoverable read errors that were encountered. If you receive hard errors, check the media for damage.  See <a href="#">“About retiring damaged media”</a> on page 388.

## Media rotation strategies

Many media rotation strategies exist for tape and disk cartridge media that you can use to back up your data.

The most commonly used media rotation strategies include the following:

- **Son**, which uses the same media each day to run a full backup.  
See [“Son media rotation strategy”](#) on page 398.
- **Father/Son**, which uses multiple media, and includes a combination of weekly full and daily differential or incremental backups for a two-week schedule. This strategy provides backups for off-site storage .  
See [“Father/son media rotation strategy”](#) on page 399.
- **Grandfather**, which uses multiple media, and includes a combination of weekly and monthly full and daily differential or incremental backups. This strategy also provides backups for off-site storage.  
See [“Grandfather media rotation strategy”](#) on page 400.

### Son media rotation strategy

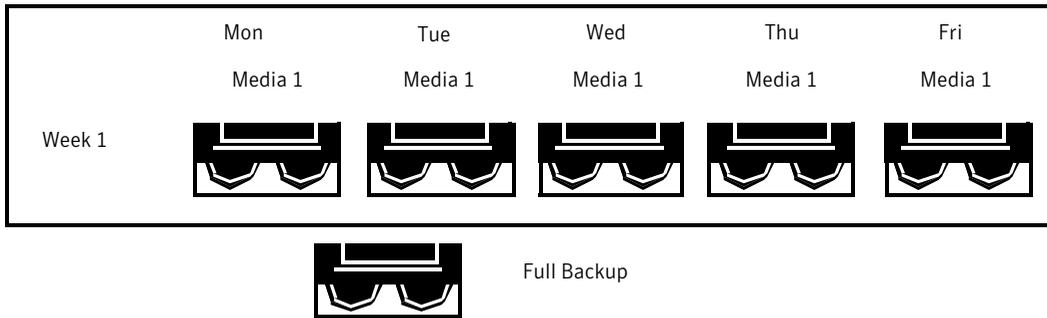
The Son media rotation strategy requires the following:

**Table 13-10** Son media rotation strategy

Item	Description
Number of media required	1 (minimum)
Overwrite protection period	Last backup

The Son strategy involves performing a full backup every day.

**Figure 13-3** Son backup strategy



Although the Son strategy is easy to administer, backing up with a single media is not an effective method of backup. Magnetic media eventually wears out after many uses and the data you can restore only spans back to your last backup.

## Father/son media rotation strategy

The Father/son media rotation strategy requires the following:

**Table 13-11** Father/son media rotation strategy

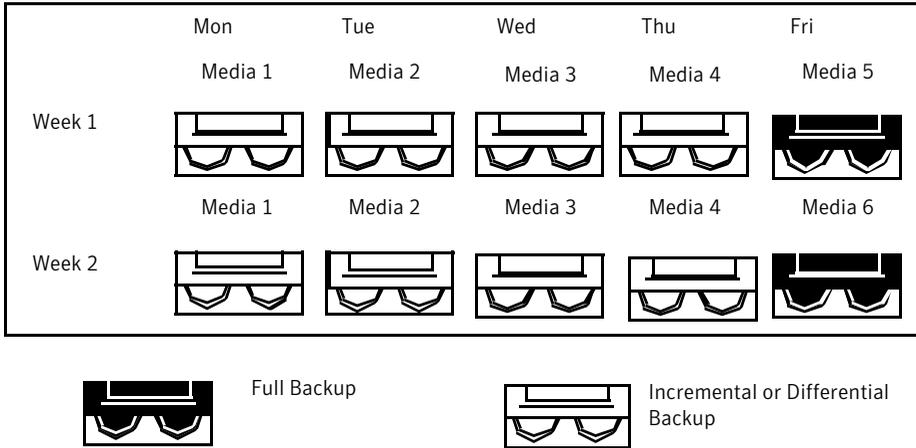
Item	Description
Number of media required	6 (minimum)
Overwrite protection period	Two weeks

The Father/Son media rotation strategy uses a combination of full and differential or incremental backups for a two-week schedule.

In the Father/Son scenario, four media are used Monday through Thursday for differential or incremental backups. The other two media containing full backups are rotated out and stored off-site every Friday.

The Father/Son strategy is easy to administer and lets you keep data longer than the Son strategy. The Father/Son strategy is not suitable for the stringent data protection needs of most network environments.

**Figure 13-4** Father/Son backup strategy



When this backup strategy is first implemented, you must start with a full backup.

## Grandfather media rotation strategy

The Grandfather media rotation strategy requires the following:

**Table 13-12** Grandfather media rotation strategy

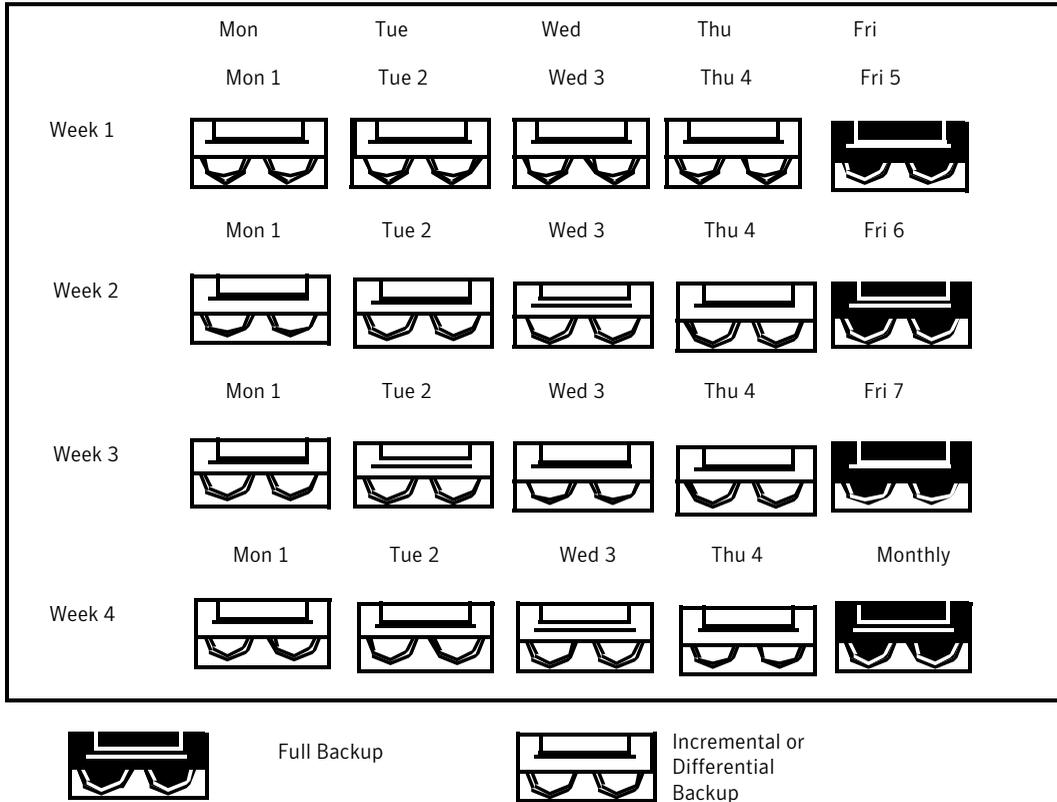
Item	Description
Number of media required	19 (minimum)
Overwrite protection period	One year

The Grandfather method is one of the most common media rotation strategies. The Grandfather method is easy to administer and comprehensive enough to allow easy location of files when they need to be restored.

In the Grandfather scenario, four media are used Monday through Thursday for incremental or differential backups; another three media are used every Friday for full backups.

The remaining 12 media are used for monthly full backups and are kept off-site.

**Figure 13-5** Grandfather backup strategy



The Grandfather strategy is recommended because it offers a good media number to storage life ratio (19 media/1 year). You can easily incorporate more media. For example, you can perform a full backup on the last Saturday of the month to keep permanently.



# Storage device pools

This chapter includes the following topics:

- [About storage device pools](#)
- [Creating a storage device pool](#)
- [Viewing jobs, job histories, and active alerts for a storage device pool](#)
- [Editing storage device pool properties](#)
- [Storage device pool properties](#)

## About storage device pools

A storage device pool is a group of similar types of storage devices that enables load-balancing of Backup Exec jobs. The workload is shared across the storage device pool. You can send backup jobs to specific storage devices or to a storage device pool. If the specific storage device is busy, the job must wait until the storage device becomes available.

When you send a job to specific storage devices, Backup Exec cannot automatically route the job to the next available storage device. When you submit a backup job to a storage device pool, the job is automatically sent to an available storage device in that pool. As other jobs are created and started, they can run concurrently on other storage devices in the storage device pool. By dynamically allocating storage devices as jobs are submitted, Backup Exec processes jobs quickly and efficiently. Storage device pools provide fault tolerance if you configure error-handling rules to resubmit a job that fails because of a storage device error.

When you configure a new storage device, Backup Exec automatically adds it to the appropriate storage device pool. Backup Exec also detects attached storage devices and adds them to the appropriate storage device pool. However, you must

edit the properties of the pool and check the check box next to the device before jobs can use that device in the pool.

You can perform the following actions for the storage device pools that you create:

- Edit the storage pool properties to check the check box next to the storage devices that you want to use in the pool.
- View or filter data to display, such as jobs, job history, and active alerts.

You can view any storage device pools that you create on the **Storage** tab, under **All Storage Pools**.

Backup Exec automatically creates some storage device pools and adds any storage devices that you configure to the appropriate storage device pool. You cannot edit any properties or storage devices in the storage device pools that Backup Exec creates. You can select these storage device pools when you select the storage for a backup job.

**Table 14-1** Storage device pools created by Backup Exec

Storage device pools that are created by Backup Exec	Description
<b>Any disk storage</b>	Contains the fixed-disk storage.
<b>Any tape cartridge</b>	Contains the tape cartridges. Backup Exec creates this pool when it detects an attached tape drive or robotic library.  In a tape cartridge storage pool, Backup Exec uses the oldest recyclable media first.
<b>Any disk cartridge</b>	Contains the disk cartridges that you have configured to use as storage. Backup Exec creates this pool the first time that you configure disk cartridge storage.
<b>Any virtual disk</b>	Contains the virtual disks that are on storage arrays. Backup Exec creates this pool when you install the Storage Provisioning Option.

If you have the Central Admin Server Option installed, you can create managed Backup Exec server pools.

See [“About the Configure Storage wizard”](#) on page 145.

See [“Creating a storage device pool”](#) on page 405.

See [“Editing storage device pool properties”](#) on page 406.

See [“Adding managed Backup Exec servers to a Backup Exec server pool”](#) on page 1031.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

## Creating a storage device pool

Use the **Configure Storage** wizard to create storage device pools. You can view any storage device pools that you create on the **Storage** tab, under **All Storage Pools**.

See [“About storage device pools”](#) on page 403.

### To create a storage device pool

- 1 On the **Storage** tab, in the **Configure** group, click **Configure Storage**.
- 2 Select **Storage pools**, and then click **Next**.
- 3 Follow the on-screen prompts.
- 4 Edit the storage device pool properties, and check the check boxes next to the devices that you want to use in the pool.

See [“Editing storage device pool properties”](#) on page 406.

## Viewing jobs, job histories, and active alerts for a storage device pool

You can view the jobs that are sent to a storage device pool, and the job histories as well as any active alerts. You must create a storage pool before **All Storage Pools** appears on the **Storage** tab.

See [“About managing and monitoring active and scheduled jobs”](#) on page 247.

See [“About alerts”](#) on page 279.

### To view jobs, job histories, and active alerts for a storage device pool

- 1 On the **Storage** tab, expand **All Storage Pools**.
- 2 Right-click the storage device pool for which you want to view the jobs, and then click **Details**.
- 3 In the left pane, click the appropriate tab.

## Editing storage device pool properties

You can edit storage device pool properties. You must create a storage device pool before **All Storage Pools** appears on the **Storage** tab.

You can check and uncheck the storage devices that you want to use in these pools. Only similar types of storage devices can belong to the same storage device pool.

See [“About storage device pools”](#) on page 403.

### To edit storage device pool properties

- 1 On the **Storage** tab, expand **All Storage Pools**.
- 2 Double-click the storage pool for which you want to edit properties.
- 3 In the left pane, click **Properties**.
- 4 Change the appropriate options.  
See [“Storage device pool properties”](#) on page 406.
- 5 (Optional) Do one or both of the following:

To use a storage device in the pool	Check the check box next to the storage device.
To prevent the use of a storage device in a pool	Uncheck the check box next to the storage device.

- 6 Click **Apply**.

## Storage device pool properties

You can change the name and description of a storage device pool. You can also uncheck specific storage devices in the storage device pool that you no longer want to be part of that pool. Unchecked storage devices still appear in the pool properties, but are not used by Backup Exec. If you do not want the storage device to appear in the storage device pool, you must delete the device from Backup Exec. Then, Backup Exec deletes the storage device from a storage device pool.

See [“Editing storage device pool properties”](#) on page 406.

**Table 14-2** Storage device pool properties

Item	Description
<b>Name</b>	Displays the name of the storage device pool.

**Table 14-2** Storage device pool properties (*continued*)

<b>Item</b>	<b>Description</b>
<b>Description</b>	Displays a description of the storage device pool.
<b>Storage device pool type</b>	Displays the type of storage that is in this pool. You cannot edit this field.
<b>Storage devices that belong to the pool</b>	<p>Displays the storage devices that are currently in this pool. Storage devices that have a checkmark next to the them are used in the pool.</p> <p>When you configure a storage device for the first time, Backup Exec automatically adds it to the appropriate storage device pool. If Backup Exec detects an attached storage device, the storage device is automatically added to the appropriate storage device pool. However, you must check the check box next to the storage device if you want it to be used as part of the storage device pool.</p>



# Storage operations

This chapter includes the following topics:

- [About storage operation jobs](#)
- [Storage operations for virtual tape libraries and simulated tape libraries](#)
- [Sending a notification when a scheduled storage operation job completes](#)
- [Editing global settings for storage](#)
- [About sharing storage devices](#)
- [About deleting a storage device](#)
- [Renaming a storage device](#)
- [Viewing jobs, job histories, backup sets, and active alerts for storage devices](#)
- [About inventorying a storage device](#)
- [Cataloging a storage device](#)
- [Scanning a storage device](#)
- [Changing the state of a storage device to online](#)
- [Pausing and unpausing a storage device](#)
- [Disabling and enabling a storage device](#)
- [Initializing a robotic library](#)
- [Retensioning a tape](#)
- [Formatting media in a drive](#)
- [Labeling media](#)

- [Ejecting media from a disk cartridge or tape drive](#)
- [Cleaning a robotic library drive](#)
- [About importing media](#)
- [About exporting expired media](#)
- [About locking the robotic library's front portal](#)
- [Unlocking the robotic library's front portal](#)
- [Backup Exec server and storage device states](#)

## About storage operation jobs

Backup Exec provides the storage operations that help you manage storage devices and media. You can perform most storage operations by right-clicking the storage device, and then selecting the operation. Only the storage operations that are supported for that storage device or media are available on the right-click menu. Not all storage operations are available for virtual tape libraries and simulated tape libraries.

You can schedule some storage operations as recurring jobs. You can specify a schedule and a recipient for notification when these jobs run.

Storage operations that you can schedule include the following:

- Inventory
- Clean
- Import
- Export

In addition to storage operations, you can perform the following actions:

- Delete a storage device.
- Share a storage device.
- Rename a storage device.
- View a history of storage operations that you perform on a specific storage device.

The following table provides more information about storage operation jobs.

Table 15-1 Storage operation jobs

Storage operation job	For more information
<b>Scan</b>	See <a href="#">“Scanning a storage device”</a> on page 424.
<b>Inventory</b>	You can run this operation immediately, or schedule it. See <a href="#">“About inventorying a storage device”</a> on page 422.
<b>Catalog</b>	See <a href="#">“About catalogs ”</a> on page 242. See <a href="#">“Cataloging a storage device”</a> on page 424.
<b>Inventory and Catalog</b>	See <a href="#">“Inventorying and cataloging a storage device”</a> on page 423.
<b>Initialize</b>	See <a href="#">“Initializing a robotic library”</a> on page 426.
<b>Lock</b>	See <a href="#">“About locking the robotic library’s front portal”</a> on page 433.
<b>Unlock</b>	See <a href="#">“Unlocking the robotic library’s front portal”</a> on page 433.
<b>Clean</b>	You can run this operation immediately, or schedule it. See <a href="#">“Cleaning a robotic library drive”</a> on page 429.
<b>Label</b>	See <a href="#">“Labeling media”</a> on page 427.
<b>Import</b>	You can run this operation immediately, or schedule it. See <a href="#">“Importing media ”</a> on page 431.
<b>Export</b>	You can run this operation immediately, or schedule it. See <a href="#">“Robotic library slot properties”</a> on page 432 on page 432.
<b>Erase</b>	See <a href="#">“About erasing media”</a> on page 389.
<b>Eject</b>	You can run this operation immediately, or schedule it. See <a href="#">“Ejecting media from a disk cartridge or tape drive”</a> on page 428.
<b>Retention</b>	See <a href="#">“Retensioning a tape”</a> on page 426.

**Table 15-1** Storage operation jobs (*continued*)

Storage operation job	For more information
Format	See <a href="#">“Formatting media in a drive”</a> on page 427.

See [“About deleting a storage device”](#) on page 420.

See [“About sharing storage devices”](#) on page 418.

See [“Renaming a storage device”](#) on page 421.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

See [“Sending a notification when a scheduled storage operation job completes”](#) on page 413.

See [“Storage operations for virtual tape libraries and simulated tape libraries”](#) on page 412.

## Storage operations for virtual tape libraries and simulated tape libraries

Backup Exec treats virtual tape libraries and simulated tape libraries as physical robotic libraries. You can identify virtual tape libraries by the label VTL that displays on a library's properties pages. You can identify simulated tape libraries by the label TLS (Tape Library Simulator Utility).

The virtual tape libraries and simulated tape libraries do not support all of the storage operations that are available for physical robotic libraries.

The following storage operations are available for virtual tape libraries:

- Label
- Import
- Export

The following storage operations are available for simulated tape libraries:

- Scan
- Inventory and Catalog
- Inventory
- Initialize

See [“About storage operation jobs”](#) on page 410.

# Sending a notification when a scheduled storage operation job completes

You can assign recipients to be notified when a scheduled storage operation job completes. Recipients must be set up before you can set up notification.

See [“About storage operation jobs”](#) on page 410.

## To send a notification when a scheduled storage operation job completes

- 1 Create a new scheduled storage operation job or edit an existing one.  
 See [“About storage operation jobs”](#) on page 410.
- 2 On the storage operation job dialog box, in the left pane, click **Notification**.  
 See [“Notification options for scheduled storage operation jobs”](#) on page 413.
- 3 Select the check box for each recipient that you want to notify when each type of storage operation job completes.
- 4 You can continue selecting other options, or click **OK**.

## Notification options for scheduled storage operation jobs

When you create or edit a scheduled storage operation job, you can select recipients to receive notification when the job completes.

See [“Sending a notification when a scheduled storage operation job completes”](#) on page 413.

**Table 15-2** Notification options for scheduled storage operation jobs

Item	Description
<b>Recipient name</b>	Shows the names of the individual and group recipients.
<b>Recipient type</b>	Indicates <b>Recipient</b> for an individual recipient or <b>Group</b> for a group recipient.
<b>Manage Recipients</b>	Lets you add, edit, or delete recipients.  See <a href="#">“About managing recipients for alert notifications”</a> on page 292.

**Table 15-2** Notification options for scheduled storage operation jobs (*continued*)

Item	Description
<b>Properties</b>	<p>Lets you view or change the properties of a selected recipient.</p> <p>See <a href="#">“Add/Edit Individual Recipient options”</a> on page 294.</p> <p>See <a href="#">“Add/Edit Recipient Group options”</a> on page 296.</p>

## Schedule options for storage operation jobs

When you schedule a storage operation job, you can configure the time and frequency that you want to run the job.

See [“About storage operation jobs”](#) on page 410.

**Table 15-3** Schedule options for storage operation jobs

Item	Description
<b>Recurrence</b>	Specifies a recurring pattern on which to run the job.
<b>Recurrence pattern</b>	<p>Specifies the frequency with which the job recurs.</p> <p>You can choose to run the job in hourly, daily, weekly, monthly, or yearly increments.</p>
<b>Starting on</b>	Specifies the date on which the schedule takes effect.
<b>Calendar</b>	Lets you view all of the scheduled jobs on a calendar so that you can check for scheduling conflicts.
<b>Keep the job scheduled for X hours before it is rescheduled</b>	Specifies the maximum amount of time past the scheduled start time at which Backup Exec reschedules the job.
<b>Cancel the job if it is still running X hours after its scheduled start time</b>	Specifies the amount of time after the scheduled start time at which Backup Exec cancels the job if it is still running.
<b>Run now with no recurring schedule</b>	Runs the job immediately.

**Table 15-3** Schedule options for storage operation jobs (*continued*)

Item	Description
<b>Run on</b>	Specifies a schedule on which to run the job one time on the selected date at the selected time.

## Editing global settings for storage

You can edit the global settings that apply to the robotic libraries, media, and disk-based storage that are in your environment.

See [“Inventorying robotic libraries when Backup Exec services start”](#) on page 350.

See [“About media overwrite protection levels for tape and disk cartridge media”](#) on page 377.

See [“Editing disk storage properties”](#) on page 309.

### To edit global settings for storage

- 1 Click the Backup Exec button, click **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, click **Storage**.
- 3 Select the appropriate options.  
See [“Global settings for storage”](#) on page 415.
- 4 Click **OK**.

## Global settings for storage

Global settings for storage let you perform the following actions:

- Run an inventory job on robotic libraries whenever Backup Exec services start.
- Set the media overwrite protection level and the media overwrite options for tape media.
- Specify the number of days to protect disk-based storage from overwrite when you reattach it.

See [“Editing global settings for storage”](#) on page 415.

**Table 15-4** Global settings for storage

Item	Description
<b>Inventory robotic libraries when Backup Exec services start</b>	<p>Enables Backup Exec to inventory all of the slots in a robotic library when Backup Exec services start. Depending on the number of slots and robotic libraries, this process may take a few minutes.</p> <p>This option is not enabled by default.</p>
<b>Full - protect allocated and imported media</b>	<p>Prevents Backup Exec from overwriting media that are in media sets and the media that is imported from another installation of Backup Exec or from another product.</p> <p>See <a href="#">“About media overwrite protection and append periods”</a> on page 369.</p> <p>This is the safest option to choose because the media that is protected cannot be overwritten until one of the following actions occur:</p> <ul style="list-style-type: none"> <li>■ The overwrite protection period for the media expires.</li> <li>■ You move the media that belongs to an active media set to scratch media.</li> <li>■ You erase, format, or label the media.</li> <li>■ You move imported media to <b>Scratch Media</b>.</li> </ul>
<b>Partial - protect only allocated media</b>	<p>Lets Backup Exec overwrite scratch media and the media that is imported from another installation of Backup Exec or from another product. Media in a media set that has an overwrite protection period that has not expired (allocated media) cannot be overwritten.</p> <p>Symantec recommends this option if you want to use media from another installation of Backup Exec or from another product</p> <p>This option is enabled by default.</p>
<b>Prompt before overwriting imported media</b>	<p>Prompts you before Backup Exec overwrites media that is imported from another installation of Backup Exec or from another product. You must select the option <b>Partial - protect only allocated media</b>.</p> <p>The job cannot run until you respond to this prompt.</p>

Table 15-4 Global settings for storage (continued)

Item	Description
<b>None</b>	<p>Disables the media overwrite protection feature for media in tape and disk cartridges. With this option, you are responsible for making sure that the media in tape drives and disk cartridges are not accidentally overwritten.</p> <p>When an overwrite job is submitted to a tape drive and the media overwrite protection level is <b>None</b>, the media is overwritten.</p> <p><b>Note:</b> This option is not recommended because it does not protect data from being overwritten.</p>
<b>Prompt before overwriting allocated or imported media</b>	<p>Prompts you before Backup Exec overwrites allocated or imported media in tape and disk cartridges. If you selected <b>None</b>, Symantec recommended that you select this option to be prompted before overwriting allocated or imported media.</p> <p>The job cannot run until you respond to this prompt.</p>
<b>Overwrite scratch media before overwriting recyclable media contained in the targeted media set</b>	<p>Lets Backup Exec overwrite scratch media first in a tape drive or disk cartridge when an overwrite job occurs.</p> <p>See <a href="#">“How Backup Exec searches for overwriteable media in tape drives and disk cartridges”</a> on page 378.</p> <p>If no scratch media are found in any of the tape drives or disk cartridges, Backup Exec overwrites recyclable media in the selected media set.</p> <p>If no recyclable media are found in the selected media set, Backup Exec searches for recyclable media in any media set.</p> <p>If no recyclable media are found, Backup Exec automatically searches for other media to overwrite. The media that is overwritten depends on the level of the overwrite protection that you set. If you select this option, more media may be required for the same number of jobs than if you choose to overwrite recyclable media first.</p> <p>This option affects the order in which Backup Exec overwrites media. If you choose to overwrite scratch media first, the recyclable media may be preserved longer for possible recovery.</p> <p>This option is enabled by default.</p>

**Table 15-4** Global settings for storage (*continued*)

Item	Description
<p><b>Overwrite recyclable media contained in the targeted media set before overwriting scratch media</b></p>	<p>Lets Backup Exec overwrite recyclable media in a tape drive or disk cartridge in the seelcted media set first when an overwrite job occurs.</p> <p>If no recyclable media are found in any of the storage devices, Backup Exec overwrites scratch media.</p> <p>If no recyclable media or scratch media are found, Backup Exec searches for media to overwrite. The media that is overwritten depends on the level of the overwrite protection that you set.</p> <p>See <a href="#">“How Backup Exec searches for overwritable media in tape drives and disk cartridges”</a> on page 378.</p> <p>If you choose to overwrite recyclable media in the selected media set first, the same media is re-used more frequently than if you choose to overwrite scratch media first.</p>
<p><b>Limit Backup Exec to read-only operations on disk-based storage if it has been detached for at least</b></p>	<p>Specifies the number of days that the disk-based storage must be detached from the Backup Exec server before Backup Exec is limited to read-only operations.</p> <p>This setting prevents Backup Exec from reclaiming disk space on any disk-based storage device if you re-attach the device after a specified number of days.</p> <p>The default setting is 14 days.</p> <p>When the number of days specified has passed for a detached disk storage device, Backup Exec is then limited to read-only operations on any disk storage device that you reattach until you manually change the setting on the disk storage properties.</p> <p>See <a href="#">“Disk storage properties”</a> on page 310.</p> <p>See <a href="#">“About keeping backup sets”</a> on page 213.</p> <p>See <a href="#">“About restoring data from a reattached disk-based storage device”</a> on page 308.</p>

## About sharing storage devices

In environments in which there is more than one Backup Exec server, those servers can share storage devices. For example, multiple Backup Exec servers in a CASO environment can share storage devices. In these environments, Backup Exec

maintains a database of the shared storage device. Otherwise, the backup data that one server submits to the storage device can overwrite the data that another server submits.

Backup Exec servers can share the following types of storage:

- Storage that is attached to an NDMP server
- Deduplication disk storage
- OpenStorage devices
- Virtual disks
- Disk storage
- Remote Media Agents
- The Backup Exec agents that are configured to send data directly to storage

---

**Note:** For disk storage devices and virtual disk, you must specify a UNC path by which the Backup Exec servers can access the storage device.

---

When you share a storage device, you can select which Backup Exec servers can access the storage device. The Backup Exec server from which you added the storage device is automatically enabled to share the storage device. However, you can remove the sharing capability from that Backup Exec server at any time. For example, if you add a storage device to a central administration server, then that server can use the storage device. However, if your environment does not allow the central administration server to operate as a managed Backup Exec server, then you can remove the sharing capability from the central administration server.

If you have multiple Backup Exec servers and multiple types of storage in your environment, you can select a Backup Exec server and manage the storage for it.

See [“Sharing a storage device”](#) on page 419.

## Sharing a storage device

You can let multiple Backup Exec servers use the same storage device.

See [“About sharing storage devices”](#) on page 418.

### To share a storage device

- 1 On the **Storage** tab, right-click the storage device that you want to share.
- 2 Click **Share**.
- 3 To share a disk storage device or a virtual disk, enter a UNC path by which the servers can access the storage device that you want to share.

- 4 Check the Backup Exec servers or managed Backup Exec servers that you want to share this storage device.  
See [“Shared Storage options”](#) on page 420.
- 5 Click **OK**.

## Shared Storage options

You can let multiple Backup Exec servers access a storage device.

See [“Sharing a storage device”](#) on page 419.

**Table 15-5** Shared Storage options

Item	Description
<b>Enter a UNC path to share X</b>	Indicates the UNC path that the servers can use to access the storage device. <b>Note:</b> This field only displays when you share disk storage or a virtual disk.
<b>Server</b>	Indicates the names of the Backup Exec servers or managed Backup Exec servers that share the storage device.
<b>State</b>	Indicates the status of the shared storage device, or the status of the Backup Exec server that you selected to share the device. The server must be able to access the UNC path and the storage device.  See <a href="#">“Backup Exec server and storage device states”</a> on page 434.

## About deleting a storage device

You can delete a storage device from the Backup Exec Database. If the storage device is a legacy backup-to-disk folder or a disk storage device, then the associated files remain on the disk. You can recreate the legacy backup-to-disk folder or the disk storage device later. To delete the storage files from the disk, you must delete the backup sets.

If you delete the backup sets from the disk, then you cannot recreate the legacy backup-to-disk folder or the disk storage device.

You can also use Windows Explorer to navigate to the legacy backup-to-disk folder or to the disk storage and then delete it. If you delete the folder or disk storage from Windows, you cannot recreate the storage in Backup Exec.

A storage device must be offline or disabled before you can delete it. If the device is shared, it must be offline or disabled on the server from which you want to delete it.

See [“Disabling and enabling a storage device”](#) on page 425.

See [“Deleting a storage device”](#) on page 421.

See [“Recreating a legacy backup-to-disk folder and its contents”](#) on page 331.

See [“Deleting backup sets”](#) on page 214.

## Deleting a storage device

You can delete a storage device from the Backup Exec Database.

See [“About deleting a storage device”](#) on page 420.

### To delete a storage device

- 1 On the **Storage** tab, right-click the device that you want to delete.
- 2 Click **Delete**.
- 3 When you are prompted to delete the storage device, click **Yes**.

## Renaming a storage device

You can rename a storage device that is in your environment.

You cannot rename system-defined storage device pools, but you can rename any storage device pools that you create.

See [“About storage operation jobs”](#) on page 410.

### To rename a storage device

- 1 On the **Storage** tab, double-click the storage device that you want to rename.
- 2 In the storage device properties, in the **Name** field, type the new name.
- 3 Click **Apply**.

## Viewing jobs, job histories, backup sets, and active alerts for storage devices

You can view the job histories for a storage device. The job history is a report of what happened during the processing of the job.

See [“About storage operation jobs”](#) on page 410.

### To view jobs, job histories, backup sets, and active alerts for storage devices

- 1 On the **Storage** tab, double-click the storage device for which you want to view the job history, backup sets, or active alerts.

- 2 In the left pane, click the appropriate tab.

See [“About the Job History”](#) on page 260.

See [“About managing and monitoring active and scheduled jobs”](#) on page 247.

See [“About alerts”](#) on page 279.

See [“About backup sets”](#) on page 212.

## About inventorying a storage device

You can run an inventory operation to have Backup Exec read a storage device and update the Backup Exec database with information about the media that is on that device.

For robotic libraries, you can inventory all of the slots in the robotic library when you change tapes. You can also select specific slots to inventory. You are not required to re-inventory slots when you add the tapes that Backup Exec requests. For example, if the data that you want to restore is on a tape that is not in the robotic library, you are prompted to insert the correct tape for the restore operation. In this case, you are not required to re-inventory the slot where the tape is inserted. When you add or remove a tape that Backup Exec does not request, you should run an inventory operation on the changed slots. You can select specific slots to inventory. If you swap tapes often, you may want to run an inventory operation on the robotic library magazine each time that you restart the Backup Exec services.

For tape drives, you can run an inventory operation to mount the media in tape drives and to read the media label. If you change the media that is in a drive, run an inventory operation so that the current media's label appears in the properties. Otherwise, the previous media continues to appear in the properties. There may be a delay as the media is mounted and inventoried in a robotic library.

See [“Inventorying robotic libraries when Backup Exec services start”](#) on page 350.

See [“Inventorying a storage device”](#) on page 423.

## Inventorying a storage device

You can run an inventory operation to update the Backup Exec database with information about the media that is on the device.

See [“About storage operation jobs”](#) on page 410.

### To inventory a storage device

- 1 On the **Storage** tab, right-click the storage device that you want to inventory.
- 2 Click **Inventory**, and then do one of the following:

To immediately run an inventory operation

Click **Inventory**.

The inventory operation runs. You can view the job log for details about the job.

To schedule an inventory operation

Click **Schedule**.

Continue with the next step.

- 3 To send notification when the job completes, in the left pane, click **Notification** and select the appropriate options.

See [“Notification options for scheduled storage operation jobs”](#) on page 413.

- 4 To schedule the job, in the left pane, click **Schedule** and select the appropriate options.

See [“Schedule options for storage operation jobs”](#) on page 414.

- 5 Click **OK**.

- 6 (Optional) View the job log for details about the job.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Inventorying and cataloging a storage device

You can run the inventory and the catalog operations together on a storage device, if the device supports both operations.

See [“About storage operation jobs”](#) on page 410.

### To inventory and catalog a storage device

- 1 On the **Storage** tab, right-click the storage device that you want to inventory and catalog.
- 2 Click **Inventory and Catalog**.
- 3 (Optional) View the job history for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Cataloging a storage device

You can run a catalog operation to do the following:

- Log the contents of a media that was created by another installation of Backup Exec.
- Create a new catalog on the local hard drive if the catalog for the storage device no longer exists.

Before you can restore or verify data on a storage device, a catalog for that device must exist. If Backup Exec has not used this storage device before, you must run an **Inventory and Catalog** storage operation on the device first.

See [“Inventorying and cataloging a storage device”](#) on page 423.

See [“About catalogs ”](#) on page 242.

### To catalog storage

- 1 On the **Storage** tab, right-click the storage device for which you want to create a catalog.
- 2 Click **Catalog**.
- 3 (Optional) View the job log for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Scanning a storage device

The scan operation gets information about the media that are in the slots, including barcode information if it is available. Then, the scan operation updates the Backup Exec Database with the latest information about where the media are located. When you change magazines or insert new media in a magazine in a robotic library, use the scan operation to update the slot information.

See [“About storage operation jobs”](#) on page 410.

**To scan a storage device**

- 1 On the **Storage** tab, right-click the robotic library or slot that you want to scan.
- 2 Click **Scan**.
- 3 (Optional) View the job log for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Changing the state of a storage device to online

If storage goes offline, you can change the status to online after you correct the problem.

See [“Troubleshooting hardware-related issues”](#) on page 650.

**To change the state of a storage device to online**

- 1 On the **Storage** tab, right-click the storage device that you want to change to online.
- 2 Click **Offline** to clear the check mark.

## Pausing and unpausing a storage device

You can pause a storage device to prevent scheduled jobs and new jobs from running on the storage while you perform maintenance activities. Active jobs are not affected if they start before the storage device is paused.

See [“About storage operation jobs”](#) on page 410.

**To pause and unpause a storage device**

- 1 On the **Storage** tab, right-click the storage device that you want to pause.
- 2 Click **Pause**.
- 3 To unpause the storage device, right-click it, and then click **Pause** to clear the check mark.

## Disabling and enabling a storage device

You can disable a storage device to prevent scheduled and new jobs from running on it. Backup Exec does not discover disabled NDMP storage devices when the Backup Exec services start.

#### To disable and enable a storage device

- 1 On the **Storage** tab, right-click the storage device that you want to disable.
- 2 Click **Disable**.
- 3 To enable the storage device, right-click it, and then click **Disable** to clear the check mark.

## Initializing a robotic library

You can initialize the robotic library. You can also enable initialization whenever the Backup Exec service is started.

See [“About storage operation jobs”](#) on page 410.

See [“Editing global settings for storage”](#) on page 415.

#### To initialize a robotic library

- 1 On the **Storage** tab, right-click the robotic library that you want to initialize.
- 2 Click **Initialize**.
- 3 (Optional) View the job history for details about the job.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Retensioning a tape

You can run the tape in the tape drive from beginning to end at a fast speed. Retensioning helps the tape wind evenly and run more smoothly past the tape drive heads. Refer to the documentation that came with your tape drive to see how often to run this operation.

This operation is only available if the tape drive supports retensioning.

See [“About storage operation jobs”](#) on page 410.

#### To retension a tape

- 1 On the **Storage** tab, do either of the following:
  - Right-click the drive that contains the tape that you want to retension.

- Double-click **Slots**, and then right-click the slot that contains the tape that you want to retention.
- 2 Click **Retention**.
  - 3 (Optional) View the job log for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Formatting media in a drive

Backup Exec can format the media in a drive if the drive supports formatting. Most tape drives do not support formatting.

If you use the format operation on a DC2000 tape, the formatting may take two or more hours to complete.

---

**Caution:** Formatting erases the media. All data on the media is destroyed.

The media label that is displayed was read during the last inventory operation. The media label does not change until another inventory operation occurs. If you change the media that is in the device but do not inventory the device, the media label that displays may not match the actual media that is in the device.

---

See [“About storage operation jobs”](#) on page 410.

### To format media in a drive

- 1 On the **Storage** tab, do either of the following:
  - Right-click the drive that contains the tape that you want to format.
  - Double-click **Slots**, and then right-click the slot that contains the tape that you want to format.
- 2 Click **Format**.
- 3 To format the media that is displayed, click **Yes**.
- 4 (Optional) View the job log for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Labeling media

Backup Exec can write a new media label on the media in the selected drive. This operation destroys any data on the media. To change the media label without

destroying the data on the media until an overwrite operation occurs, rename the media label.

---

**Note:** Media that use barcode labels cannot be renamed. When you try to label the media that use barcode labels, the job logs report successfully completed jobs. However, the media label names do not change.

---

See [“About labeling tape and disk cartridge media”](#) on page 381.

#### To label media

- 1 On the **Storage** tab, do either of the following:
  - Right-click the drive that contains the tape that you want to label.
  - Double-click **Slots**, and then right-click the slot that contains the tape that you want to label.

- 2 Click **Label**.

The following warning appears:

This operation is performed on the current media in the drive or slot. If the media has changed since the last inventory ran, the media label in the next dialog may not match the media in the selected device.

- 3 Click **OK**.
- 4 Type the name that you want to use as the media label for this media.
- 5 To erase all data on the media and re-label the media, click **OK**.
- 6 Write this same media label on an external label that is fixed to the outside of the physical media.
- 7 (Optional) View the job history for details about the job.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Ejecting media from a disk cartridge or tape drive

Backup Exec can eject the media that is in a disk cartridge or tape drive. Some devices do not support a software-driven media eject. If the media is a tape, the tape is rewound and you may be instructed to manually remove it.

See [“About storage operation jobs”](#) on page 410.

### To eject media from a disk cartridge or tape drive

- 1 On the **Storage** tab, right-click the disk cartridge or tape drive that you want to eject the media from.
- 2 Do one of the following:

To eject the media now

Click **Eject media now**.

The eject operation runs. You can view the job log for details about the job.

To schedule an eject storage operation

Click **Schedule**.

Continue with the next step.

- 3 To send notification when the job completes, in the left pane, click **Notification** and select the appropriate options.

See [“Notification options for scheduled storage operation jobs”](#) on page 413.

- 4 To schedule the job, in the left pane, click **Schedule** and select the appropriate options.

See [“Schedule options for storage operation jobs”](#) on page 414.

- 5 Click **OK**.

- 6 (Optional) View the job history for details about the job.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Cleaning a robotic library drive

You can create and schedule a cleaning job for a robotic library drive. Additionally, if a cleaning media is in the slot, Backup Exec automatically cleans a robotic library drive when the drive issues an alert that it requires cleaning.

See [“About storage operation jobs”](#) on page 410.

### To create a cleaning job

- 1 Ensure that you have defined the slot that contains the cleaning tape.

See [“Defining a cleaning slot”](#) on page 351.

- 2 On the **Storage** tab, do either of the following:

- Right-click the drive that contains the cleaning tape.

- Double-click **Slots**, and then right-click the slot that contains the cleaning tape.
- 3 Click **Clean**.
- 4 To send a notification when the job completes, in the left pane, click **Notification** and select the options you want.  
See “[Notification options for scheduled storage operation jobs](#)” on page 413.
- 5 To schedule the job, in the left pane, click **Schedule** and select the options that you want.  
See “[Schedule options for storage operation jobs](#)” on page 414.
- 6 (Optional) View the job history for details about the job.  
See “[Viewing jobs, job histories, backup sets, and active alerts for storage devices](#)” on page 422.

## About importing media

When you insert media into a robotic library, you must create an import storage operation job. The import storage operation updates the Backup Exec Database with the information about the media.

Before you import media, note the following:

- If the media does not have a barcode, you must select the inventory after import storage operation.
- If the robotic library uses a media magazine, ensure that no jobs are currently running. Before you swap the magazine, ensure that all media are ejected from the drive and are back in the magazine slots.

You can select any number of slots to import media to.

The import storage operation supports robotic libraries with portals. When this storage operation job runs, Backup Exec checks the selected slots for media. If media is found, it is exported to the portals. After all of the media is exported, you are prompted to insert new media into the portal so it can be imported. This process continues until all of the requested media have been imported into the robotic library.

Use the inventory after import storage operation option to let Backup Exec inventory the slots after the import operation run.

See “[Importing media](#)” on page 431.

## Importing media

Run an Import storage operation to update the Backup Exec Database with information about the media that you insert into a robotic library.

### To import media

- 1 On the **Storage** tab, do one of the following
  - Expand the robotic library, right-click **Slots**, and then click **Import media now**.
  - Right-click the robotic library, and then click **Import media now**.
- 2 Do one of the following:

To immediately import the media that have barcodes	Click <b>Import media now</b> . The operation runs. You can view the job history for details about the job.
--	--

To immediately import the media that do not have barcode and inventory the slots after the operation	Click <b>Inventory after import</b> . The operation runs. You can view the job history for details about the job.
--	--

To schedule an import media job	Click <b>Schedule</b> . Continue with the next step.
---------------------------------	---

- 3 To send Notification when the job completes, in the left pane, click **Notification** and select the appropriate options.  
See [“Notification options for scheduled storage operation jobs”](#) on page 413.
- 4 To schedule the job, in the left pane, click **Schedule** and select the appropriate options.  
See [“Schedule options for storage operation jobs”](#) on page 414.
- 5 Click **OK**
- 6 (Optional) View the job history for details about the job.  
See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## About exporting expired media

The export expired media operation lets you automate media handling in robotic libraries. This operation removes the media that Backup Exec cannot write to.

You can then use the import storage operation to add scratch media to the robotic library to prepare for the next backup.

After you export the expired media from the robotic library, the expired media appears in **OfflineTape/Disk Cartridge Media**. If the media is in a media set that has an applicable vault media rule, then the media appears in the vault location.

You can export cleaning media with the export expired media storage operation. You can include all cleaning media, or all cleaning media that has been used more than a specified number of times.

You can choose to be reminded to import new media after an export expired media operation completes successfully.

See [“Robotic library slot properties” on page 432](#) on page 432.

## Exporting media

The export media operation fully supports robotic libraries that have portals. When this operation is run on one or more robotic library slots, the exported media is placed in the portals. If you select more media than there are portals, the robotic library fills as many slots as possible. Then, you are prompted to remove the media from the portal. This process continues until all of the selected media have been removed from the robotic library. You can also export expired media from a robotic library.

See [“About storage operation jobs”](#) on page 410.

See [“About exporting expired media”](#) on page 431.

See [“About importing media”](#) on page 430.

### To export media

- 1 On the **Storage** tab, do one of the following: .
  - Expand the robotic library, right-click **Slots**, and then click **Export media now**.

- Right-click the robotic library, and then click **Export media now**.
- 2 Do one of the following:

To immediately export the media to the portal	Click <b>Export media now</b> . The operation runs. You can view the job history for details about the job.
To immediately export only the media that Backup Exec cannot write to and place it in the portal	Click <b>Export expired media now</b> . The operation runs. You can view the job history for details about the job.
To immediately import media after the export	Click <b>Import after export</b> . The operation runs. You can view the job history for details about the job.
To schedule an export media job	Click <b>Schedule</b> . Continue with the next step.
  - 3 To send notification when the job completes, in the left pane, click **Notification** and select the appropriate options.  
See “[Notification options for scheduled storage operation jobs](#)” on page 413.
  - 4 To schedule the job, in the left pane, click **Schedule** and select the appropriate options.  
See “[Schedule options for storage operation jobs](#)” on page 414.
  - 5 Click **OK**.
  - 6 (Optional) View the job history for details about the job.  
See “[Viewing jobs, job histories, backup sets, and active alerts for storage devices](#)” on page 422.

## About locking the robotic library's front portal

By default, the robotic library portal is not locked, even when you run the lock storage operation. For instructions on how to lock the library portal, go to:

<http://www.symantec.com/docs/TECH67698>

## Unlocking the robotic library's front portal

You must create a job to unlock the robotic library's front portal.

See [“About storage operation jobs”](#) on page 410.

**To unlock the robotic library’s front portal**

- 1 On the **Storage** tab, right-click the robotic library that has the front portal that you want to unlock.
- 2 Click **Unlock**.
- 3 (Optional) View the job log for details about the job.

See [“Viewing jobs, job histories, backup sets, and active alerts for storage devices”](#) on page 422.

## Backup Exec server and storage device states

Backup Exec servers and storage devices display a state that indicates their current condition.

**Table 15-6** Possible states for Backup Exec servers and storage devices

State	Description
All the Backup Exec services need to be restarted on <Backup Exec server>	The Backup Exec services and the Backup Exec deduplication services must be restarted.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.
An error occurred while discovering this device. Cycle the services on <Backup Exec server> to retry device discovery.	The Backup Exec services must be restarted.  See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.
Active	The storage device is in use by a job.
Configuration failed	Configuration has failed for a local disk storage device or virtual disk.
Configuring	A local disk storage device or virtual disk is in the process of configuration.
Disabled	The storage device is disabled and Backup Exec cannot use it. The device is available for other applications.
Disabled; Active	The storage device was changed to disabled while a job was running to the device.

**Table 15-6** Possible states for Backup Exec servers and storage devices  
*(continued)*

State	Description
Low disk space; Active	The storage device is in a low disk space condition, but is currently in use by a job.
Low disk space	The storage device has low disk space. See <a href="#">“Disk storage properties”</a> on page 310. See <a href="#">“Deduplication disk storage properties”</a> on page 762. See <a href="#">“Properties for virtual disks on storage arrays”</a> on page 1180.
No communication	Communications have stopped between a managed Backup Exec server and a central administration server in a Central Admin Server Option environment. See <a href="#">“What happens when CASO communication thresholds are reached”</a> on page 1025.
Not configurable	The disk cannot be configured because it is in a bad state, or it has failed.
Not configured	The disk is available for configuration but has not yet been configured.
Offline	The storage device is offline. A storage device can appear offline if any of the following actions occur: <ul style="list-style-type: none"> <li>■ The device was turned off after Backup Exec started.</li> <li>■ The device was being used by another application when Backup Exec started.</li> <li>■ The device is removed from the server.</li> <li>■ The device reports a critical error.</li> <li>■ The firmware of the device was updated.</li> </ul> See <a href="#">“Changing the state of a storage device to online”</a> on page 425.
Online	The storage device is online.

**Table 15-6** Possible states for Backup Exec servers and storage devices  
*(continued)*

State	Description
Paused	The storage device is paused.  See <a href="#">"Pausing and unpausing a storage device"</a> on page 425.
Paused; Active	The storage device is paused, but is currently in use by a job.
Stalled	Communications have stalled during communications between a managed Backup Exec server and a central administration server in a Central Admin Server Option environment.  See <a href="#">"What happens when CASO communication thresholds are reached"</a> on page 1025.
The Backup Exec deduplication services need to be restarted on <Backup Exec server>.	The Backup Exec deduplication services should be restarted. The deduplication services are separate from the Backup Exec services so the Backup Exec services are not affected.  See <a href="#">"Starting and stopping Backup Exec services"</a> on page 511.
The Backup Exec services on <Backup Exec server> need to be restarted	The Backup Exec services must be restarted.  See <a href="#">"Starting and stopping Backup Exec services"</a> on page 511.
This device has not been discovered correctly. Cycle the services on <Backup Exec server> to retry device discovery.	A state that can occur after you add a new storage device to Backup Exec. You must restart the Backup Exec services so that the device discovery process can run again.
Uninitialized	The device has not been initialized.

# Virtualization

This chapter includes the following topics:

- [About conversion to virtual machines](#)
- [Requirements for conversion to virtual machines](#)
- [Creating a backup job with a simultaneous conversion to a virtual machine](#)
- [Creating a backup job with a conversion to a virtual machine after the backup](#)
- [Adding a stage to convert to a virtual machine](#)
- [Converting to a virtual machine from a point in time](#)
- [Virtual machine conversion options](#)
- [Disk configuration details](#)
- [About editing a conversion to virtual machine job](#)
- [Setting default options for conversion to virtual machines](#)

## About conversion to virtual machines

Backup Exec provides the ability to convert to virtual machines in the following ways:

- Back up a physical computer and simultaneously convert it to a virtual machine.
- Back up a physical computer and schedule a conversion to a virtual machine to run after the backup job runs.
- Convert existing backup sets to a virtual machine.

The newly created virtual machine is bootable and is identical to the physical computer from which the virtual machine was converted. Conversion to a virtual machine enables business continuity for both Hyper-V and VMware environments.

You use one of the following backup options on the **Backup and Restore** tab to set up a conversion to a virtual machine with a backup job:

**Table 16-1** Convert to virtual machine options

Name of option	Description
<p><b>Back up to Disk and Simultaneously Convert to Virtual Machine</b></p> <p><b>Back up to Deduplication Disk Storage and Simultaneously Convert to Virtual Machine</b></p>	<p>These options run the conversion simultaneously with the backup job. Because two operations are performed at the same time, this job may take longer to run than a regular backup job. A large backup window is recommended for this option.</p> <p>A conversion from a full backup creates the new virtual machine. Incremental and differential backups are not converted.</p> <p>Although the backup runs simultaneously with the conversion, the backup is the primary job. Therefore, if the backup fails, then the conversion fails also. However, if the conversion fails, the backup continues to run. For a conversion failure, the job is marked as a success with exceptions. In the case of a failed conversion, the conversion process runs again during the next full backup.</p>
<p><b>Back Up to Disk and then Convert to Virtual Machine</b></p> <p><b>Back Up to Deduplication Disk Storage and then Convert to Virtual Machine</b></p>	<p>These options let you schedule the conversion to run after the backup job. These options require a smaller backup window than the simultaneous conversion options.</p> <p>A conversion from a full backup creates the new virtual machine. Incremental and differential backups are not converted.</p>

Alternatively, you can add a stage to a backup job to convert to a virtual machine. Two types of stages are available: **Convert to Virtual Machine After Backup** and **Convert to Virtual Machine Simultaneously with Backup**.

The option **Convert to Virtual From Point-in-Time** is also available. A conversion to a virtual machine from a point in time converts existing backup sets from a backup job in which all components that are necessary for a virtual machine

conversion were selected. When a backup job has all necessary components selected, Backup Exec identifies that job as **Fully selected** and the **Simplified Disaster Recovery** option has a status of **ON**. The option to convert to a virtual machine from a point in time is useful in a disaster recovery situation in which you want to quickly recover a failed server. The backup sets contain all of the critical components of the server. Additionally, you can select application data or user data to include in the conversion.

---

**Note:** The option **Convert to virtual machine from point-in-time** becomes available for selection only after you run at least one full backup that includes all critical system components.

---

Regardless of the option that is used to initiate the conversion, Backup Exec does not power on the virtual machine after creating it. You should not power on the virtual machine to validate that the conversion completed successfully.

Backup Exec creates a snapshot of the virtual machine at the end of the conversion process. The snapshot is removed before the next job runs as long as the virtual machine is not powered on and the only snapshot on the virtual machine is the one that Backup Exec created. If you want to start using the virtual machine, you must manually remove the snapshot.

If the converted virtual machine's host fails and you bring the virtual machine online, the existing conversion job continues to run and then fails. In this situation, you must create a new conversion job.

See [“Requirements for conversion to virtual machines”](#) on page 439.

See [“Creating a backup job with a simultaneous conversion to a virtual machine”](#) on page 440.

See [“Creating a backup job with a conversion to a virtual machine after the backup”](#) on page 441.

## Requirements for conversion to virtual machines

Before you use the conversion to virtual machine feature, review the following requirements:

- For conversion in a Hyper-V environment:
  - Windows Server 2008 SP2 or R2 is required on the Backup Exec server.
  - The Agent for Windows must be installed on the Hyper-V host to which the conversion is sent.
  - The maximum disk size is 2 TB.

- For conversion in a VMware environment, VMware ESX 4.0 or later is supported.
- The option **Simplified Disaster Recovery** must have a status of **ON** on the **Browse** tab of the **Backup Selections** dialog box.
- Only basic disks are supported. Dynamic disks are not supported.
- Only Windows servers are supported.

---

**Note:** The Agent for VMware and Hyper-V is not required for conversion to virtual machines.

---

See “[About conversion to virtual machines](#)” on page 437.

## Creating a backup job with a simultaneous conversion to a virtual machine

With this type of a conversion, the backup and the conversion run at the same time.

---

**Note:** If the backup fails, then the conversion fails also. However, if the conversion fails, the backup continues to run. For a conversion failure, the job is marked as a success with exceptions and the conversion process runs again during the next full backup.

---

### To create a backup job with a simultaneous conversion to a virtual machine

- 1 On the **Backup and Restore** tab, right-click the server that contains the data you want to back up and convert.
- 2 Select **Backup**, and then select **Back up to Disk and Simultaneously Convert to Virtual Machine** or **Back up to Deduplication Disk Storage and Simultaneously Convert to Virtual Machine**, depending on the type of storage device that you want to use.

**3** Do any of the following:

To change the backup selections

In the <Name of Server> box, click **Edit**, and then select the items to back up.

**Note:** The option **Simplified Disaster Recovery** must have a status of **ON**.

Click **OK**.

To change the backup options

In the **Backup** box, click **Edit**, and then change the backup options as needed.

Click **OK**.

- 4** In the **Conversion to Virtual** box, click **Edit** to set the options for conversion. See [“Virtual machine conversion options”](#) on page 446.
- 5** Click **OK**.
- 6** On the **Backup Properties** dialog box, click **OK** to create the job. See [“About conversion to virtual machines”](#) on page 437.

## Creating a backup job with a conversion to a virtual machine after the backup

Backup Exec sets up this type of conversion as a stage that runs after the backup job runs. The backup sets that are created from the backup job are used to create the virtual machine.

**To create a backup job with a conversion to a virtual machine after the backup**

- 1** On the **Backup and Restore** tab, right-click the server that contains the data you want to back up and convert.
- 2** Select **Backup**, and then select **Back Up to Disk and then Convert to Virtual Machine** or **Back Up to Deduplication Disk Storage and then Convert to Virtual Machine**, depending on the type of storage device that you want to use.

**3** Do any of the following:

To change the backup selections

In the <Name of Server> box, click **Edit**, and then select the items to back up.

**Note:** The option **Simplified Disaster Recovery** must have a status of **ON**.

Click **OK**.

To change the backup options

In the **Backup** box, click **Edit**, and then change the backup options as needed.

Click **OK**.

**4** In the **Conversion to Virtual** box, click **Edit**.

**5** In the left pane, select **Schedule** to schedule the conversion.

See [“Schedule options for a conversion to virtual machine job”](#) on page 442.

**6** In the left pane, select **Notification** if you want to notify a recipient when the job completes.

See [“Notification options for a conversion to virtual machine job”](#) on page 443.

**7** In the left pane, select **Conversion Settings** to set the options for the conversion.

See [“Virtual machine conversion options”](#) on page 446.

**8** Click **OK** to save your selections.

**9** On the **Backup Properties** dialog box, click **OK** to create the job.

See [“About conversion to virtual machines”](#) on page 437.

## Schedule options for a conversion to virtual machine job

The following scheduling options appear for a conversion to a virtual machine after a backup job runs. These options also appear when you set default schedule options for conversion to virtual machines.

See [“Creating a backup job with a conversion to a virtual machine after the backup”](#) on page 441.

See [“Setting default options for conversion to virtual machines”](#) on page 451.

**Table 16-2** Schedule options for a conversion to a virtual machine after a backup

Item	Description
<b>According to schedule</b>	Lets you schedule the conversion to occur any time after the backup job runs.
<b>Source</b>	Lets you select all backups or the most recent full backup as the source to initiate the scheduled conversion.
<b>Schedule</b>	Lets you select the frequency, start date, and options for the scheduled conversion.
<b>Convert to virtual immediately after source task completes</b>	Initiates the conversion immediately after the backup job completes.
<b>Submit job on hold</b>	Lets you submit the job with an on-hold status.

## Notification options for a conversion to virtual machine job

The following notification options appear for jobs that convert to a virtual machine after a backup job runs. These options also appear when you set default notification options for conversion to virtual machines.

See [“Creating a backup job with a conversion to a virtual machine after the backup”](#) on page 441.

**Table 16-3** Notification options

Item	Description
<b>Recipient name</b>	Shows the names of the individual and group recipients.
<b>Recipient type</b>	Indicates <b>Recipient</b> for an individual recipient or <b>Group</b> for a group recipient.
<b>Include the job log with email notifications</b>	Enables Backup Exec to include a copy of the job log with the notification.
<b>Manage Recipients</b>	Lets you add, edit, or delete recipients.
<b>Properties</b>	Lets you view or change the properties of the selected recipient.

## Adding a stage to convert to a virtual machine

You can add a stage to a backup definition to convert a backup to virtual machine. A conversion to virtual machine job requires that the **Simplified Disaster Recovery** option on the backup selections has a status of **ON**. This status means that all components that are necessary for virtualization are selected. Backup Exec automatically selects the necessary components when you add a stage to convert to a virtual machine.

### To add a stage to convert to a virtual machine

- 1 Create a backup job, or edit an existing job.
- 2 In the **Backup** box, click **Add Stage**.
- 3 Select **Convert to Virtual Machine** to set up a conversion to run after the backup job completes, or select **Convert to Virtual Simultaneously With Backups** to run the conversion at the same time as the backup job.
- 4 In the **Conversion to Virtual** box, click **Edit**.
- 5 If you selected the **Convert to Virtual Machine** option in step 3, in the left pane, select **Schedule** to schedule the conversion, and then select **Notification** if you want to notify a recipient when the job completes.  
See [“Schedule options for a conversion to virtual machine job”](#) on page 442.  
See [“Notification options for a conversion to virtual machine job”](#) on page 443.
- 6 In the left pane, select **Conversion Settings** to set the options for the conversion.  
See [“Virtual machine conversion options”](#) on page 446.
- 7 Click **OK** to save your selections.
- 8 On the **Backup Properties** dialog box, edit the backup job properties, and then click **OK** to create the job.  
See [“About conversion to virtual machines”](#) on page 437.

## Converting to a virtual machine from a point in time

A conversion to a virtual machine from a point in time converts existing backup sets from a backup job in which the Simplified Disaster Recovery option was enabled. The Simplified Disaster Recovery option enables all of the critical system components for a virtual machine conversion to be included in the backup job.

---

**Note:** The option **Convert to virtual machine from point-in-time** becomes available for selection only after you run at least one full backup that includes all critical system components.

---

The option to convert to a virtual machine from a point in time is useful in a disaster recovery situation in which you want to quickly recover a failed server. The backup sets contain all of the necessary components of the system. Additionally, you can select application data or user data to include in the conversion.

#### To convert to a virtual machine from a point in time

- 1 On the **Backup and Restore** tab, select the server that contains the backup sets you want to convert.
- 2 In the **Virtualization** group, click **Convert**, and then select **Convert to virtual from point-in-time**.
- 3 On the **Options** dialog box, in the **Selected Point-in-Time** box, click **Edit**.
- 4 Select the items that you want to include in the conversion, and then click **OK**.  
See [“Conversion from point in time options”](#) on page 445.
- 5 On the **Options** dialog box, in the **Convert to Virtual** box, click **Edit**.
- 6 In the left pane, select **Schedule** to schedule the conversion, and then select **Notification** if you want to notify a recipient when the job completes.  
See [“Schedule options for a conversion to virtual machine job”](#) on page 442.  
See [“Notification options for a conversion to virtual machine job”](#) on page 443.
- 7 In the left pane, select **Conversion Settings** to set the options for the conversion  
See [“Virtual machine conversion options”](#) on page 446.
- 8 Click **OK** to save your selections.
- 9 On the **Options** dialog box, click **OK**.

## Conversion from point in time options

A conversion to a virtual machine from a point in time converts existing backup sets from a backup job in which the Simplified Disaster Recovery option was enabled.

See [“Converting to a virtual machine from a point in time”](#) on page 444.

**Table 16-4** Conversion from point-in-time options

Item	Description
<b>Point in time</b>	Lets you select the point in time that you want to use for the conversion.
<b>Name</b>	Lets you select all of the components for inclusion in the conversion.
<b>Components necessary for a complete online restore</b>	Indicates the components that Backup Exec requires to complete the operation. You cannot deselect these components.
<b>Application data or non-system user data</b>	Lets you select additional data to include in the conversion.

## Schedule options for a conversion from a point in time

The following schedule options appear for a conversion to a virtual machine from a point in time.

See [“Converting to a virtual machine from a point in time”](#) on page 444.

**Table 16-5** Schedule options for a conversion to a virtual machine from a point in time

Item	Description
<b>Job priority</b>	Lets you set the priority for the job.
<b>Run now</b>	Enables the job to run immediately.
<b>Run on</b>	Lets you select the date and time when you want the job to run.
<b>Submit job on hold</b>	Lets you submit the job with an on-hold status.

## Virtual machine conversion options

The options for virtual machine conversion vary depending on whether you choose to convert for a Hyper-V environment or a VMware environment.

See [“Creating a backup job with a simultaneous conversion to a virtual machine”](#) on page 440.

See [“Creating a backup job with a conversion to a virtual machine after the backup”](#) on page 441.

The following options appear when you select a virtual machine conversion for a VMware environment.

**Table 16-6** VMware virtual machine conversion options

Item	Description
<b>Convert for</b>	Lets you select conversion for either Hyper-V or VMware.
<b>ESX/ vCenter server name</b>	Lets you specify the name or IP address of the ESX or vCenter server. After you type the name or IP address, you should select the appropriate logon account for the server before you click <b>Select</b> to choose the datastore or datastore cluster. After you select these items, Backup Exec fills in the remaining information for the server.
<b>Logon account</b>	Lets you select the appropriate logon account for the ESX or vCenter server.
<b>Data center</b>	Indicates the name of the datacenter that is associated with the ESX or vCenter server that you selected.
<b>Datastore or Datastore Cluster</b>	Indicates the name of the datastore that is associated with the ESX or vCenter server that you selected.
<b>Host or cluster</b>	Indicates the name of the host or cluster that is associated with the ESX or vCenter server that you selected.
<b>Virtual machine folder</b>	Lets you enter the name of the virtual machine folder that is associated with the ESX or vCenter server that you selected.
<b>Resource pool</b>	Lets you enter the name of the resource pool that is associated with the ESX or vCenter server that you selected.

**Table 16-6** VMware virtual machine conversion options (*continued*)

Item	Description
<b>Virtual machine name</b>	<p>Shows the name of the virtual machine. Backup Exec generates this name automatically by adding "VM-" before the name of the physical computer.</p> <p>For example, if the physical computer name is Server1, then the virtual machine name is VM-Server1.</p> <p><b>Note:</b> This name is the display name and not the actual machine name.</p>
<b>Overwrite the virtual machine if it already exists</b>	<p>Indicates whether Backup Exec can overwrite a virtual machine if a virtual machine with the same name already exists.</p> <p>If this option is not selected and the virtual machine already exists, then the job will fail.</p>
<b>Full path of VMware Tools ISO image</b>	<p>Indicates the location of your VMware Tools ISO image.</p> <p>This path should be accessible with the default credentials. The ISO image is needed to make the virtual machine bootable.</p> <p>If you use a network disk, Symantec recommends using a mapped drive on the local Backup Exec server.</p>
<b>Server configuration</b>	<p>Shows the CPU count and the amount of physical RAM on the physical computer and the amount on the destination virtual machine. You can change the amounts for the virtual machine. However, the amounts are limited by the amounts on the host server.</p>
<b>Disk configuration</b>	<p>Lets you view and edit the properties of the disks for the virtual machine.</p>
<b>Edit disk configuration</b>	<p>Lets you change the disk type and the virtual disk name for any disk in the list. You can also set the datastore to which each virtual disk is sent.</p> <p>See <a href="#">“Disk configuration details”</a> on page 450.</p>

The following options appear when you select a virtual machine conversion for a Hyper-V environment.

**Table 16-7** Hyper-V virtual machine conversion options

Item	Description
<b>Convert for</b>	Indicates whether the conversion is for Hyper-V or VMware.
<b>Hyper-V server name</b>	Indicates the name of the Hyper-V server where you want to create the virtual machine.
<b>Destination drive or path</b>	Indicates the location on the physical computer where the virtual disks should be located. Enter a UNC path.
<b>Logon account</b>	Indicates the logon account for the Hyper-V server that was selected in the <b>Hyper-V server</b> field.
<b>Virtual machine name</b>	Shows the name of the virtual machine. Backup Exec generates this name automatically.  For example, if the physical computer name is AccountingServer, then the virtual machine name is VM-AccountingServer.
<b>Overwrite the virtual machine if it already exists</b>	Indicates whether Backup Exec can overwrite a virtual machine if a virtual machine with the same name already exists.  If this option is not selected and the virtual machine already exists, the job fails.
<b>Full path of Hyper-V Integration Components ISO image</b>	Indicates the location of your Hyper-V Integration Components ISO image.  The ISO image is needed to make the virtual machine bootable.  <b>Note:</b> You cannot use a UNC path for remote shares. However, you can map a drive to the remote share.

**Table 16-7** Hyper-V virtual machine conversion options (*continued*)

Item	Description
<b>Server configuration</b>	Shows the CPU count and the amount of physical RAM on the physical computer and the amount on the destination virtual machine. You can change the amounts for the virtual machine. However, the amounts are limited by the amounts on the host server.
<b>Disk configuration</b>	Lets you view and edit the properties of the disks for the virtual machine.
<b>Edit disk configuration</b>	Lets you change the disk type and the virtual disk name for any disk in the list.  See <a href="#">“Disk configuration details”</a> on page 450.

## Disk configuration details

You can edit the disk type and the virtual disk name.

See [“Creating a backup job with a conversion to a virtual machine after the backup”](#) on page 441.

See [“Creating a backup job with a simultaneous conversion to a virtual machine”](#) on page 440.

See [“Virtual machine conversion options”](#) on page 446.

**Table 16-8** Disk configuration details

Item	Description
<b>Disk name</b>	Indicates the name of the disk, such as Disk 1. The Boot or System disk is always listed as Disk 0.
<b>Disk size</b>	Indicates the current size of the disk.
<b>Controller</b>	Indicates the type of disk controller, such as IDE or SCSI.

**Table 16-8** Disk configuration details (*continued*)

Item	Description
<b>Disk type</b>	Indicates the type of disk. For VMware, the choices are thin or thick. For Hyper-V, the choices are fixed size or dynamically expanding.
<b>Virtual disk name</b>	Indicates the name that Backup Exec generated for the virtual disk. Backup Exec generates the name of the disks automatically by adding an underscore and a number at the end of the physical computer name. For example, if the physical computer name is Server1, then the disks are named Server1_1, Server1_2, and so on. The name of the Boot or System disk does not have a number appended to the physical computer name.
<b>Virtual disk location</b>	Indicates the datastore where the VMDK file (for VMware) or the VHD file (for Hyper-V) is placed.

## About editing a conversion to virtual machine job

After a conversion to virtual machine job is created, the **Convert for** field cannot be changed. For example, a conversion for a Hyper-V environment cannot be changed to a conversion for a VMware environment. However, you can change the other conversion settings for the job.

See “[About conversion to virtual machines](#)” on page 437.

## Setting default options for conversion to virtual machines

You can set default options for all conversion to virtual machine jobs. However, you can override the default options by changing the defaults for individual jobs.

### To set default options for conversion to virtual machines

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Job Defaults**, and then select **Convert to Virtual**.

- 3 Set the default options for the schedule, notification, and conversion.
  - See [“Schedule options for a conversion to virtual machine job”](#) on page 442.
  - See [“Notification options for a conversion to virtual machine job”](#) on page 443.
  - See [“Default conversion settings for conversion to virtual machines”](#) on page 452.
- 4 Click **OK**

## Default conversion settings for conversion to virtual machines

The following default options are available for conversion to virtual machines in a Hyper-V environment.

See [“Setting default options for conversion to virtual machines”](#) on page 451.

**Table 16-9** Default conversion options for Hyper-V

Item	Description
<b>Convert for</b>	Indicates whether the conversion is for Hyper-V or VMware.
<b>Hyper-V server name</b>	Indicates the name of the Hyper-V server where you want to create the virtual machine.
<b>Destination drive or path</b>	Indicates the location on the physical computer where the virtual disks should be located. Enter a fully-qualified path.
<b>Logon account</b>	Indicates the logon account for the Hyper-V server that was selected in the <b>Hyper-V server name</b> field.
<b>Overwrite the virtual machine if it already exists</b>	Indicates whether Backup Exec can overwrite a virtual machine if a virtual machine with the same name already exists.  If this option is not selected, the job fails.
<b>Full path of Hyper-V Integration Components ISO image</b>	Indicates the location of your Hyper-V Integration Components ISO image.  The ISO image is needed to make the virtual machine bootable.  You cannot use a UNC path for remote shares. However, you can map a drive to the remote share.

The following default options are available for conversion to virtual machines in a VMware environment.

**Table 16-10**      Default conversion options for VMware

<b>Item</b>	<b>Description</b>
<b>Convert for</b>	Indicates whether the conversion is for Hyper-V or VMware.
<b>ESX/ vCenter server name</b>	Lets you specify the name or IP address of the ESX or vCenter server. After you type the name or IP address, you should select the appropriate logon account for the server before you click <b>Select</b> to choose the datastore or datastore cluster. After you select these items, Backup Exec fills in the remaining information for the server.
<b>Logon account</b>	Lets you select the appropriate logon account for the ESX or vCenter server.
<b>Overwrite the virtual machine if it already exists</b>	Indicates whether Backup Exec can overwrite a virtual machine if a virtual machine with the same name already exists.  If this option is not selected, the job fails.
<b>Full path of VMware Tools ISO image</b>	Indicates the location of your VMware Tools ISO image.  The path should be accessible with the default credentials. The ISO image is needed to make the virtual machine bootable.  Symantec recommends that you use a mapped drive on the local Backup Exec server.



# Configuration and settings

This chapter includes the following topics:

- [About configuring Backup Exec](#)
- [About job defaults](#)
- [About global Backup Exec settings](#)
- [About logon accounts](#)
- [About the Backup Exec Services Manager](#)
- [About audit logs](#)
- [Copying configuration settings to another Backup Exec server](#)
- [About viewing server properties](#)

## About configuring Backup Exec

When you start Backup Exec for the first time, defaults are already configured. You can adjust the defaults to meet the needs of your environment. Default settings are available for the following:

- Jobs  
See [“About job defaults”](#) on page 456.
- Backup Exec settings  
See [“About global Backup Exec settings”](#) on page 463.
- Logon accounts  
See [“About logon accounts”](#) on page 498.
- Alerts and notifications  
See [“About alerts”](#) on page 279.

Additionally, you can perform the following configuration techniques to help you to better manage your backup operations:

- Starting, stopping, or setting startup options for services using Backup Exec Services Manager  
See [“About the Backup Exec Services Manager”](#) on page 511.
- Reviewing information about operations using audit logs  
See [“About audit logs”](#) on page 516.
- Copying configuration settings from one server to another  
See [“Copying configuration settings to another Backup Exec server”](#) on page 519.
- Viewing server properties  
See [“About viewing server properties”](#) on page 523.

## About job defaults

When you start Backup Exec for the first time, defaults are already configured. You can run backup and restore jobs safely by using only the defaults that were set during installation. After you establish a backup strategy and configure your storage devices, you may want to customize the default settings to better meet your needs. Job defaults can be changed for individual jobs if the default settings do not apply.

You can configure job defaults for the following:

- Backup jobs  
See [“Setting default backup job settings”](#) on page 456.
- Restore jobs  
See [“Setting defaults for restore jobs”](#) on page 231.
- Schedule settings  
See [“Setting global schedule options”](#) on page 457.
- Dates that you want to exclude from the backup schedule  
See [“About excluding dates from the backup schedule”](#) on page 458.
- Content that you want to exclude from backups  
See [“Excluding selections from all backups”](#) on page 462.

## Setting default backup job settings

Backup Exec is preconfigured with default settings for backup jobs. You can change the default settings for your backup jobs. When you create a backup job, the job inherits the default settings that you configure. You can override the default

settings for backup jobs when you create them. Backup job settings include storage, security, and file system options for backup jobs, among other things.

You can set unique backup job defaults for the following types of backup jobs:

- Back Up to Deduplication Disk Storage Device
- Back Up to Disk
- Back Up to Tape
- Duplicate to Deduplication Disk Storage Device
- Duplicate to Tape
- Convert to Virtual

---

**Note:** Backup Exec displays only the types of backup jobs for which your system is configured. For example, if you do not have a tape drive, you do not see the Back Up to Tape option in the list of backup job types.

---

#### To set default backup job settings

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select the type of backup for which you want to set default options.
- 3 In the left pane, select the setting for which you want to configure default options.  
See [“About backup job settings”](#) on page 185.
- 4 Select the appropriate options.
- 5 When you are finished configuring default options, click **OK**.

## Setting global schedule options

You can configure global schedule options. Backup Exec applies the global schedule options whenever you change a rule-based job or a run now job into a recurring scheduled job. You can override the global settings when you edit the newly scheduled job.

See [“About job defaults”](#) on page 456.

#### To set global schedule options

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select **Schedule**.

- 3 Select the appropriate options.  
 See “[Global schedule options](#)” on page 458.
- 4 Click **OK**.

## Global schedule options

You can configure global schedule options as default settings. Backup Exec applies the global schedule options whenever you change a rule-based job or a run now job into a recurring, scheduled job.

See “[Setting global schedule options](#)” on page 457.

**Table 17-1** Global schedule options

Item	Description
<b>Recurrence pattern</b>	Lets you configure the frequency with which jobs recur. You can select to run jobs in hourly , daily, weekly, monthly, or yearly increments.
<b>Starting on</b>	Designates the date on which the schedule takes effect.
<b>Calendar</b>	Lets you view all scheduled jobs on a calendar to check for scheduling conflicts.
<b>Keep the job scheduled for X hours before it is rescheduled</b>	Specifies the maximum amount of time past the job's scheduled start time at which Backup Exec considers the job to be missed and reschedules it.
<b>Cancel the job if it is still running X hours after its scheduled start time</b>	Specifies the amount of time after the job's scheduled start time at which you want to cancel the job if it is still running.

## About excluding dates from the backup schedule

You can exclude specific dates, such as holidays, from your backup schedule. When you exclude dates, any scheduled backups do not run on those dates. You can still create and run backup jobs and restore jobs on excluded dates, as long as they are not scheduled.

You can exclude dates in Backup Exec by selecting or typing dates on the **Exclude Dates** dialog box. Or you can create a .txt file with a list of dates to exclude and then import the .txt file. After you create a list of dates to exclude, you can export a new .txt file with those dates. Exporting the .txt file can be useful if you want to copy your exclude dates from one Backup Exec server to another. You can also exclude dates from the backup schedule using the **Backup Calendar** option.

See [“Selecting dates to exclude from the backup schedule”](#) on page 459.

See [“Importing a list of dates to exclude from the backup schedule”](#) on page 459.

See [“Exporting excluded backup dates to another server”](#) on page 460.

See [“Deleting dates from the exclude dates list”](#) on page 460.

See [“Excluding dates from the schedule using the backup calendar”](#) on page 226.

## Selecting dates to exclude from the backup schedule

You can exclude specific dates, such as holidays, from your backup schedule.

See [“About excluding dates from the backup schedule”](#) on page 458.

### To select dates to exclude from the backup schedule

1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.

2 Select **Exclude Dates**.

See [“Exclude Dates options”](#) on page 461.

3 Do one of the following:

To manually enter the date

Type the date that you want to exclude from the backup schedule in the **Select Date** field.

To select the date from the calendar

- Click the calendar icon.
- Select the date that you want to exclude.

4 Click **Add**.

---

**Note:** You can add only one date at a time.

---

5 When you are finished selecting dates, click **OK**.

## Importing a list of dates to exclude from the backup schedule

You can exclude specific dates, such as holidays, from your backup schedule.

See [“About excluding dates from the backup schedule”](#) on page 458.

You can build a list of dates to exclude from the backup schedule in a .txt file. Then, you can import the .txt file into Backup Exec and add all the exclude dates

at once. The .txt file is formatted as a newline delimited list. You can configure dates in the local format or the coordinated universal time format.

#### To import a list of dates to exclude from the backup schedule

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select **Exclude Dates**.  
See “[Exclude Dates options](#)” on page 461.
- 3 Click **Browse**.
- 4 Select the .txt file that contains the exclude dates.
- 5 Click **Open**.
- 6 Click **Import**.
- 7 Click **OK**.

## Exporting excluded backup dates to another server

You can exclude specific dates, such as holidays, from your backup schedule. When you exclude dates, any regularly scheduled backups do not run on those dates. You can create a list of dates to exclude in Backup Exec.

See “[About excluding dates from the backup schedule](#)” on page 458.

You can import or export a list of dates to exclude as a .txt file. This may be useful if you want to copy a list of exclude dates from one Backup Exec server to another.

See “[Importing a list of dates to exclude from the backup schedule](#)” on page 459.

#### To export a list of exclude dates

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select **Exclude Dates**.  
See “[Exclude Dates options](#)” on page 461.
- 3 Click **Export**.
- 4 Browse to the location where you want to save the .txt file.
- 5 Click **Save**.

## Deleting dates from the exclude dates list

You can create a list of dates to exclude from your backup schedule. Backup Exec does not run any scheduled backup jobs on the dates that you select to exclude

from the backup schedule. If you later decide that you do not want to exclude a date from your backup schedule, you can delete the date from the list.

See [“About excluding dates from the backup schedule”](#) on page 458.

**To delete dates from the exclude dates list**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select **Exclude Dates**.  
 See [“Exclude Dates options”](#) on page 461.
- 3 Select the date or dates that you want to remove from the list.
- 4 Click **Delete**.

**Exclude Dates options**

You can exclude specific dates, such as holidays from your backup schedule.

See [“Selecting dates to exclude from the backup schedule”](#) on page 459.

See [“Importing a list of dates to exclude from the backup schedule”](#) on page 459.

See [“Exporting excluded backup dates to another server”](#) on page 460.

See [“Deleting dates from the exclude dates list”](#) on page 460.

**Table 17-2** Exclude Dates options

Item	Description
<b>File</b>	Displays the name of the .txt file to import into Backup Exec.
<b>Browse</b>	Lets you select a .txt file to import.
<b>Import</b>	Imports the dates from the .txt file you selected into Backup Exec.  The dates from the .txt file appear in the <b>Exclude Dates</b> field when they are successfully imported.
<b>Select Date</b>	Lets you select a date from a calendar.  You can select only one date at a time using the calendar.
<b>Add</b>	Adds the date you selected from the calendar to the list of dates to exclude from the backup schedule.
<b>Exclude Dates</b>	Lists the dates that Backup Exec excludes from your backup schedule.

**Table 17-2** Exclude Dates options (*continued*)

Item	Description
<b>Delete</b>	Lets you remove a date from the list of dates.
<b>Export</b>	Exports a .txt file that lists the dates you selected to exclude from your backup schedule.  You can import the .txt file on another Backup Exec server to quickly recreate the list of dates.

## Excluding selections from all backups

Backup Exec lets you select specific files or types of files to exclude from your backup jobs. You can specify exclusions when you create a backup job. Or you can specify global exclusions that apply to all the backup jobs that you create. If you want to override a global exclusion for a specific job, you can delete the excluded selections when you create the job.

See [“Setting default backup job settings”](#) on page 456.

### To exclude selections from backups globally

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select **Exclude Selections**.
- 3 Click **Insert**.
- 4 Complete the appropriate options.  
 See [“Exclude Files and Folders options”](#) on page 210.
- 5 Click **OK**.
- 6 Click **OK**.

## Global Exclude Selections options

You can select types of data or specific files to globally exclude from all backups.

See [“Excluding selections from all backups”](#) on page 462.

**Table 17-3** Global Exclude Selections options

Item	Description
<b>Globally excluded selections</b>	Lists the files that are globally excluded from all backups.

**Table 17-3** Global Exclude Selections options (*continued*)

Item	Description
<b>Insert</b>	Lets you add files to exclude from all backups. See <a href="#">“Exclude Files and Folders options”</a> on page 210.
<b>Modify</b>	Lets you edit the list of globally excluded selections. See <a href="#">“Exclude Files and Folders options”</a> on page 210.
<b>Delete</b>	Lets you delete files from the list of globally excluded selections.

## About global Backup Exec settings

You can configure global settings for the following things in Backup Exec.

**Table 17-4** Backup Exec settings

Item	Description
Preferences	Lets you configure settings for how you prefer Backup Exec to display various screens, indicators, and alerts. See <a href="#">“Changing the default preferences”</a> on page 465.
Job Status and Recovery	Lets you configure how Backup Exec responds when services become unresponsive. See <a href="#">“Setting job status and recovery options”</a> on page 277.
Job Logs	Lets you configure job log settings. You can configure what information is included in the log, the file name, e-mail settings, and the directory in which logs are saved. See <a href="#">“Configuring default job log options”</a> on page 268.
Catalog	Lets you configure catalog settings. See <a href="#">“Editing global options for catalogs”</a> on page 242.
Database Maintenance	Lets you configure how Backup Exec maintains its database. You can choose to allow Backup Exec to delete old data, save the database contents, and optimize the databases's size. See <a href="#">“Changing database maintenance options”</a> on page 467.

**Table 17-4** Backup Exec settings (*continued*)

Item	Description
Reports	<p>Lets you configure how reports are displayed in Backup Exec.</p> <p>See <a href="#">“Editing application settings for reports”</a> on page 586.</p>
Discover Data to Back Up	<p>Lets you configure how Backup Exec discovers data that has not been backed up.</p> <p>See <a href="#">“Configuring Backup Exec to discover data to back up”</a> on page 469.</p>
LiveUpdate	<p>Lets you configure how LiveUpdate checks for and applies updates to Backup Exec.</p> <p>See <a href="#">“Application settings for LiveUpdate”</a> on page 118.</p>
Network and Security	<p>Lets you configure network and security settings.</p> <p>You can select which network ports you want to use and whether you want to encrypt backups. You can also configure Backup Exec to work with Symantec's ThreatCon reporting system.</p> <p>See <a href="#">“Changing network and security options”</a> on page 470.</p>
Simplified Disaster Recovery	<p>Lets you configure disaster recovery settings.</p> <p>See <a href="#">“Changing the default path for the disaster recovery information files”</a> on page 712.</p>
Storage	<p>Lets you configure settings for tape, disk, and disk cartridge devices.</p> <p>See <a href="#">“Editing global settings for storage”</a> on page 415.</p>
Granular Recovery Technology	<p>Lets you configure Granular Recovery Technology (GRT) options.</p> <p>GRT lets you restore individual items from backup sets. To restore individual items, GRT must be enabled when you create a backup job.</p> <p>See <a href="#">“Setting default Granular Recovery Technology (GRT) options”</a> on page 482.</p>
Oracle	<p>Lets you configure settings for any Oracle servers.</p> <p>See <a href="#">“Oracle job settings options”</a> on page 899.</p>

**Table 17-4** Backup Exec settings (*continued*)

Item	Description
DBA-initiated Job Settings	Lets you configure settings for DBA-initiated jobs.  See <a href="#">“About configuring DBA-initiated job templates”</a> on page 483.

## Changing the default preferences

You can change the settings for how you prefer Backup Exec to display various screens, indicators, and alerts.

### To change the default preferences

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Preferences**.
- 3 Select the appropriate options.  
  
See [“Options for Backup Exec preferences”](#) on page 465.
- 4 Click **OK**.

## Options for Backup Exec preferences

You can change the settings for how you prefer Backup Exec to display various screens, indicators, and alerts.

See [“Changing the default preferences”](#) on page 465.

**Table 17-5** Options for Backup Exec preferences

Item	Description
<b>Show splash screen at startup</b>	Displays the splash screen when you start Backup Exec. If this option is cleared, the Backup Exec Administration Console is the first thing to display on startup.
<b>Automatically display new alerts</b>	Enables alerts to automatically appear in a pop-up window for 20 seconds at the bottom of the administration console. From the pop-up window, you can select the Details option, which allows you to view the details of the alert and to respond to the alert.

**Table 17-5** Options for Backup Exec preferences (*continued*)

Item	Description
<p><b>Display progress indicators for backup jobs. This requires additional time to pre-scan storage.</b></p>	<p>Displays the percentage complete number while a backup job processes. These indicators appear in the <b>Job Activity</b> dialog box, and they allow you to monitor the progress of the active job. Backups might take a little longer to complete when this option is selected because the backup sources must be scanned to determine the amount of data to be backed up.</p> <p>Due to the amount of time that is required to scan the backup sources, you should not select this option when you back up remote resources.</p>
<p><b>Allow Backup Exec to report anonymous usage information (No personally identifiable information will be returned to Symantec).</b></p>	<p>Enables you to participate in the Symantec Backup Exec product improvement program.</p> <p>General Backup Exec usage and statistical information is periodically collected and sent anonymously to Symantec. Symantec uses the information to help improve the Backup Exec customer experience.</p> <p><b>Note:</b> Although usage and statistical information is collected, Symantec never collects specific user information.</p>
<p><b>Send an alert on this date as a reminder to renew your maintenance contracts</b></p>	<p>Lets you select the date on which you want to receive a reminder to renew your maintenance contracts for Backup Exec features that are installed.</p> <p>Symantec recommends that you keep your maintenance contracts current for the Backup Exec products that are installed. Maintenance contracts ensure that you have access to the latest upgrades and to technical support. If your maintenance contracts expire, your entitlement to technical support also expires, and upgrades are no longer automatically sent.</p>
<p><b>Re-enable</b></p>	<p>Enables any messages that you have disabled.</p>

## About database maintenance

The Database Maintenance option lets you manage the Backup Exec database. Each database maintenance operation is performed independently on each database. The Backup Exec database maintains a record of the files and data that you have configured.

Database maintenance lets you perform the following:

- Optimize database size.
- Delete expired data.
- Save the contents of the database files.
- Perform a database consistency check.

Backup Exec generates informational alerts at the beginning and at the end of the database maintenance process each time database maintenance is performed. The alerts provide details about the type of maintenance that was performed on each database and the amount of time that the maintenance took to complete. If the database maintenance process fails, the alert indicates where the failure occurred and the reason for the failure.

See [“Changing database maintenance options”](#) on page 467.

## Changing database maintenance options

The Database Maintenance option lets you manage the Backup Exec database. Each database maintenance operation is performed independently on each database. The Backup Exec database maintains a record of files and data you have configured such as templates and catalogs.

You do not have to select all the options; however, each one performs a different process that enables you to protect and maintain your database. Selecting all the options enables you to recover the database quickly and maintain optimal performance.

See [“About database maintenance”](#) on page 466.

### To configure database maintenance

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Database Maintenance**.
- 3 Select the appropriate options.

See [“Database maintenance options”](#) on page 467.

- 4 Click **OK**.

## Database maintenance options

You can manage the Backup Exec Database to optimize space and performance.

See [“Changing database maintenance options”](#) on page 467.

**Table 17-6** Database Maintenance options

Item	Description
<b>Enable Backup Exec database maintenance</b>	Activates the database maintenance process.
<b>Last time maintenance was performed</b>	Indicates the date and time the last database maintenance was performed.
<b>Perform database maintenance daily at</b>	Indicates the time you want to perform database maintenance.  All the maintenance will occur once a day at the time you specify.
<b>Delete aged data</b>	Activates the deletion of expired job history, job logs, alert history, and reports from the Backup Exec Database after the specified number of days have passed.
<b>Keep job history for data on media that have current overwrite protection periods</b>	Keeps all job history data for any media to which an overwrite protection period is currently assigned.  After a media's overwrite protection period expires, the media's job history data can be deleted.
<b>Keep job history for specified number of days</b>	Indicates the number of days to keep job history data in the database before it is deleted.  Job history data includes summary statistics for a job and details about media, devices, and backup sets that were used to process the job.
<b>Job logs</b>	Indicates the number of days to keep job logs in the database before they are deleted.  Job logs include detailed information about the job.
<b>Alert history</b>	Indicates the number of days to keep alert history data in the database before it is deleted.  Alert history data includes property and response information for the alert.
<b>Reports</b>	Indicates the number of days to keep report data in the database before it is deleted.  Report data includes property information about report jobs that were generated. The report itself is not deleted.

**Table 17-6** Database Maintenance options (*continued*)

Item	Description
<b>Audit logs</b>	<p>Indicates the number of days to keep audit log data in the database before it is deleted.</p> <p>The audit log includes information about operations that are performed in Backup Exec.</p> <p>See <a href="#">“About audit logs”</a> on page 516.</p>
<b>Perform database consistency check</b>	<p>Checks the logical and physical consistency of the data in the database.</p> <p>The option is not checked by default. It is recommended that you run a consistency check periodically at a time when there is minimal activity from Backup Exec.</p>
<b>Save contents of database to the Backup Exec data directory</b>	<p>Places the data that is contained in the database into the Backup Exec data directory so that the database backup file (BEDB.bak) can be backed up.</p> <p>The dump file will be maintained in the data directory until the next database maintenance process is performed and then this file will be overwritten. Selecting this option enables you to recover the database in the event of failure.</p>
<b>Optimize database size</b>	<p>Reorganizes fragmented pages and decrease the size of the physical database to 10 percent above what is actually used.</p>

## Configuring Backup Exec to discover data to back up

Backup Exec’s **Discover Data to Back Up** option detects new backup content within a Windows or Active Directory domain. This option lets you configure a job that searches for new server volumes, databases, or application data.

See [“About discovering data to back up”](#) on page 537.

### To configure Backup Exec to discover data to back up

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Discover Data to Back Up**.
- 3 Select the appropriate options.  
 See [“Discover Data to Back Up options”](#) on page 470.
- 4 Click **OK**.

## Discover Data to Back Up options

You can configure Backup Exec to discover data that needs to be backed up.

See “[Configuring Backup Exec to discover data to back up](#)” on page 469.

**Table 17-7** Discover Data to Back Up options

Item	Description
<b>Discover servers that have data that has not been backed up</b>	Enables Backup Exec to discover data that needs to be backed up.  When this option is selected, Backup Exec automatically checks your network for data that has not been backed up.
<b>Frequency</b>	Determines the frequency with which Backup Exec searches for data that needs to be backed up.  You can select to let Backup Exec search for data that needs to be backed up daily, weekly, or monthly.
<b>Interval</b>	Determines the interval at which Backup Exec searches for data that needs to be backed up.  You can select different intervals based on the frequency you selected.
<b>Cancel data discovery if not completed within</b>	Determines the number of hours after which the data discovery process is cancelled if it is not finished.  Canceling the data discovery process can help prevent it from impacting your system resources.

## Changing network and security options

You can configure how Backup Exec works with your network configuration and security. The network and security options are global options that affect all Backup Exec jobs.

### To edit network and security options

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Network and Security**.
- 3 Select the appropriate options.  
See “[Network and security options](#)” on page 471.
- 4 Click **OK**.

## Network and security options

You can configure global network and security options for Backup Exec.

See “[Changing network and security options](#)” on page 470.

**Table 17-8** Network and security options

Item	Description
<b>Network interface</b>	Specifies the name of the network interface card that connects the Backup Exec server to the default network that you want to use for backup jobs. The list includes all available network interfaces on the Backup Exec server.
<b>Protocol</b>	<p>Specifies the default protocol you want to use for backup jobs.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> <li>■ Use any available protocol</li> <li>■ IPv4</li> <li>■ IPv6</li> </ul>
<b>Subnet</b>	Displays the 32-bit number that determines the subnet to which the network interface card belongs.
<b>Allow use of any available network interface, subnet, or protocol for Backup Exec agents not bound to the above network interface, subnet, or protocol</b>	<p>Lets Backup Exec use any available network if the remote system that you selected for backup or restore is not part of the specified backup network.</p> <p>If you do not select this option and the remote system is not part of the specified backup network, the job fails. Backup Exec cannot access the data from the remote system.</p>
<b>Interface Details</b>	Displays the Media Access Control (MAC) address, adapter type, description, IP addresses, and subnet prefixes for the interface that you selected for the backup network.
<b>Enable selection of user shares</b>	<p>Lets you include user-defined shares in jobs.</p> <p>If you do not select this option, you cannot select user-defined shares when you create jobs.</p>

**Table 17-8** Network and security options (*continued*)

Item	Description
<b>Enable remote agent TCP dynamic port ranges</b>	<p>Lets Backup Exec agents use a range of ports for communication.</p> <p>You enter the port range. If the first port that Backup Exec attempts to use is not available, Backup Exec attempts to use one of the other ports in the range. If none of the ports in the range is available, Backup Exec uses any available dynamic port. Default port ranges are 1025 to 65535. Symantec recommends using a range of 25 allocated ports for the remote system if you use Backup Exec with a firewall.</p> <p>See <a href="#">“About using Backup Exec with firewalls”</a> on page 472.</p>
<b>Use a custom port to receive operation requests from the Oracle server</b>	<p>Specifies the port that Backup Exec uses for communication between the Backup Exec server and the remote computer for both DBA and Backup Exec server-initiated operations. By default, Backup Exec uses port 5633.</p> <p>If you change the port number on the remote Windows or Linux computer, you must also change it on the Backup Exec server. Then you must restart the Backup Exec Job Engine service on the Backup Exec server.</p> <p>See <a href="#">“About Oracle instance information changes ”</a> on page 900.</p>
<b>Use FIPS 140-2 compliant software encryption</b>	<p>Enables software encryption that complies with FIPS 140-2 standards. If you select this option, you must use a 256-bit AES encryption key. This option is available only for Windows computers.</p> <p>You must stop and restart the Backup Exec services for this change to take effect.</p>
<b>Manage Keys</b>	<p>Lets you create a new encryption key or manage existing encryption keys.</p>

## About using Backup Exec with firewalls

In firewall environments, Backup Exec provides the following advantages:

- The number of ports that are used for backup network connections is kept to a minimum.
- Open ports on the Backup Exec server and remote systems are dynamic and offer high levels of flexibility during browsing, backup, and restore operations.

- You can set specific firewall port ranges and specify backup and restore networks within these ranges. You can use specific ranges to isolate data traffic and provide high levels of reliability.

---

**Note:** The Agent for Windows is required to perform remote backups and restores.

---

Firewalls affect system communication between a Backup Exec server and any remote systems that reside outside the firewall environment. You should consider special port requirements for your firewall when you configure Backup Exec.

Symantec recommends that you open port 10000 and make sure that it is available on the Backup Exec server and any remote systems. In addition, you must open the dynamic port ranges that Backup Exec uses for communications between the Backup Exec server and Backup Exec agents.

See “[Backup Exec Ports](#)” on page 475.

When a Backup Exec server connects to a remote system, it initially uses port 10000. The agent listens for connections on this predefined port. The Backup Exec server is bound to an available port, but additional connections to the agent are initiated on any available port.

When you back up data, up to two ports may be required on the computer on which the agent is installed. To support simultaneous jobs, you must configure your firewall to allow a range of ports large enough to support the number of simultaneous operations desired.

If there is a conflict, you can change the default port to an alternate port number by modifying the `%systemroot%\System32\drivers\etc\services` file. You can use a text editor such as Notepad to modify your NDMP entry or add an NDMP entry with a new port number. You should format the entry as follows:

```
ndmp      100000/tcp      #Network Data Management Protocol
```

---

**Note:** If you change the default port, you must change it on the Backup Exec server and all remote systems that are backed up through the firewall.

---

When you set up TCP dynamic port ranges, Symantec recommends that you use a range of 25 allocated ports for the remote computer. The number of ports that remote computers require depends on the number of devices you protect and the number of tape devices you use. You may need to increase these port ranges to maintain the highest level of performance.

Unless you specify a range, Backup Exec uses the full range of dynamic ports available. When performing remote backups through a firewall, you should select a specific range on the **Network and Security** settings dialog.

See [“Changing network and security options”](#) on page 470.

See [“Backup Exec Listening Ports”](#) on page 476.

## Browsing systems through a firewall

Because most firewalls do not allow a remote system to be displayed in the Microsoft Windows Network tree, you may need to take additional steps to select these remote systems in Backup Exec.

See [“About using Backup Exec with firewalls”](#) on page 472.

### To browse systems through a firewall

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, select **Network and Security**.
- 3 Verify that a dynamic range of ports has been set for the Backup Exec server and the Backup Exec agent and that the firewall is configured to pass these port ranges and the 10,000 port (which is used for the initial connection from the Backup Exec server to the Backup Exec agent).  
  
Port 6101 must be open to browse Windows systems in the backup selections tree.
- 4 Click **OK**.

## About enabling a SQL instance behind a firewall

If you want to connect to a SQL instance behind a firewall, you must enable the SQL instance for communication. To enable the SQL instance for communication, you must make the SQL port static and configure the Windows Firewall.

The Backup Exec SQL instance is configured to use a dynamic port by default. Each time SQL Server is started, the port number can change.

See [“Changing the dynamic port on the SQL Express instance in CASO to a static port”](#) on page 1008.

See [“Opening a SQL port in CASO for a SQL 2005 or 2008 instance”](#) on page 1010.

You also must configure the Windows Firewall to allow connections to the SQL instance. There may be multiple ways to configure the Windows Firewall based on your system configuration. You can add sqlsvr.exe and sqlbrowser.exe to the Windows Firewall Exceptions list or you can open a port in the Windows Firewall for TCP access. Refer to the Microsoft Knowledge Base for more information or to determine which configuration is best for your network.

## Backup Exec Ports

You may have special port requirements for Backup Exec if you use a firewall. Firewalls sometimes affect system communications between a Backup Exec server and remote systems that reside outside the firewall environment.

See [“About using Backup Exec with firewalls”](#) on page 472.

The following table provides more information about which ports Backup Exec and its agents and options use:

**Table 17-9** Backup Exec Ports

Service or Process	Port	Port Type
Backup Exec Agent Browser (process=benetns.exe)	6101	TCP
Backup Exec Agent for Windows (process=beremote.exe)	10000	TCP
Backup Exec server (process=beserver.exe)	3527, 6106	TCP
MSSQL\$BKUPEXEC (process=sqlservr.exe)	1125 1434 (ms-sql-m)	TCP UDP
Agent for Oracle on Windows or Linux Servers	Random port unless configured otherwise	
Agent for Linux	Default NDMP port, typically 10000	TCP
Backup Exec deduplication engine (process=spoold.exe)	10082	TCP
Backup Exec deduplication manager (process=spad.exe)	10102	TCP
Kerberos	88	UDP
NETBIOS	135	TCP, UDP
NETBIOS Name Service	137	UDP
NETBIOS Datagram Service	138	UDP
NETBIOS Session Service	139	TCP
NETBIOS	445	TCP

**Table 17-9** Backup Exec Ports (*continued*)

Service or Process	Port	Port Type
DCOM/RPC	3106	TCP
Agent for Windows	6103	TCP
Push Install - Check for conflicts in message queue for CASO which is part of beserver.exe	103x	TCP
Push Install	441	TCP
SMTP email notification	25 outbound from Backup Exec server	TCP
SNMP	162 outbound from Backup Exec server	TCP

## Backup Exec Listening Ports

You may have special port requirements for Backup Exec if you use a firewall. Firewalls sometimes affect system communications between a Backup Exec server and remote systems that reside outside the firewall environment.

See [“About using Backup Exec with firewalls”](#) on page 472.

When Backup Exec is not running operations, it listens to ports for incoming communication from other services and agents. Backup Exec initially communicates with the agent using a static listening port to begin an operation. The agent and the Backup Exec server then use dynamic ports to pass data back and forth.

Backup Exec uses the following listening ports:

**Table 17-10** Backup Exec Listening Ports

Service	Port	Port Type
Backup Exec Agent Browser (benetns.exe)	6101	TCP
Backup Exec Agent for Windows (beremote.exe)	10000	TCP
Backup Exec server (beserver.exe)	3527, 6106	TCP

**Table 17-10** Backup Exec Listening Ports (*continued*)

Service	Port	Port Type
MSSQL\$BKUPEXEC (sqlsevr.exe)	1125 1434	TCP UDP
Agent for Linux (RALUS)	10000	TCP
DBA-initiated backups for Oracle	5633	TCP

## About encryption key management

When a user creates an encryption key, Backup Exec marks that key with an identifier based on the logged-on user's security identifier. The person who creates the key becomes the owner of the key.

Backup Exec stores the keys in the Backup Exec database. However, Backup Exec does not store the pass phrases for the keys. The owner of each key is responsible for remembering the pass phrase for the key.

To protect your keys, Symantec recommends the following:

- Maintain a written log of the pass phrases. Keep the log in a safe place in a separate physical location from the encrypted backup sets.
- Back up the Backup Exec database. The database keeps a record of the keys.

---

**Caution:** If you do not have a backup of the Backup Exec database and do not remember your pass phrases, you cannot restore data from the encrypted media. In addition, Symantec cannot restore encrypted data in this situation.

---

A key that is created on a Backup Exec server is specific to that Backup Exec server. You cannot move keys between Backup Exec servers. However, you can create new keys on a different Backup Exec server by using existing pass phrases. A pass phrase always generates the same key. In addition, if you delete a key accidentally, you can recreate it by using the pass phrase.

If a Backup Exec database becomes corrupted on a Backup Exec server and is replaced by a new database, you must manually recreate all of the encryption keys that were stored on the original database.

If you move a database from one Backup Exec server to another Backup Exec server, the encryption keys remain intact as long as the new Backup Exec server meets the following criteria:

- Has the same user accounts as the original Backup Exec server.

- Is in the same domain as the original Backup Exec server.

See “[About pass phrases in encryption](#)” on page 553.

See “[About deleting an encryption key](#)” on page 481.

## Encryption Key Management options

From the **Encryption Key Management** dialog box, you can perform several encryption key management tasks.

See “[Creating an encryption key](#)” on page 478.

See “[Replacing an encryption key](#)” on page 480.

See “[Deleting an encryption key](#)” on page 481.

Table 17-11 Encryption Key Management options

Item	Description
<b>Key name</b>	Indicates the name of the encryption key.
<b>Created By</b>	Indicates who created the encryption key. When a user creates an encryption key, Backup Exec marks that key with an identifier based on the logged-on user’s security identifier. The person who creates the key becomes the owner of the key.
<b>Restricted</b>	Indicates if the key is a restricted key. If a key is restricted, anyone can use the key to back up data. But only the key owner or a user who knows the pass phrase can use the restricted key to restore the encrypted data.
<b>Encryption Type</b>	Indicates the type of encryption that is associated with the encryption key.
<b>Date Created</b>	Indicates the date the encryption key was created.
<b>Date Last Accessed</b>	Indicates the date the encryption key was last accessed.
<b>New</b>	Lets you create a new encryption key.
<b>Delete</b>	Deletes the selected encryption key.
<b>Replace</b>	Replaces the selected encryption key with the key you select from the <b>Replace Encryption Key</b> dialog.

## Creating an encryption key

When you create an encryption key, you select the type of encryption to use.

See [“About encryption key management”](#) on page 477.

**To create an encryption key**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Network and Security**.
- 3 Click **Manage Keys**.
- 4 Click **New**.
- 5 Complete the appropriate options.  
 See [“Add Encryption Key options”](#) on page 479.
- 6 Click **OK**.

**Add Encryption Key options**

You have several options when you create an encryption key.

See [“Creating an encryption key”](#) on page 478.

**Table 17-12 Add Encryption Key options**

Item	Description
<b>Key name</b>	Designates a unique name for this key. The name can include up to 256 characters.
<b>Encryption type</b>	Designates the encryption type to use for this key. Your choices are 128-bit AES or 256-bit AES. The default type is 256-bit AES.  The 256-bit AES encryption provides a stronger level of security than 128-bit AES encryption. However, backup jobs may process more slowly with 256-bit AES encryption than with 128-bit AES encryption.  Hardware encryption that uses the T10 standard requires 256-bit AES.
<b>Pass phrase</b>	Designates a pass phrase for this key. For 128-bit AES encryption, the pass phrase must be at least eight characters. For 256-bit AES encryption, the pass phrase must be at least 16 characters. Symantec recommends that you use more than the minimum number of characters.  You can use only printable ASCII characters.  See <a href="#">“About pass phrases in encryption”</a> on page 553.

**Table 17-12** Add Encryption Key options (*continued*)

Item	Description
<b>Confirm pass phrase</b>	Confirms the pass phrase.
<b>Common</b>	Makes this key a common key. If a key is common, any user of this installation of Backup Exec can use the key to back up and restore data.
<b>Restricted</b>	Makes the key a restricted key. If a key is restricted, anyone can use the key to back up data. But only the key owner or a user who knows the pass phrase can use the restricted key to restore the encrypted data.

## Replacing an encryption key

You can replace one encryption key with another for all backup jobs and duplicate backup set jobs.

See [“About encryption key management”](#) on page 477.

### To replace a default encryption key

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Network and Security**.
- 3 Click **Manage Keys**.
- 4 Select the key that you want to replace.
- 5 Click **Replace**.
- 6 In the **Select an encryption key to replace <key name>** field, do one of the following:

To use an existing key    Select the key from the list.

To create a new key    Click **New** and complete the options on the Add Encryption Key dialog box.

See [“Add Encryption Key options”](#) on page 479.

- 7 Click **OK**.

## About deleting an encryption key

You should be cautious when you delete encryption keys. When you delete an encryption key, you cannot restore the backup sets that you encrypted with that key unless you create a new key that uses the same encryption key and pass phrase as the original key.

See [“Deleting an encryption key”](#) on page 481.

You can delete encryption keys in the following situations:

- The encrypted data on the tape has expired or if the tape is retired.
- The encryption key is not the default key.
- The encryption key is not being used in a job. If the key is being used, you must select a new key for the job.

If you delete an encryption key that is being used in a scheduled restore job, you cannot replace the key. Therefore, any scheduled restore job in which you delete an encryption key fails.

See [“About encryption key management”](#) on page 477.

See [“Replacing an encryption key”](#) on page 480.

## Deleting an encryption key

You should be cautious when you delete encryption keys. When you delete an encryption key, you cannot restore the backup sets that you encrypted with that key unless you create a new key that uses the same encryption key and pass phrase as the original key.

See [“About deleting an encryption key”](#) on page 481.

### To delete an encryption key

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Network and Security**.
- 3 Click **Manage Keys**.
- 4 Select the key that you want to delete.
- 5 Click **Delete**.
- 6 Click **Yes**.
- 7 If the key is used in a job, do the following:
  - In the **Select an encryption key to replace "key name"** box, select the new key for the job or click **New** to create a new key.

- Click **OK**.

## Setting default Granular Recovery Technology (GRT) options

You can configure default settings for Granular Recovery Technology.

See [“About job defaults”](#) on page 456.

### To set default Granular Recovery Technology options

- 1 Click the Backup Exec button, and then select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **Granular Recovery Technology**.
- 3 Select the appropriate options.

See [“Granular Recovery Technology Job Settings”](#) on page 482.

- 4 Click **OK**.

## Granular Recovery Technology Job Settings

You can configure default settings for Granular Recovery Technology (GRT).

See [“Setting default Granular Recovery Technology \(GRT\) options”](#) on page 482.

**Table 17-13** Granular Recovery Technology Job Settings options

Item	Description
<b>If Granular Recovery Technology (GRT) is enabled for backup, enter the path to an NTFS volume of the local Backup Exec server where Backup Exec can stage temporary data</b>	<p>Designates a location where Backup Exec can stage temporary data during GRT-enabled backup jobs.</p> <p>Ensure that the location is an NTFS volume and that it is not a system volume. If the default path of C:\TEMP does not meet these requirements, type a different path on the Backup Exec server where Backup Exec can stage temporary data.</p> <p>Backup Exec deletes the data when the backup job is completed.</p> <p>At least 1 GB of disk space is required.</p>

**Table 17-13** Granular Recovery Technology Job Settings options (*continued*)

Item	Description
<p><b>Enter the path to an NTFS volume of the local Backup Exec server where Backup Exec can store temporary data (Microsoft Hyper-V, Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory, and VMware restore jobs only)</b></p>	<p>Designates a location where Backup Exec can stage temporary data during GRT restore jobs.</p> <p>This option is applicable only when you restore individual items under the following conditions:</p> <ul style="list-style-type: none"> <li>■ The backup of Microsoft Hyper-V, Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory, or VMware Virtual Infrastructure was enabled for Backup Exec Granular Recovery Technology (GRT).</li> <li>■ The backup is on a tape.</li> <li>■ The backup is on disk storage on a volume that has size limitations. FAT and FAT32 are examples of types of volumes that have file size limitations.</li> </ul> <p>Type the path to a folder on an NTFS volume on this Backup Exec server. Restore data and metadata for this job are stored here temporarily before the individual items are restored. The staged data is automatically deleted when the restore job is completed.</p> <p>Symantec recommends that you avoid using system volumes for temporary staging locations.</p>

## About configuring DBA-initiated job templates

When you create a DBA-initiated backup operation, you can specify the default job template in Backup Exec. You can also specify a new job template that you create in Backup Exec. The job template contains the settings that Backup Exec applies to DBA-initiated jobs.

Make sure that the name of the job template that you want to use is also configured in the instance information on the Windows computer.

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

Note the following about DBA-initiated jobs:

- DBA-initiated jobs fail when the related job template is deleted. To stop DBA-initiated jobs from running, delete the related DBA-initiated job template. See [“Deleting a job template for DBA-initiated jobs”](#) on page 485.
- All DBA-initiated backup and restore jobs are deleted after the jobs have completed.
- You cannot set minimum device requirements for DBA-initiated jobs.

See [“About performing a DBA-initiated backup job for Oracle”](#) on page 902.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Editing DBA-initiated job templates”](#) on page 485.

## About DBA-initiated job settings

You can configure settings for DBA-initiated job templates.

See [“About configuring DBA-initiated job templates”](#) on page 483.

**Table 17-14** DBA-initiated job settings

Setting	Description
<b>Storage</b>	<p>Lets you specify the storage device that you want to use for the DBA-initiated job template.</p> <p>You can also configure compression, encryption, and data lifecycle management settings for storage.</p> <p>See <a href="#">“Storage options for DBA-initiated jobs”</a> on page 486.</p>
<b>General</b>	<p>Lets you specify general settings for the DBA-initiated job template.</p> <p>You can name the job and create a description for its backup sets. You can also enable a verify operation for the job.</p> <p>See <a href="#">“General options for DBA-initiated jobs”</a> on page 493.</p>
<b>Network</b>	<p>Lets you specify the network interface that Backup Exec uses to access remote computers.</p> <p>See <a href="#">“Network options for DBA-initiated jobs”</a> on page 493.</p>
<b>Migrator for Enterprise Vault</b>	<p>Lets you configure credentials for Migrator for Enterprise Vault, if necessary.</p> <p>See <a href="#">“Migrator for Enterprise Vault options”</a> on page 952.</p>
<b>Notification</b>	<p>Lets you configure Backup Exec to notify specified recipients when the backup job is completed.</p> <p>Backup Exec can notify people by email or text message.</p> <p>See <a href="#">“Notification options for jobs”</a> on page 299.</p>
<b>Duplicate Job Settings</b>	<p>Lets you configure options for duplicate jobs, which create a second set of backup sets for the job.</p> <p>See <a href="#">“Duplicate job settings for DBA-initiated jobs”</a> on page 494.</p>

## Creating a template for DBA-initiated jobs

You can create a new job template that Backup Exec applies to DBA-initiated jobs.

See [“About configuring DBA-initiated job templates”](#) on page 483.

See [“Troubleshooting the Oracle Agent”](#) on page 910.

See [“Deleting a job template for DBA-initiated jobs”](#) on page 485.

### To create a template for DBA-initiated jobs

- 1 Click the Backup Exec button, and then select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **DBA-initiated Job Settings**.
- 3 Click **New**.
- 4 Select the appropriate options.  
See [“About DBA-initiated job settings”](#) on page 484.
- 5 Click **OK**.

## Editing DBA-initiated job templates

You can edit the job template settings that Backup Exec applies to DBA-initiated jobs.

See [“About configuring DBA-initiated job templates”](#) on page 483.

### To edit DBA-initiated job templates for Oracle

- 1 Click the Backup Exec button, and then select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **DBA-initiated Job Settings**.
- 3 Select the job template that you want to edit.
- 4 Click **Edit**.
- 5 Edit the appropriate options.  
See [“About DBA-initiated job settings”](#) on page 484.
- 6 Click **OK**.

## Deleting a job template for DBA-initiated jobs

The job template contains the settings that Backup Exec applies to DBA-initiated jobs.

See [“About configuring DBA-initiated job templates”](#) on page 483.

### To delete a job template for DBA-initiated jobs for Oracle

- 1 Click the Backup Exec button, and then select **Configuration and Settings**, and then click **Backup Exec Settings**.
- 2 In the left pane, select **DBA-initiated Job Settings**.
- 3 Select the job template that you want to delete.
- 4 Click **Delete**.
- 5 Click **Yes**.

### Storage options for DBA-initiated jobs

You can configure storage settings for DBA-initiated jobs.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Editing DBA-initiated job templates”](#) on page 485.

**Table 17-15** Storage options for DBA-initiated jobs

Item	Description
<b>Backup Exec server or Backup Exec server pool</b>	Specifies if you want a job to run on devices on a specific managed Backup Exec server or on devices that are on a group of managed Backup Exec servers.  This option displays only if you have the Central Admin Server Option installed. This option is an additional filter that lets you control where certain jobs are delegated. For example, to always run backups of Exchange databases only on the devices that are attached to managed Backup Exec servers in a pool named Exchange Backups, select this option. Then select the Exchange Backups Backup Exec server pool.

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<b>Storage</b>	<p>Specifies the storage device to which you want to send backup data for the DBA-initiated jobs.</p> <p>See <a href="#">“About storage device pools”</a> on page 403.</p> <p>See <a href="#">“About the Any Virtual Disk Storage device pool in the Storage Provisioning Option”</a> on page 1171.</p> <p>See <a href="#">“About the Remote Media Agent for Linux”</a> on page 1132.</p> <p>See <a href="#">“About disk-based storage”</a> on page 305.</p>
<b>Enable the remote computer to directly access the storage device and to perform client-side deduplication, if it is supported</b>	<p>Enables a remote computer to send data directly to an OpenStorage device or a deduplication disk storage device, and to perform client-side deduplication if the device supports it. The Backup Exec server is bypassed, which leaves the Backup Exec server free to perform other operations. If client-side deduplication cannot be performed, then either Backup Exec server deduplication or Appliance deduplication is performed.</p> <p>This option appears if the Deduplication Option is installed and an OpenStorage device or a deduplication disk storage device is selected in the <b>Storage</b> field.</p> <p>See <a href="#">“About client-side deduplication”</a> on page 773.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<p><b>Enable the remote computer to access the storage device through the Backup Exec server and to perform Backup Exec server-side deduplication, if it is supported</b></p>	<p>Enables a remote computer to send data through the Backup Exec server to an OpenStorage device or a deduplication disk storage device, and to perform Backup Exec server-side deduplication if it is supported. If the Backup Exec server does not support deduplication, the data is deduplicated on an intelligent disk device, such as Symantec PureDisk or a device from a third-party vendor.</p> <p>This option appears if the Deduplication Option is installed and an OpenStorage device or a deduplication disk storage device is selected in the <b>Storage</b> field.</p> <p>See <a href="#">“About the Deduplication Option”</a> on page 752.</p>
<p><b>Keep for</b></p>	<p>Designates the amount of time for which you want to keep the backup sets or job history from the DBA-initiated jobs.</p>
<p><b>Media set</b></p>	<p>Indicates the media set to use for the DBA-initiated jobs. The media set specifies the overwrite protection period and the append period for the backup data on the media.</p> <p>If you want to create a new media set for this backup job, click the icon to the right of the media set drop-down menu.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“About media sets”</a> on page 366.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<b>Overwrite media</b>	<p>Indicates that the backup job is placed on an overwritable media. Ensure that appropriate media is in the storage device that you select.</p> <p>Appropriate media for an overwrite job includes the following:</p> <ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Media for which the overwrite protection period has expired</li> </ul> <p>Allocated or imported media may also be overwritten depending on the media overwrite protection level that is set.</p> <p>Depending on your configuration, overwritable media is selected from scratch media or recyclable media.</p> <p>If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“About tape and disk cartridge media”</a> on page 365.</p> <p>See <a href="#">“About media overwrite protection levels for tape and disk cartridge media”</a> on page 377.</p> <p>See <a href="#">“How Backup Exec searches for overwritable media in tape drives and disk cartridges”</a> on page 378.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<p><b>Append to media, overwrite if no appendable media is available</b></p>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec searches for an overwritable media and adds it to the media set.</p> <p>If an append job fills a media, the backup job continues on an overwritable media. If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p>
<p><b>Append to media, terminate job if no appendable media is available</b></p>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec terminates the job.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p>
<p><b>Eject media after job completes</b></p>	<p>Ejects the media from the drive or slot when the operation completes. You can also schedule a job to eject media.</p> <p>This option is available only if you selected a tape device in the <b>Storage</b> field.</p> <p>See <a href="#">“Ejecting media from a disk cartridge or tape drive”</a> on page 428.</p>
<p><b>Retension media before backup</b></p>	<p>Runs the tape in the drive from beginning to end at a fast speed. Retensioning helps the tape wind evenly and run more smoothly past the tape drive heads. This option is available only if you select a tape drive that supports retensioning.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<b>Use Write once, read many (WORM) media</b>	<p>Specifies the use of WORM (write once, read many) media as the default for DBA-initiated jobs. Backup Exec confirms that the destination device is or contains a WORM-compatible drive, and that the WORM media is available in the drive. If WORM media or a WORM-compatible drive is not found, an alert is sent.</p> <p>See <a href="#">“About WORM media”</a> on page 383.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<b>Compression</b>	<p>Provides the following compression options:</p> <ul style="list-style-type: none"> <li> <p>■ <b>None</b></p> <p>Copies the data to the media in its original form (uncompressed). Using some form of data compression can help expedite backups and preserve storage space. Hardware data compression should not be used in environments where storage devices that support hardware compression are used interchangeably with devices that do not have that functionality. In this situation, hardware compression is automatically disabled. You can manually turn on hardware compression on the drives that support it, but this results in media inconsistency. If the drive that supports hardware compression fails, the compressed media cannot be restored with the non-compression drive.</p> </li> <li> <p>■ <b>Software</b></p> <p>Uses STAC software data compression, which compresses the data before it is sent to the storage device.</p> </li> <li> <p>■ <b>Hardware (if available, otherwise none)</b></p> <p>Uses hardware data compression if the storage device supports it. If the drive does not feature data compression, the data is backed up uncompressed.</p> </li> <li> <p>■ <b>Hardware (if available, otherwise software)</b></p> <p>Uses hardware data compression if the storage device supports it. If the drive does not feature hardware data compression, STAC software compression is used.</p> </li> </ul>
<b>Encryption type</b>	<p>Specifies the type of encryption that you want to use, if any.</p> <p>See <a href="#">“About encryption”</a> on page 551.</p>

**Table 17-15** Storage options for DBA-initiated jobs (*continued*)

Item	Description
<b>Encryption key</b>	Specifies the encryption key that you want to use, if you selected to use encryption.  See <a href="#">“Encryption keys”</a> on page 552.
<b>Manage Keys</b>	Lets you manage your encryption keys.  You can delete or replace existing encryption keys. You can also create a new encryption key.  This option is available only if you select an encryption type.  See <a href="#">“About encryption key management”</a> on page 477.

## General options for DBA-initiated jobs

You can configure general options for DBA-initiated jobs.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Editing DBA-initiated job templates”](#) on page 485.

**Table 17-16** General options for DBA-initiated jobs

Item	Description
<b>Job name</b>	Specifies the name for this backup template. You can accept the default name that appears or enter a name. The name must be unique.
<b>Backup set description</b>	Describes the information in the backup set for future reference.
<b>Verify after backup completes</b>	Performs a verify operation automatically to make sure that the media can be read once the backup has been completed. Verifying all backups is recommended.

## Network options for DBA-initiated jobs

You can configure network options for DBA-initiated jobs.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Editing DBA-initiated job templates”](#) on page 485.

**Note:** Some of these options may not display in a CASO environment.

**Table 17-17** Network options for DBA-initiated jobs

Item	Description
<b>Network interface</b>	Specifies the name of the network interface card that connects the Backup Exec server to the network that you want to use for this backup job. The list includes all available network interfaces on the Backup Exec server.
<b>Protocol</b>	<p>Specifies the protocol you want to use for this backup job. The options are as follows:</p> <ul style="list-style-type: none"> <li>■ Use any available protocol</li> <li>■ Use IPv4</li> <li>■ Use IPv6</li> </ul>
<b>Subnet</b>	Displays the 32-bit number that determines the subnet to which the network interface card belongs.
<b>Allow use of any available network interface, subnet, or protocol for Backup Exec agents not bound to the above network interface, subnet, or protocol</b>	<p>Lets Backup Exec use any available network if the remote system that you selected for backup or restore is not part of the specified backup network.</p> <p>If you do not select this option and the remote system is not part of the specified backup network, the job fails. Backup Exec cannot access the data from the remote system.</p>
<b>Interface Details</b>	Displays the Media Access Control (MAC) address, adapter type, description, IP addresses, and subnet prefixes for the interface that you selected for the backup network.
<b>Allow managed Backup Exec server to use any network interface to access Backup Exec agents</b>	<p>Lets a job use any network interface to access Backup Exec agents if the selected network interface is unavailable. Enabling this option lets the managed Backup Exec server use an alternate network interface to run any important backup jobs that would otherwise fail.</p> <p>This option is available only if the Central Admin Server Option (CASO) is installed.</p> <p>See <a href="#">“About the Central Admin Server Option”</a> on page 996.</p>

## Duplicate job settings for DBA-initiated jobs

You can configure duplicate job template settings for DBA-initiated jobs.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Editing DBA-initiated job templates”](#) on page 485.

**Table 17-18** Duplicate job settings for DBA-initiated jobs

Item	Description
<b>Enable settings to duplicate backup sets for this job</b>	Enables the settings for a duplicate backup set template.
<b>Storage</b>	Specifies the storage device to which you want to send backup data for the duplicate DBA-initiated job.
<b>Keep for</b>	Designates the amount of time for which you want to keep the backup sets or job history from the duplicate DBA-initiated job.
<b>Media set</b>	<p>Indicates the media set to use for the duplicate DBA-initiated job. The media set specifies the overwrite protection period and the append period for the backup data on the media.</p> <p>If you want to create a new media set for this backup job, click the icon to the right of the media set drop-down menu.</p> <p>See <a href="#">“About media sets”</a> on page 366.</p>
<b>Overwrite media</b>	<p>Indicates that the backup job is placed on an overwritable media. Ensure that appropriate media is in the storage device that you select.</p> <p>Appropriate media for an overwrite job include the following:</p> <ul style="list-style-type: none"> <li>■ Scratch media</li> <li>■ Media for which the overwrite protection period has expired</li> </ul> <p>Depending on your configuration, overwritable media is selected from scratch media or recyclable media.</p> <p>If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p> <p>See <a href="#">“About tape and disk cartridge media”</a> on page 365.</p> <p>See <a href="#">“About media overwrite protection levels for tape and disk cartridge media”</a> on page 377.</p> <p>See <a href="#">“How Backup Exec searches for overwritable media in tape drives and disk cartridges”</a> on page 378.</p>

**Table 17-18** Duplicate job settings for DBA-initiated jobs (*continued*)

Item	Description
<b>Append to media, overwrite if no appendable media is available</b>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec searches for an overwritable media and adds it to the media set.</p> <p>If an append job fills a media, the backup job continues on an overwritable media. If the media in the storage device is not overwritable, an alert appears to prompt you to insert overwritable media.</p>
<b>Append to media, terminate job if no appendable media is available</b>	<p>Appends this backup job to the specified media set if an appendable media is available. Otherwise, Backup Exec terminates the job.</p>
<b>Eject media after job completes</b>	<p>Ejects the media from the drive or slot when the operation completes. You can also schedule a job to eject media.</p> <p>See <a href="#">“Ejecting media from a disk cartridge or tape drive”</a> on page 428.</p>
<b>Retension media before backup</b>	<p>Runs the tape in the drive from beginning to end at a fast speed. Retensioning helps the tape wind evenly and run more smoothly past the tape drive heads. This option is available only if you select a tape drive that supports retensioning.</p>
<b>Use Write once, read many (WORM) media</b>	<p>Specifies the use of WORM (write once, read many) media as the default for DBA-initiated jobs. Backup Exec confirms that the destination device is or contains a WORM-compatible drive, and that the WORM media is available in the drive. If WORM media or a WORM-compatible drive is not found, an alert is sent.</p> <p>See <a href="#">“About WORM media”</a> on page 383.</p>
<b>Enable DirectCopy to tape</b>	<p>Enables Backup Exec to coordinate the movement of data from virtual storage directly to a physical storage device.</p> <p>The Backup Exec server records information about the data in the catalog. Therefore, you can restore data from either the virtual storage or the physical storage.</p> <p>See <a href="#">“How to copy data directly from a virtual tape library to a physical tape device”</a> on page 225.</p>

**Table 17-18** Duplicate job settings for DBA-initiated jobs (*continued*)

Item	Description
<b>Compression</b>	<p>Provides the following compression options:</p> <ul style="list-style-type: none"> <li>■ <b>None</b> Copies the data to the media in its original form (uncompressed). Using some form of data compression can help expedite backups and preserve storage space. Hardware data compression should not be used in environments where storage devices that support hardware compression are used interchangeably with devices that do not have that functionality. In this situation, hardware compression is automatically disabled. You can manually turn on hardware compression on the drives that support it, but this results in media inconsistency. If the drive that supports hardware compression fails, the compressed media cannot be restored with the non-compression drive.</li> <li>■ <b>Software</b> Uses STAC software data compression, which compresses the data before it is sent to the storage device.</li> <li>■ <b>Hardware (if available, otherwise none)</b> Uses hardware data compression if the storage device supports it. If the drive does not feature data compression, the data is backed up uncompressed.</li> <li>■ <b>Hardware (if available, otherwise software)</b> Uses hardware data compression if the storage device supports it. If the drive does not feature hardware data compression, STAC software compression is used.</li> </ul>
<b>Encryption type</b>	<p>Specifies the encryption key that you want to use, if any. See <a href="#">“About encryption”</a> on page 551.</p>
<b>Encryption key</b>	<p>Specifies the encryption key that you want to use, if you selected to use encryption. See <a href="#">“Encryption keys”</a> on page 552.</p>
<b>Manage Keys</b>	<p>Lets you manage your encryption keys. You can delete or replace existing encryption keys. You can also create a new encryption key. This option is available only if you select an encryption type. See <a href="#">“About encryption key management”</a> on page 477.</p>

**Table 17-18** Duplicate job settings for DBA-initiated jobs (*continued*)

Item	Description
<b>Preferred source device</b>	Specifies the preferred source device that you want to use as the storage for the duplicate job.
<b>Verify after backup completes</b>	Performs a verify operation automatically to make sure that the data can be read once the backup has been completed. Verifying all backups is recommended.

## About logon accounts

A Backup Exec logon account stores the credentials of a user account that you use to access a computer. Backup Exec logon accounts enable Backup Exec to manage user names and passwords and can be used to browse computers or process jobs. Using Backup Exec logon accounts enables you to apply credential changes to the jobs that use them.

Backup Exec logon accounts are used to browse local and remote computers. Whenever the Backup Exec logon credentials are passed between the Backup Exec server and the remote computer, the credentials are encrypted.

Backup Exec logon accounts can also be associated with backup data at the device level such as shares, databases, etc. If you need to edit the credentials, you can edit the Backup Exec logon account. Any changes are applied to the selected computers that use the Backup Exec logon account.

Backup Exec logon accounts are not user accounts. When you create a Backup Exec logon account, an entry for the account is entered into the Backup Exec database; no operating system accounts are created. If your user account credentials change, you must update the Backup Exec logon account with the new information. Backup Exec does not maintain a connection with the user account.

You can view, create, delete, edit, and replace Backup Exec logon accounts.

See [“Creating a Backup Exec logon account”](#) on page 500.

See [“Deleting a Backup Exec logon account”](#) on page 504.

See [“Editing a Backup Exec logon account”](#) on page 502.

See [“Replacing a Backup Exec logon account”](#) on page 503.

The following types of logon accounts are included in Backup Exec:

**Table 17-19** Types of logon accounts

Type of logon account	Description
Default Backup Exec logon account	Used to browse local and remote computers, make backup job selections, and restore data.  See “ <a href="#">About the default Backup Exec logon account</a> ” on page 499.
Backup Exec system logon account	Used to access most or all of your data. It contains the Backup Exec Services credentials.  See “ <a href="#">About the Backup Exec System Logon Account</a> ” on page 501.
Backup Exec logon account	Used to manage Backup Exec user names and passwords, browse local and remote data, process jobs, and apply credential changes to the jobs that use them.

## About the default Backup Exec logon account

The default Backup Exec logon account enables you to browse, make selections, or restore data. The first time you start Backup Exec, you must specify a default Backup Exec logon account using the Logon Account Wizard. You can select an existing Backup Exec logon account or create a new one.

You can create multiple Backup Exec logon accounts; however, each Backup Exec user can have only one default Backup Exec logon account.

Your default Backup Exec logon account enables you to perform the following:

- Browse data. Your default Backup Exec logon account enables you to browse local and remote computers when you create backup jobs. To browse computers, each user must have a default Backup Exec logon account that is associated with their user account. The Backup Exec logon account does not have to be the same user name as the user that is used to log on to Backup Exec. For example, you are logged on to a Backup Exec server named BACKUPSERVER as the local Windows administrator. When you start Backup Exec, you are prompted to create a default Backup Exec logon account for the local administrator because one does not exist. You can create a Backup Exec logon account for the local administrator that has the credentials for a domain administrator. The Backup Exec logon account has the following properties:

User name: DOMAIN\Administrator  
 Description: BACKUPSERVER\Administrator Default Account  
 Owner: BACKUPSERVER\Administrator

When you change your default Backup Exec logon account, you can use your new default Backup Exec logon account to browse computers immediately. You do not have to restart your system in order for the changes take effect.

- **Make backup selections.** You can select a different Backup Exec logon account when you make selections for backup. If your default logon account does not have rights, the **Logon Account Selection** dialog box appears and lets you create or select a different Backup Exec logon account.

See [“How to use Backup Exec logon accounts for SQL databases”](#) on page 812.

See [“Requirements for accessing Exchange mailboxes”](#) on page 845.

- **Restore.** You can assign Backup Exec logon accounts to computers when you create restore jobs. The default Backup Exec logon account is used unless you choose a different Backup Exec logon account when you create the restore job.

See [“Changing your default Backup Exec logon account”](#) on page 505.

See [“About Backup Exec restricted logon accounts”](#) on page 500.

## About Backup Exec restricted logon accounts

Backup Exec logon accounts can be common or restricted. When you create a Backup Exec logon account, you can designate it as a restricted account. To use a restricted logon account, you must be the owner of the logon account or you must know the password for the logon account. The person who created the logon account is the owner. If you authorize only a few people to back up or restore data, you can make the logon account a restricted logon account.

The main reasons to restrict a logon account are as follows:

- To help you limit access to the computers available for backup.
- To help you limit the computers to which you can restore.

When you use a restricted logon account to select the data for a job, the logon account information is saved with the selection list. Anyone who tries to edit the job must provide the password to the restricted logon account. Backup Exec loads the selections for that job only when the password for the restricted logon account is provided.

See [“Creating a Backup Exec logon account”](#) on page 500.

See [“Editing a Backup Exec logon account”](#) on page 502.

## Creating a Backup Exec logon account

You can create Backup Exec logon accounts using the Logon Account Wizard, which guides you through the creation of a Backup Exec logon account, or by using the Logon Account Management dialog. You can enter Backup Exec logon

account property information when you create the Backup Exec logon account; however, Backup Exec assigns the Backup Exec logon account owner to the user name you used to log on to Backup Exec. The owner of the Backup Exec logon account cannot be modified.

See [“Editing a Backup Exec logon account”](#) on page 502.

See [“Replacing a Backup Exec logon account”](#) on page 503.

See [“Changing your default Backup Exec logon account”](#) on page 505.

### To create a Backup Exec logon account

◆ Do one of the following:

To create a new logon account by using the Logon Account wizard

Do the following in the order listed:

- Click the Backup Exec button, and then select **Configuration and Settings**.
- Select **Logon Accounts**, and then select **Logon Account Wizard**.

The wizard guides you through the setup process.

To create a new logon account manually

Do the following in the order listed:

- Click the Backup Exec button, and then select **Configuration and Settings**.
- Select **Logon Accounts**, and then select **Manage Logon Accounts**.
- Click **New**.
- Enter the appropriate options.  
 See [“Add Logon Credentials options”](#) on page 508.

## About the Backup Exec System Logon Account

The Backup Exec System Logon Account (SLA) is created when you install Backup Exec. When the SLA is created, the user name and password match the credentials that were provided during install for the Backup Exec Services credentials. The owner of the SLA is the user that installed Backup Exec and is a common account by default. Common accounts are shared accounts that all users can access.

The Backup Exec System Logon Account may have access to most or all of your data since it contains the Backup Exec Services credentials. If you want to make Backup Exec more secure, you can change the SLA to be a restricted account. You can also delete it after making another logon account the default. However, if you

delete the SLA, the jobs in which it is used may fail. If the SLA is deleted, you can re-create it using the Logon Account Management dialog box.

The SLA is used for the following tasks and jobs:

- Jobs that were migrated from a previous version of Backup Exec
- Duplicate backup data jobs
- Command Line Applet (bemcli.exe)

See [“Creating a new Backup Exec System Logon Account”](#) on page 505.

See [“Creating a Backup Exec logon account”](#) on page 500.

See [“Editing a Backup Exec logon account”](#) on page 502.

See [“Replacing a Backup Exec logon account”](#) on page 503.

See [“Deleting a Backup Exec logon account”](#) on page 504.

See [“Changing your default Backup Exec logon account”](#) on page 505.

See [“Copying logon account information to another Backup Exec server”](#) on page 505.

## Editing a Backup Exec logon account

When you edit a Backup Exec logon account, the changes are automatically applied to all the content that uses the Backup Exec logon account. Changes made to a Backup Exec logon account are applied immediately. You do not have to restart your system for the changes to take effect.

You can edit the following properties for a Backup Exec logon account:

- Type (restricted, common, or default)
- Account name
- Password
- User name
- Notes

See [“Changing your default Backup Exec logon account”](#) on page 505.

### To edit a Backup Exec logon account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.

- 3 Select the Backup Exec logon account you want to change, and then click **Edit**.

If you are not logged on to Backup Exec with the same user name as the Backup Exec logon account owner, you must provide the password before you can edit the account.

- 4 Modify the Backup Exec logon account properties as needed.  
See “[Edit Logon Credentials options](#)” on page 509.
- 5 On the **Edit Logon Credentials** dialog box, click **OK**.
- 6 On the **Logon Account Management** dialog box, click **OK**.

## Changing the password for a Backup Exec logon account

You can change a Backup Exec logon account password using the following steps. Changes made to a Backup Exec logon account password are applied immediately.

See “[About logon accounts](#)” on page 498.

### To change the password for a Backup Exec logon account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Select the Backup Exec logon account that you want to change, and then click **Edit**.  
  
If you are not logged on to Backup Exec with the same user name as the Backup Exec logon account owner, you must provide the password before you can edit the account.
- 4 Click **Change password**.
- 5 In the **Password** field, type a new password.
- 6 In the **Confirm** field, re-type the password, and then click **OK**.
- 7 On the **Edit Logon Credentials** dialog box, click **OK**.
- 8 On the **Logon Account Management** dialog box, click **OK**.

## Replacing a Backup Exec logon account

You can replace a Backup Exec logon account within all existing jobs. The data in existing jobs that use the Backup Exec logon account will be updated to use the new Backup Exec logon account. If the new Backup Exec logon account is restricted, you must provide the password.

See [“About logon accounts”](#) on page 498.

#### To replace a Backup Exec logon account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Select the Backup Exec logon account you want to replace, and then click **Replace**.
- 4 On the **Replace Logon Account** dialog box, select the Backup Exec logon account with which you want to replace the selected Backup Exec logon account.

If the Backup Exec logon account is restricted and you are not logged on to Backup Exec with the same user name as the Backup Exec logon account owner, you must provide the password before you can edit the account.

- 5 Click **OK**.

## Deleting a Backup Exec logon account

You cannot delete a Backup Exec logon account in the following situations:

- It is being referenced by a job.
- It is owned by a user who is logged on to the Backup Exec server.
- It is set as the default Backup Exec logon account of a user who is logged on to the Backup Exec server.

You can delete a Backup Exec logon account when the owner is logged off and all users who have it set as their default logon account are logged off.

See [“About logon accounts”](#) on page 498.

#### To delete a Backup Exec logon account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Select the Backup Exec logon account you want to delete, and then click **Delete**.
- 4 Click **Yes** to confirm the deletion.

## Changing your default Backup Exec logon account

You can change your default Backup Exec logon account that enables you to browse, make selections, or restore data.

See [“About the default Backup Exec logon account”](#) on page 499.

### To change your default Backup Exec logon account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Select the Backup Exec logon account that you want to use as your default Backup Exec logon account, and then do one of the following:
  - Click **Set as Default**.
  - Click **Edit**, select **This is my default account**, and then click **OK**.

## Creating a new Backup Exec System Logon Account

The Backup Exec System Logon Account enables you to perform several operations. If you delete the Backup Exec System Logon Account, you should create a new one that enables you to perform the specified operations.

See [“About the Backup Exec System Logon Account”](#) on page 501.

### To create a new Backup Exec System Logon Account

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Click **System Account**.
- 4 Select the appropriate options, and then click **OK** to create the system logon account.

See [“Edit Logon Credentials options”](#) on page 509.

## Copying logon account information to another Backup Exec server

You can copy logon account information to a different Backup Exec server.

See [“About logon accounts”](#) on page 498.

### To copy logon account information to another Backup Exec server

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Logon Accounts**.
- 2 Select **Manage Logon Accounts**.
- 3 Select the logon account that you want to copy, and then click **Copy to Servers**.
- 4 If prompted, enter the password for the logon account that you selected.
- 5 Do one of the following:
  - To add individual servers manually, in the **Server Name** field, enter the name of the Backup Exec server that you want to copy the logon account information to, and then click **Add**
  - To add several servers from a list, click **Import List**, and then browse to the list of server names.
- 6 If you want to overwrite a logon account with the same name on the destination Backup Exec server, check **If an account with this description already existson the destination server, overwrite it**.
- 7 Click **OK**.

## Logon Account Management options

You can view, create, delete, edit, and replace Backup Exec logon accounts using the Logon Account Management dialog box.

See [“Creating a Backup Exec logon account”](#) on page 500.

See [“Deleting a Backup Exec logon account”](#) on page 504.

See [“Editing a Backup Exec logon account”](#) on page 502.

See [“Replacing a Backup Exec logon account”](#) on page 503.

See [“Changing the password for a Backup Exec logon account”](#) on page 503.

See [“Changing your default Backup Exec logon account”](#) on page 505.

See [“Creating a new Backup Exec System Logon Account”](#) on page 505.

See [“Copying logon account information to another Backup Exec server”](#) on page 505.

The dialog box displays property information for each Backup Exec logon account you create. It also displays your default Backup Exec logon account and the Windows user name that is currently logged on to the Backup Exec server.

**Table 17-20** Logon Account Management options

Item	Description
<b>Account Name</b>	Indicates the unique name for this Backup Exec logon account. You can name this account when you create a new logon account. If you do not give the logon account a name, the user name is automatically added. The System Logon Account is created when you install Backup Exec.
<b>User Name</b>	Indicates the fully qualified user name for the Backup Exec logon account. The user name is provided when you attempt to connect to a computer.
<b>Default</b>	Indicates the default Backup Exec logon account used to browse, make selections, or restore data on your local and remote computers.
<b>Type</b>	<p>Indicates whether the account is common or restricted.</p> <p>A restricted account can be used only by the owner of the logon account and those who know the password. A common account is a shared account that can be accessed by all users.</p> <p>To use a restricted logon account, you must be the owner of the logon account or you must know the logon account's password. The person who created the logon account is the owner. If you authorize only a few people to back up or restore data, you can make the logon account a restricted logon account.</p> <p>The main reasons to restrict a logon account are as follows:</p> <ul style="list-style-type: none"> <li>■ To limit access to the content available for backup.</li> <li>■ To limit the ability to restore data.</li> </ul> <p>When you use a restricted logon account to select the data for a job, the logon account information is saved with the selection list. Anyone who tries to edit the job must provide the password to the restricted logon account. Backup Exec only loads the selections for that job when the password for the restricted logon account is provided.</p>
<b>Owner</b>	Indicates the name of the logon account's owner. Backup Exec assigns the Backup Exec logon account owner to the Windows user name you used to log on to Backup Exec. The owner of the Backup Exec logon account cannot be modified.
<b>Add</b>	<p>Enables you to create a new Backup Exec logon account.</p> <p>See <a href="#">"Creating a Backup Exec logon account"</a> on page 500.</p>

**Table 17-20** Logon Account Management options (*continued*)

Item	Description
<b>Delete</b>	<p>Enables you to delete a Backup Exec logon account. You cannot delete a Backup Exec logon account that is currently being referenced by a job. You can delete the Backup Exec logon account for users that are logged off.</p> <p>See <a href="#">“Deleting a Backup Exec logon account”</a> on page 504.</p>
<b>Edit</b>	<p>Enables you to edit properties for a Backup Exec logon account. When you edit a Backup Exec logon account, the changes will automatically be applied to all the content that uses the Backup Exec logon account.</p> <p>See <a href="#">“Editing a Backup Exec logon account”</a> on page 502.</p>
<b>Replace</b>	<p>Enables you to replace a Backup Exec logon account within all existing jobs and selection lists. The data in existing jobs that use the Backup Exec logon account will be updated to use the new Backup Exec logon account.</p> <p>See <a href="#">“Replacing a Backup Exec logon account”</a> on page 503.</p>
<b>Set as Default</b>	<p>Enables you to change your default Backup Exec logon account.</p>
<b>System Account</b>	<p>Enables you to create a new Backup Exec System logon account. The system logon account enables you to perform several operations, such as copy jobs. It is also used with the Command Line Applet. If you delete the system logon account, you should create a new one that enables you to perform the operations and use the Command Line Applet.</p>
<b>Copy to Servers</b>	<p>Copies logon account information to another Backup Exec server.</p> <p>See <a href="#">“Copying logon account information to another Backup Exec server”</a> on page 505.</p>

## Add Logon Credentials options

You can enter Backup Exec logon account property information when you create the Backup Exec logon account.

See [“Creating a Backup Exec logon account”](#) on page 500.

**Table 17-21** Add Logon Credentials options

Item	Description
<b>User name</b>	Indicates the fully qualified user name for the Backup Exec logon account. For example, DOMAIN\Administrator. The user name is provided when you attempt to connect to a computer. The user name is not case sensitive for the computers that are accessed.
<b>Password</b>	Indicates the password for the account. The password you enter is encrypted for security. You can leave this field blank if this Backup Exec logon account does not need a password.
<b>Confirm password</b>	Verifies the password. The password must match the password you typed in the Password field.
<b>Account name</b>	Indicates the unique name for the Backup Exec logon account. The user name is automatically added if you do not enter information into the field.
<b>Notes</b>	Indicates how the Backup Exec logon account will be used.
<b>This is a restricted logon account</b>	Enables the Backup Exec logon account to be used only by the owner of the logon account and those who know the password. If this is not selected, the Backup Exec logon account will be a common account. Common accounts are shared accounts that can be accessed by all users.  See <a href="#">“About Backup Exec restricted logon accounts”</a> on page 500.
<b>This is my default account</b>	Makes this account your default Backup Exec logon account, which is used to browse, make selections, or restore data on your local and remote computers.  See <a href="#">“About the default Backup Exec logon account”</a> on page 499.

## Edit Logon Credentials options

You can change the properties of an existing logon account.

See [“Editing a Backup Exec logon account”](#) on page 502.

**Table 17-22** Edit Logon Credentials options

Item	Description
<b>User name</b>	Indicates the fully qualified user name for the Backup Exec logon account. For example, DOMAIN\Administrator. The user name is provided when you attempt to connect to a computer. The user name you enter is not case sensitive for the computers that are accessed.
<b>Change Password</b>	Enables you to change the password for the account. The password you enter is encrypted for security.
<b>Account name</b>	Indicates the unique name for the Backup Exec logon account. The user name is automatically added if you do not enter information into the field.
<b>Notes</b>	Indicates how the Backup Exec logon account will be used.
<b>This is a restricted logon account</b>	Enables the Backup Exec logon account to be used only by the owner of the logon account and those who know the password. If this is not selected, the Backup Exec logon account will be a common account. Common accounts are shared accounts that can be accessed by all users.  See <a href="#">“About Backup Exec restricted logon accounts”</a> on page 500.
<b>This is my default account</b>	Makes this account your default Backup Exec logon account used to browse, make selections, or restore data on your local and remote computers.  See <a href="#">“About the default Backup Exec logon account”</a> on page 499.

## Copy Logon Account options

You can copy logon account information to a different Backup Exec server.

See [“Copying logon account information to another Backup Exec server”](#) on page 505.

**Table 17-23** Copy Logon Account options

Item	Description
<b>Server Name</b>	Indicates the name of the Backup Exec server to which you want to copy the logon account information, and then click <b>Add</b> .

**Table 17-23** Copy Logon Account options (*continued*)

Item	Description
<b>Logon Account</b>	Indicates the name of the current logon account that is used on the server to which you want to copy logon account information.
<b>Add</b>	Adds the Backup Exec server from the Server Name field to the list of Backup Exec servers.
<b>Remove</b>	Removes a Backup Exec server from the list.
<b>Import List</b>	Imports a list of Backup Exec servers to be added to the Backup Exec servers in the list. The list should include only the Backup Exec server name, with one per line.
<b>Logon Account</b>	Specifies the logon account to use when connecting to the Backup Exec servers in the list.
<b>Overwrite logon account if one with this description already exists on the destination server</b>	Overwrites logon accounts for an existing job having the same name. This option appears only if you copy a job to another Backup Exec server.

## About the Backup Exec Services Manager

The Backup Exec Services Manager lets you manage the Backup Exec services. You can perform the following actions using the Backup Exec Services Manager

- Start, restart, or stop Backup Exec services  
 See [“Starting and stopping Backup Exec services”](#) on page 511.
- Change or edit the Backup Exec service account  
 See [“Changing service account information”](#) on page 513.
- Change startup options for services  
 See [“Changing service startup options”](#) on page 514.

### Starting and stopping Backup Exec services

You can start, stop, and restart Backup Exec services.

### To start or stop Backup Exec services

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Services**.
- 2 Select the appropriate options.  
See [“Backup Exec Services Manager options”](#) on page 512.

## Backup Exec Services Manager options

You can start, stop, and restart Backup Exec services.

See [“Starting and stopping Backup Exec services”](#) on page 511.

Table 17-24 Backup Exec Services Manager options

Item	Description
<b>Server name</b>	Indicates the name of a server for which you want to start, stop, or restart services. You can type the name of a server or import a list of servers.
<b>Add server</b>	Enables you to add a server for which you want to start, stop, or restart services.
<b>Remove server</b>	Enables you to remove a server that you no longer use.
<b>Start all services</b>	Starts all Backup Exec services for the selected server.
<b>Stop all services</b>	Stops all Backup Exec services for the selected server.
<b>Restart all services</b>	Stops all Backup Exec services and then restart the services for the selected server.
<b>Edit credentials</b>	Lets you change service account information or startup options.
<b>Connect</b>	Lets you connect to a different server.
<b>Enable deduplication services to be started or stopped</b>	Lets you include any deduplication services in the list of services so that you can start or stop them.

## About the Backup Exec service account

All Backup Exec services on the Backup Exec server run in the context of a user account that is configured for the Backup Exec system services. You can create this account during the Backup Exec installation, or you can use an existing user account.

---

**Note:** The Backup Exec service account and the Backup Exec system logon account are set to the same user name when Backup Exec is installed. If you need to change the user name for the service account or if the service account is no longer used, then you should also change the Backup Exec system logon account to use new credentials.

---

See [“Changing service account information”](#) on page 513.

If this computer is in a domain, enter a Domain Administrators account, or an equivalent account that is part of the Domain Admins group. In the Domain list, select or enter the Domain name.

If this computer is in a workgroup, enter an Administrators account, or an equivalent account that is part of the Administrators group on the computer. In the Domain list, select or enter the computer name.

The account that you designate for Backup Exec services, whether it is a new account or an existing user account, is assigned the following rights:

- Authenticate as any user and gain access to resources under any user identity.
- Create a token object, which can then be used to access any local resources.
- Log on as a service.
- Administrative rights (provides complete and unrestricted rights to the computer).
- Backup operator rights (provides rights to restore files and directories).
- Manage auditing and security log.

See [“Required user rights for backup jobs”](#) on page 157.

Due to security implementations in Microsoft Small Business Server, the service account must be Administrator.

## Changing service account information

On the Backup Exec server, all Backup Exec services run in the context of a user account that is configured for the Backup Exec system services.

---

**Note:** The Backup Exec service account and the Backup Exec system logon account are set to the same user name when Backup Exec is installed. If you need to change the user name for the service account or if the service account is no longer used, then you should also change the Backup Exec system logon account to use new credentials.

---

See [“About the Backup Exec service account”](#) on page 512.

#### To change service account information

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Services**.
- 2 On the **Backup Exec Services Manager** dialog box, select the appropriate server, and then select the service for which you want to change the service account.
- 3 Click **Edit credentials**.
- 4 Check the **Change service account credentials** check box.
- 5 Enter the new user name and password for the service account.

See [“Service Account Information options”](#) on page 515.

- 6 Click **OK**.
- 7 Click **Close**.

## Changing service startup options

You can change startup options for Backup Exec services. Each individual service can be configured to start automatically or manually. Or you can disable a service entirely.

Services that are configured for automatic startup automatically start when the server starts. Services that are configured for manual startup do not start automatically. You must manually start services that are configured for manual startup. You can start, stop, or restart services in the Backup Exec Services Manager.

#### To change service startup options

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Services**.
- 2 On the **Backup Exec Services Manager** dialog box, select the appropriate server, and then select the service for which you want to change startup options.
- 3 Click **Edit credentials**.
- 4 Check the **Change startup options** check box.
- 5 Select the new startup option for the service.

See [“Service Account Information options”](#) on page 515.

- 6 Click **OK**.
- 7 Click **Close**.

## Service Account Information options

You can change the Backup Exec service account and how services start.

See [“Changing service account information”](#) on page 513.

See [“Changing service startup options”](#) on page 514.

**Table 17-25** Service Account Information options

Item	Description
<b>Change service account credentials</b>	Enables you to change the user name, domain, and password for the service account.
<b>Old user name</b>	Indicates the current user name for the service account.
<b>Old password</b>	Indicates the current password for the service account.
<b>New user name</b>	Indicates the new user name that you would like to use for the service account.
<b>New password</b>	Indicates the new password that you would like to use for the service account.
<b>Confirm password</b>	Confirms the password that you typed in the <b>New password</b> field.
<b>Change startup options for services</b>	Lets you change the startup options for the service account.
<b>Automatic</b>	Indicates that the service account starts automatically at system startup.
<b>Manual</b>	Indicates that the service account does not start automatically at system startup. You must start it manually.
<b>Disabled</b>	Indicates that the service account is disabled at system startup.
<b>Grant required rights to the service account</b>	Lets the service account have the system service rights.

## About audit logs

Use audit logs to examine and review information about operations that have been performed in Backup Exec. The audit log displays the date and time of the activity, who performed it, what the activity was, and a description of the activity. You can view information about activities that occur for all or any of the following:

- Alerts
- Audit logs
- Devices and media
- Encryption keys
- Error-handling rules
- Jobs
- Logon accounts
- Server configuration

You can delete the audit logs as part of the Backup Exec database maintenance, and you can save the audit log to a file. Changes made to the audit log, such as when database maintenance occurs, can also be displayed in the audit log.

See [“Configuring the audit log”](#) on page 516.

See [“Viewing the audit log”](#) on page 517.

See [“Removing entries from the audit log”](#) on page 517.

See [“Saving the audit log to a file”](#) on page 518.

## Configuring the audit log

Configure the audit log to display information about specific operations that are performed on items in Backup Exec.

See [“About audit logs”](#) on page 516.

See [“Viewing the audit log”](#) on page 517.

### To configure the audit log

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 On the **Audit Logs** dialog box, click **Configure Logging**.

- 3 On the **Audit Log Configuration** dialog box, select the check box of the category that you want to display in the audit log.  
  
Expand the category by clicking the arrow to the left of the category. Select the operations that you want to display for the category.  
  
Clear the check box of any item or operation that you do not want to display.
- 4 Click **OK**.

## Viewing the audit log

You can view audit logs to see when changes were made in Backup Exec and which users made the changes.

See [“About audit logs”](#) on page 516.

See [“Configuring the audit log”](#) on page 516.

### To view the audit log

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 In **Select category to view**, select the category for which you want to view audit information.  
  
See [“Audit Logs options”](#) on page 518.
- 3 Use the scroll bar at the bottom of the Audit Logs window to view the whole entry, or double-click the entry to display the same information in an easy-to-read Audit Log Record.

## Removing entries from the audit log

You can remove the entries for all categories or for a selected category.

See [“About audit logs”](#) on page 516.

### To remove entries from the audit log

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 In **Select category to view**, select the category for which you want to view audit information.
- 3 Click **Clear Category Log** to remove all entries from an audit log category.  
  
If you select specific categories to view, only the logs generated for the selected categories are cleared when you click **Clear Category Log**.

## Saving the audit log to a file

You can save the audit log as a text (.txt) file.

See [“About audit logs”](#) on page 516.

### To save the audit log to a file

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Audit Log**.
- 2 Click **Save Log to File** to specify a file name and location to save the audit log entries.

## Audit Logs options

You can view audit logs to see when changes were made in Backup Exec and which users made the changes.

See [“Viewing the audit log”](#) on page 517.

See [“Removing entries from the audit log”](#) on page 517.

See [“Saving the audit log to a file”](#) on page 518.

**Table 17-26**      **Audit Logs options**

Item	Description
<b>Select category to view</b>	Lets you select the category for which you want to view audit logs.
<b>Date/Time</b>	Shows the date and time that this change was made in Backup Exec. Click the column head to sort the information by date.
<b>User Name</b>	Shows the domain and the user name of the user that made the change. Click the column head to sort the information alphabetically.
<b>Category</b>	Shows the category to which the log belongs. Click the column head to sort the information alphabetically.
<b>Message</b>	Shows the action that was recorded by Backup Exec for the operation that was performed. Click the column head to sort the information alphabetically.
<b>Refresh</b>	Updates the audit log with new entries.
<b>Clear Category Log</b>	Removes all entries from an audit log category.

**Table 17-26**      **Audit Logs options** (*continued*)

Item	Description
<b>Save Log to File</b>	Indicates where to save audit log entries. You can save the audit log as a text (.txt) file.
<b>Properties</b>	Provides information about the selected entry.
<b>Configure Logging</b>	Lets you select the categories and options to include in the audit log.

## Copying configuration settings to another Backup Exec server

If you have the Central Admin Server Option (CASO), you can copy configuration settings and logon information from one Backup Exec server to another. This copy ability allows you to quickly set up a group of Backup Exec servers with the same configuration or logon settings.

See [“Copying logon account information to another Backup Exec server”](#) on page 505.

---

**Note:** To copy configuration settings and logon information to other Backup Exec servers, you must install the **Copy Server Configurations** feature.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

---

### To copy configuration settings to another Backup Exec server

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Copy Settings to Other Servers**.
- 2 Select the appropriate settings to copy.  
 See [“Copy Settings options”](#) on page 520.
- 3 Do one of the following:

If the Backup Exec server to which you want to copy the setting appears in the <b>Destination Backup Exec servers</b> list	Select the name of the Backup Exec server.
--	--

If the Backup Exec server to which you want to copy the settings does not appear in the **Destination Backup Exec servers** list

Do one of the following:

- Click **Add** to add a Backup Exec server to the list. After you add the Backup Exec server, you can select it as a destination.  
See “[Adding a destination Backup Exec server to the Copy Settings dialog](#)” on page 521.
- Click **Import List** to add multiple Backup Exec servers from a list. After you add the list, you can select any of the Backup Exec servers on the list as a destination.

4 Click **OK**.

## Copy Settings options

On the **Copy Settings** dialog box, you can select the type of settings to copy to another Backup Exec server.

See “[Copying configuration settings to another Backup Exec server](#)” on page 519.

Table 17-27 Copy Settings options

Item	Description
<b>Default job options</b>	Lets you copy default job options from this Backup Exec server to another Backup Exec server.
<b>Default schedule</b>	Lets you copy the default schedule settings from this Backup Exec server to another Backup Exec server.
<b>Error-handling rules</b>	Lets you copy error-handling rules from this Backup Exec server to another Backup Exec server.
<b>Alert configuration</b>	Lets you copy the alert configuration from this Backup Exec server to another Backup Exec server.
<b>Name</b>	Displays the name of the Backup Exec server.
<b>Logon Account</b>	Displays the logon account that is used to connect to the selected Backup Exec server. You can change the logon account if you want to use a different one.

**Table 17-27**      **Copy Settings options** (*continued*)

Item	Description
<b>Add</b>	Lets you add a Backup Exec server to the <b>Destination Backup Exec servers</b> list. After you add a Backup Exec server to the list, you can copy settings to it.
<b>Remove</b>	Lets you remove the selected Backup Exec server from the <b>Destination Backup Exec servers</b> list.
<b>Import List</b>	Lets you import a list of Backup Exec servers to the <b>Destination Backup Exec servers</b> list. After you add Backup Exec servers to the list, you can copy settings to them.

## Importing a list of destination Backup Exec servers to the Copy Settings dialog

If you have the Central Admin Server Option (CASO), you can copy settings from one Backup Exec server to another Backup Exec server. If the Backup Exec server to which you want to copy the settings does not appear in the **Destination Backup Exec servers** list on the **Copy Settings** dialog box, you can add it by importing a list. After you add a Backup Exec server to the **Destination Backup Exec servers** list, you can select it as a destination.

See [“Copying configuration settings to another Backup Exec server”](#) on page 519.

### To import a list of destination Backup Exec servers

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Copy Settings to Backup Exec Servers**.
- 2 Click **Import List**.
- 3 Browse to select the list, and then click **Open**.
- 4 Click **OK**.

## Adding a destination Backup Exec server to the Copy Settings dialog

If you have the Central Admin Server Option (CASO), you can copy settings from one Backup Exec server to another Backup Exec server. If the Backup Exec server to which you want to copy the settings does not appear in the **Destination Backup Exec servers** list on the **Copy Settings** dialog box, you can add it. After you add a Backup Exec server to the **Destination Backup Exec servers** list, you can select it as a destination.

See [“Copying configuration settings to another Backup Exec server”](#) on page 519.

**To add a destination Backup Exec server**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Copy Settings to Backup Exec Servers**.
- 2 Click **Add**.
- 3 Select the appropriate options.  
 See [“Add Server options”](#) on page 522.
- 4 If necessary, select or enter the correct logon account information to be used to complete the copy operation.  
 See [“About logon accounts”](#) on page 498.  
 Changing a logon account's credentials for a copy operation does not permanently change the logon account.
- 5 Click **OK**.

**Add Server options**

You can use the **Add Server** dialog box to add Backup Exec servers to which you want to copy settings.

See [“Copying configuration settings to another Backup Exec server”](#) on page 519.

See [“Adding a destination Backup Exec server to the Copy Settings dialog”](#) on page 521.

**Table 17-28**      **Add Server options**

Item	Description
<b>Add an individual Backup Exec server</b>	Lets you select a single Backup Exec server to add to the <b>Destination Backup Exec servers</b> list on the <b>Copy Settings</b> dialog box. After you add the name of the Backup Exec server, you can then copy settings to it.
<b>Name</b>	Indicates the name of the Backup Exec server that you want to add to the <b>Destination Backup Exec servers</b> list on the <b>Copy Settings</b> dialog box.
<b>Add all managed Backup Exec servers</b>	Lets you add all of the managed Backup Exec servers in your environment to the <b>Destination Backup Exec servers</b> list on the <b>Copy Settings</b> dialog box. This option lets you copy settings to any managed server.
<b>Logon account used to connect to Backup Exec servers</b>	Shows the name of the logon account that is used to access the Backup Exec servers you selected.

**Table 17-28** Add Server options (*continued*)

Item	Description
Add/Edit	Lets you change the logon account that Backup Exec uses to access the Backup Exec servers you selected.

## About viewing server properties

You can view properties for the local Backup Exec server or any other server that you monitor with Backup Exec. Backup Exec displays general and system information about the servers.

You can view the following properties for any server that you monitor with Backup Exec:

- Server name
- Server description
- Operating system information
- Backup Exec version and license information

See [“Viewing server properties”](#) on page 524.

Additionally, you can view the following properties for the local Backup Exec server:

- Server name
- Server description
- Server status
- Version and license information
- Date and time zone information
- Operating system information
- Memory and page file information

See [“Viewing local Backup Exec server properties”](#) on page 524.

If you have the Central Admin Server Option (CASO), you can also view information about the Backup Exec database, device and media database, and catalog database.

See [“Viewing the settings for a central administration server”](#) on page 1041.

## Viewing local Backup Exec server properties

You can view properties for the local Backup Exec server. Backup Exec displays general and system information about the server.

See [“About viewing server properties”](#) on page 523.

### To view the local Backup Exec server properties

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then click **Local server properties**.
- 2 When you are finished viewing the local server properties, click **OK**.

## Viewing server properties

You can view properties for any server that you monitor with Backup Exec. Backup Exec displays general and system information about the server.

See [“About viewing server properties”](#) on page 523.

### To view server properties

- 1 On the **Backup and Restore** tab, double-click the server whose properties you want to view.
- 2 In the left pane, click **Properties**.

# Backup strategies

This chapter includes the following topics:

- [About backup strategies](#)
- [About backup methods](#)
- [About configuring Backup Exec to determine if a file has been backed up](#)
- [About backing up and deleting files](#)
- [About using fully qualified domain names in backup selections](#)
- [About discovering data to back up](#)
- [About using checkpoint restart](#)
- [About backing up critical system components](#)
- [About the Backup Exec Shadow Copy Components file system](#)
- [About managing Microsoft Virtual Hard Disk \(VHD\) files in Backup Exec](#)
- [About pre/post commands](#)
- [How to restore individual items by using Granular Recovery Technology](#)
- [About specifying backup networks](#)
- [About using IPv4 and IPv6 in Backup Exec](#)
- [About using Backup Exec with Symantec Endpoint Protection](#)
- [About encryption](#)

## About backup strategies

A backup strategy is the collection of procedures you implement for backing up your network. Backup strategies include what methods of backups are performed, when backups are performed, and how media is rotated back into use for your regular backups. A good backup strategy allows minimal time to recover a system in the event of a disaster.

Backup Exec offers flexible solutions for protecting the data on your network. You can let Backup Exec do all the administrative work for you or you can design and manage your own strategy that meets your exact specifications.

See [“Media rotation strategies”](#) on page 398.

See [“How to choose a backup strategy”](#) on page 526.

See [“How to determine your backup schedule”](#) on page 526.

See [“How to determine the amount of data to back up”](#) on page 527.

See [“How to determine a schedule for data storage”](#) on page 527.

See [“How to determine what data to back up”](#) on page 528.

## How to choose a backup strategy

You should consider the following to develop a secure and an effective plan for managing your data:

- The importance of the data you back up
- How often your system needs to be backed up
- How much storage media you need
- When you need to use storage media
- How to keep track of your backup information

See [“About backup strategies”](#) on page 526.

## How to determine your backup schedule

When you consider how often you should back up your data, you should take into account the cost of having to recreate data. Consider how much data would have been added or modified since the last backup.

Calculate the manpower, lost time or sales, and other costs that would be incurred in the event of a hardware failure. Imagine that the hardware failure occurred right before the next backup was scheduled to take place. You should always

assume the worst scenario. If the cost is excessive, you should adjust your backup schedule accordingly.

For example, the cost to recreate an extensive database system that several database operators continually update would be quite substantial. On the other hand, the cost to recreate the data for a user creating one or two interoffice memos would be considerably less. In this scenario, the network administrator may opt to back up the database several times daily, and run daily jobs for the user's workstation.

In an ideal environment, one full backup should be performed on workstations every day. Servers should be fully backed up more often. Important data files and any directories that constantly change may need to be backed up several times a day. Because of time and media constraints, running frequent full backups is not feasible for many environments. Instead, you can use a schedule that includes incremental or differential backups. For safety reasons, a full backup should always be performed before you add new applications or change any server configurations.

See [“About backup strategies”](#) on page 526.

## How to determine the amount of data to back up

The amount of data that you need to back up is a key factor when you decide on a media rotation strategy. If you back up large amounts of data that need to be retained for a long time, you need to select a suitable strategy.

See [“About backup strategies”](#) on page 526.

## How to determine a schedule for data storage

The amount of time that the data needs to be stored is directly related to the media rotation scheme that you use. For example, if you use one media set and back up every day, your backups are never more than a day old.

Storage is relatively inexpensive when compared to the value of your data. Therefore, it is a good idea to periodically back up your system and store it permanently. Some administrators may choose to make permanent backups every week. Others may choose to store only one permanent backup per month.

The threat of viruses is an issue also. Some viruses take effect immediately, while others may take days or weeks to cause noticeable damage.

You should have at least the following backups available to restore at any time:

- Three daily backups (for example, Monday, Tuesday, Wednesday)
- A one-week-old full backup

- A one-month-old full backup

Having these backups available should let you restore your system to its condition before it became infected.

See [“About backup strategies”](#) on page 526.

## How to determine what data to back up

Since Backup Exec can back up servers, workstations, and agents, you should consider what data you want to protect. You should select the times that are suitable to back up different computers. For example, you may want to back up file servers during the evening and back up workstations at lunchtime.

See [“About backup strategies”](#) on page 526.

## About backup methods

Before you can develop your backup strategy, you need to decide which backup method or backup methods that you want to use. You can perform full backups exclusively or you can use a strategy that includes one or more of the modified backup methods.

---

**Note:** You should perform a full backup of your server to establish a baseline for disaster recovery.

---

The backup methods used by Backup Exec are as follows:

- Full  
See [“About the full backup method”](#) on page 528.
- Differential  
See [“About the differential backup method”](#) on page 529.
- Incremental  
See [“About the incremental backup method”](#) on page 530.

Each backup method has advantages and disadvantages.

See [“About backup method advantages and disadvantages”](#) on page 530.

## About the full backup method

Full backups include all of the data that was selected for backup. Backup Exec detects that the server was backed up.

---

**Note:** You should perform a full backup of your server to establish a baseline for disaster recovery.

---

Full backups also include duplicate backups, which include all selected data. Duplicate backups do not affect your media rotation strategy because the archive bit is not reset.

Duplicate backups are useful when you need to do the following:

- Back up data for a special purpose.
- Back up specific data.
- Perform an additional backup to take off-site.
- Back up data without affecting your media rotation strategy.

See [“About duplicating backed up data”](#) on page 218.

Another option for full backups is to use the **Delete selected files and folders after successful backup** option. This option deletes the backed up data from the volume after a successful full backup to free disk space and to reduce clutter.

See [“About backing up and deleting files”](#) on page 535.

See [“About backup methods”](#) on page 528.

## About the differential backup method

Differential backups include all files that have changed since the last full backup. The difference between differential and incremental backups is that incremental backups include any files that have changed since the last full or incremental backup.

---

**Note:** In a backup definition that includes a differential task, all of the backup tasks must use storage devices that the same Backup Exec server can access.

---

By default, Backup Exec uses the Windows Change Journal to determine if files were previously backed up. You can also configure Backup Exec to use a file's modified time, archive bit, or the Backup Exec catalogs to determine if the file was backed up.

See [“Files and Folders options”](#) on page 204.

---

**Note:** If you use modified time to determine if files have been backed up, the full and the differential backups must use the same backup selections.

---

Differential backups allow much easier restoration of an entire device than incremental backups since only two backups are required. Using fewer media also decreases the risk of having a restore job fail because of media errors.

See [“About backup methods”](#) on page 528.

## About the incremental backup method

Incremental backups include only the files that have changed since the last full or incremental backup. The difference between incremental and differential backups is that differential backups include any files that have changed since the last full backup.

---

**Note:** In a backup definition that includes an incremental task, all of the backup tasks must use storage devices that the same Backup Exec server can access.

---

By default, Backup Exec uses the Windows Change Journal to determine if files were previously backed up. You can also configure Backup Exec to use a file's modified time, archive bit, or the Backup Exec catalogs to determine if the file was backed up.

See [“Files and Folders options”](#) on page 204.

---

**Note:** If you use modified time to determine if files have been backed up, the full and the incremental backups must use the same backup selections.

---

Incremental backups take much less time than full or differential backups to complete. They also require less storage space for backed up data since only any files that have changed since the last backup are backed up.

See [“About backup methods”](#) on page 528.

## About backup method advantages and disadvantages

Each backup method has advantages and disadvantages.

See [“About backup methods”](#) on page 528.

**Table 18-1** Backup method Advantages and Disadvantages

Method	Advantages	Disadvantages
Full	<ul style="list-style-type: none"> <li>■ Files are easy to find Full backups include all the data that you selected to back up. Therefore, you don't have to search through several backup sets to find a file that you need to restore.</li> <li>■ A current backup of your entire system is available on one backup set If you run a full backup of your entire system and then need to restore it, all of the most current information is located in one place.</li> </ul>	<ul style="list-style-type: none"> <li>■ Redundant backups Most of the files on your file server do not change. Each full backup that follows the first is merely a copy of what has already been backed up. Full backups require more storage.</li> <li>■ Full backups take longer to perform Full backups can be time consuming, especially when you have other servers on the network that need to be backed up (for example, agent workstations, remote servers).</li> </ul>
Differential	<ul style="list-style-type: none"> <li>■ Files are easy to find Restoring a system that is backed up with a differential method requires a maximum of two backups. Differentials require the latest full backup and the latest differential backup. Restoring differentials is less time consuming than restoring incrementals. Restoring incrementals requires the latest full backup and all incremental backups that were created since the full backup.</li> <li>■ Less time is required for backup and restore Differential backups take less time to restore than full backups. Faster recovery is possible in disaster situations because you only need the latest full and differential backup sets to fully restore a server.</li> </ul>	<ul style="list-style-type: none"> <li>■ Redundant backups All of the files that were created or modified since the last full backup are included; thus creating redundant backups.</li> </ul>

**Table 18-1** Backup method Advantages and Disadvantages (*continued*)

Method	Advantages	Disadvantages
Incremental	<ul style="list-style-type: none"> <li>■ Better use of storage Only the files that have changed since the last backup are included, so much less data storage space is required.</li> <li>■ Less time is required for backup Incremental backups take much less time than full and differential backups to complete.</li> </ul>	<ul style="list-style-type: none"> <li>■ Backups are spread across multiple backup sets Since multiple backup sets are required in a disaster situation, recovering a server can take longer. In addition, the backup sets must be restored in the correct order to effectively bring the system up to date.</li> </ul>

## About configuring Backup Exec to determine if a file has been backed up

Whenever a file is created or changed, a computer's file system notes and records the change. Computers can use a file's modified time, archive bit, or a Windows Change Journal to determine when a file is created or changed. If you use the incremental or the differential backup method as part of your backup strategy, Backup Exec must know when a file has been modified. Full backups include all of the data that you selected to back up. Subsequent incremental and differential backups back up only new files and any files that have changed.

See [“About backup methods”](#) on page 528.

Consider the following backup strategy scenario:

Fred wants to implement a backup strategy for the office file server. Fred knows that all backup strategies begin with a full backup (backup of an entire server using the full backup method). He creates and submits the backup job to run at the end of the day on Friday.

Most files on the server, such as operating system files and application files, seldom change. Therefore, Fred decides that he can save time and storage by using incremental or differential backups. Fred opts to use incremental backups. He schedules the job to run at the end of the day, Monday through Thursday, with the incremental backup method.

On Friday, Fred's backup sets contain all of the data on the file server. Backup Exec changes all of the files' statuses to backed up. At the end of the day on Monday, the incremental job runs and only the files that were created or changed are backed up. When the incremental job completes, Backup Exec turns off the

archive bit, showing that the files have been backed up. On Tuesday through Thursday, the same events happen.

If Fred's file server then crashed on Thursday, he would restore each backup in the order in which it was created. He would begin with Friday's backup and proceed through Wednesday's backup.

If Fred had decided to perform differential backups on Monday through Thursday, he would have only needed Friday's and Wednesday's backup sets. Friday's backup sets would have included all of the data from the original backup. Wednesday's backup sets would have included every file that had been created or changed since Friday's backup.

By default, Backup Exec uses the Windows Change Journal to determine if a file has been backed up. You can select another method if the Windows Change Journal is not available.

See "[Files and Folders options](#)" on page 204.

**Table 18-2** Methods to determine if a file has previously been backed up

Method	Description
By modified time	<p>Backup Exec uses the Windows Change Journal to determine if a file has changed since the last time it was backed up. If the Change Journal is not available, modified time is used.</p> <p>When Backup Exec runs a full backup or incremental backup, the time the backup launches is recorded in the Backup Exec Database. The next time you run an incremental or a differential backup, Backup Exec compares the file system time to the backup time from the Backup Exec Database. If the file system time is later than the database time, the file is backed up. If the file's modified time is older than the previous backup's modified time, that file is not backed up.</p> <p><b>Note:</b> A file's last modified date and timestamp does not change when the file is copied or moved. To ensure that the files are protected, run a full backup after you copy or you move files. If you have the Advanced Disk-based Backup Option, you can run synthetic backups to ensure that any copied or moved files are protected.</p> <p>When you run an incremental backup, Backup Exec records a new time in the Backup Exec Database. The database time is not updated with differential backups.</p> <p>Using modified time allows Backup Exec to run differential backups on the file systems that do not have an archive bit, such as UNIX.</p> <p>Backup Exec adds the time of the backup to the Backup Exec Database only if the full backup job completes successfully. If it does not complete successfully, subsequent differential or incremental backup jobs back up all of the data instead of only the data that changed.</p>

**Table 18-2** Methods to determine if a file has previously been backed up  
(continued)

Method	Description
Using archive bit	<p>Backup Exec uses the archive bit from the file system to determine if a file has changed since the last time it was backed up.</p> <p>When you choose to use the archive bit, Backup Exec turns the archive bit off when a file is backed up. Turning off the archive bit indicates to Backup Exec that the file has been backed up. If the file changes again before the next full or incremental backup, the bit is turned on again. Backup Exec backs up the file in the next full or incremental backup. Differential backups include only the files that were created or modified since the last full backup. When a differential backup is performed, the archive bit is left intact.</p>
Using catalogs	<p>Backup Exec uses the Windows Change Journal to determine if a file has changed since the last time it was backed up.</p> <p>Backup Exec compares path names, modified times, deleted and renamed files and folders, and other attributes. If the Change Journal is not available, Backup Exec compares the file information to previous Backup Exec catalogs to determine if it has changed. This method is required for synthetic backups and true image restore. It is the most thorough method, but it takes more time to run.</p>

## About backing up and deleting files

When you run a full backup, you can select to back up the files and then delete them. The **Delete selected files and folders after successful backup** option lets you free disk space on your server by deleting files and folders from the server after they are successfully backed up. Backup Exec backs up the selected data, verifies the backup sets, and then deletes the data from the server. You can back up and delete files for full backups only.

Because this option deletes data, you cannot configure it as a default backup job setting. You must configure this option in the **Files and Folders** backup job settings each time you want to use it for a job. You should not use this option as part of a regular backup schedule.

See [“Files and Folders options”](#) on page 204.

The credentials in the Backup Exec logon account that you use to run the job must have the rights to delete a file. To back up and delete files using the Agent for

Linux or the Agent for Macintosh, the Backup Exec logon account must have superuser privileges. Otherwise, the data is backed up, but is not deleted.

---

**Note:** Backup Exec does not delete data from remote computers on which Backup Exec agents are installed when you select the **Delete selected files and folders after successful backup** option.

---

Backup Exec performs a verify operation after the data is backed up. If the verify operation fails, the job stops and you are notified. If you get a verification failure, view the job log. Try to correct the problem, and then retry the job. After the data is backed up and verified, Backup Exec deletes the selected data. The job log contains a list of the data that is deleted.

You can enable the checkpoint restart option for a full backup job that uses the **Delete selected files and folders after successful backup** option. If the job fails and is resumed, the files are not deleted from the source volume after the backup completes.

The Backup Exec Archive Option offers more features for data archiving.

See [“About the Archiving Option”](#) on page 1198.

## About using fully qualified domain names in backup selections

You can enter fully qualified domain names in Backup Exec anywhere that you can enter a computer name. In addition, Backup Exec can show fully qualified domain names where computer names are listed.

For fully qualified domain names, the following rules apply:

- The maximum number of characters for each label (the text between the dots) is 63
- The maximum total number of characters in the fully qualified name is 254, including the dots, but excluding the \\
- The name cannot include the following characters: \* | < > ?

Symantec does not recommend using both fully qualified domain names and non-qualified domain names. Symantec recommends using fully qualified domain names.

For example, if you have a computer named Test\_Computer, you can have two selections for it. One selection is called Test\_Computer. The fully qualified selection is called Test\_Computer.domain.company.com. In this case, Backup Exec treats

each selection as a separate computer, even though both selections are for the same computer. For any backup jobs that use the short computer name, the catalog contains the short computer name. For any backup jobs that use the fully qualified name, the catalog contains the fully qualified name.

## About discovering data to back up

Backup Exec's **Discover Data to Back Up** option detects backup content within a Windows or Active Directory domain. The data discovery operation searches for server volumes, databases, or any application data that has not been backed up yet.

See [“Configuring Backup Exec to discover data to back up”](#) on page 469.

By default, the data discovery operation runs at noon every day. It also runs each time the Backup Exec services are restarted. Backup Exec cancels the operation if it is still running after four hours. You can disable the operation or change the default settings in the global Backup Exec settings.

See [“Discover Data to Back Up options”](#) on page 470.

The **Discover Data to Back Up** option performs three main tasks:

- Discovers any top-level computers or computer contents  
When the data discovery operation discovers top-level computers or computer contents, it adds them to the **Credentials** pane on the **Backup and Restore** tab. The operation updates any information about the computers or computer sources and their backup status. You can view information about backup sources on the **Credentials** pane.  
See [“Credentials properties”](#) on page 176.
- Discovers any servers that do not have an Agent for Windows installed on them  
If the operation discovers any servers that do not have an Agent for Windows installed on them, Backup Exec sends you an alert. You can add the servers to the list of servers by using the **Add a Server** Wizard. After you add the servers to the list of servers, you can back them up and monitor them.  
See [“Adding servers to the list of servers”](#) on page 158.
- Discovers and validates instances of the Agent for Windows  
The data discovery operation searches for any instances of the Agent for Windows on your network. When it finds an Agent for Windows, the operation checks the version to make sure that it is up to date. If an Agent for Windows is not up to date with the most recent version, Backup Exec sends you an alert.

The data discovery operation only discovers the servers that meet the following criteria:

- Belongs to the same domain as the Backup Exec server
- Has the Windows Management Instrumentation (WMI) service enabled and running
- Allows WMI access for the same user that the Backup Exec Management Service runs under  
Members of the server's "Administrators" group have this level of access.
- Has firewalls that are configured to allow WMI network traffic

## About using checkpoint restart

Checkpoint restart lets you restart jobs that are interrupted. The job restarts from the point where it was interrupted instead of starting over again at the beginning. Files that were already backed up are skipped and only the remaining files are backed up when the job restarts. Backup Exec gives restarted jobs a "Resumed" status. If checkpoint restart is not enabled, you must restart failed or interrupted jobs from the beginning. You can enable or disable checkpoint restart in the **Advance Open File** options when you create backup jobs.

See [“Advanced Open File options”](#) on page 199.

---

**Note:** Checkpoint restart cannot restart a backup job until it has backed up at least 32 MB of data. If a backup job fails before it has backed up at least that much data, you can run it again manually.

---

Checkpoint restart is enabled by default. Backup Exec waits two minutes after the error and then attempts to restart the job one time. You can modify the default checkpoint restart settings as error-handling rules.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

---

**Note:** If you use the Central Admin Server Option (CASO), any jobs that are restarted run on the same managed Backup Exec server on which the job failed. If the original Backup Exec server is not available, Backup Exec selects a different Backup Exec server on which to run the restarted job.

---

Checkpoint restart is only supported for NTFS volumes. The only type of snapshot technology that is supported for checkpoint restart is VSS.

Checkpoint restart is not supported for the following:

- FAT volumes
- FAT32 volumes

- UNIX computers
- Cluster Shared Volumes (CSV)
- Application agents
- Incremental backups
- Jobs that use catalogs to determine if a file has been backed up  
See “[About configuring Backup Exec to determine if a file has been backed up](#)” on page 532.

Backup Exec automatically cancels any jobs that run for too long according to the schedule settings that you selected when you created the job. If Backup Exec automatically cancels a job, it is not eligible to be restarted. If you manually cancel a job, Backup Exec does not automatically try to restart it.

You should consider the following things before you use checkpoint restart:

- If the failure occurs in the middle of an append job, the media is no longer appendable. The media is not appendable until it is erased, overwritten, or the retention period expires. When the restart occurs, Backup Exec uses new media. You should select an appropriate media overwrite protection level to ensure that the restart does not overwrite the media that was used before the job failure.
- If the failure occurs during a verify job or a database consistency check job, the job restarts at the beginning.
- Full backups that were interrupted and resumed from the point of failure do not display in the Simplified Disaster Recovery **Recover This Computer** Wizard. However, you can restore these backup sets manually after you make the initial recovery by using the **Recover This Computer** Wizard.
- You can enable the checkpoint restart option for a full backup job that uses the **Delete selected files and folders after successful backup** option. If the job fails and is resumed, the files are not deleted from the source volume after the backup completes.

## About backing up critical system components

Backup Exec is configured to automatically back up the critical system components that you need to perform a full system restore. Backing up critical system components ensures that you are capable of recovering your computers in the event of a disaster.

When all the critical system components are included in your backup job selections, the **Simplified Disaster Recovery** indicator on the selections pane reads **ON**. If

you deselect one or more critical system component files, the indicator changes to **OFF**.

You must include all critical system components in your backup selections if you intend to use any of the following restore scenarios:

- Simplified Disaster Recovery  
See [“About Simplified Disaster Recovery”](#) on page 704.
- Conversion to virtual  
See [“About conversion to virtual machines”](#) on page 437.
- Backup set to virtual
- Online disaster recovery  
See [“About performing a complete online restore of a Microsoft Windows computer”](#) on page 234.

When you select to back up a server, Backup Exec includes all of the server's system devices and application agents. Backup Exec dynamically discovers and protects all critical and non-critical system devices and application agents. You can explicitly include or exclude any non-critical devices or application data from the backup selections without affecting your ability to perform a full system restore. You can exclude Microsoft Exchange data from your backup, for example, and still use the backup sets to perform a disaster recovery.

The following system resources are considered critical, however. They must be included in backups if you want to be able to use the backup sets to perform a full system restore:

- System volume (including EFI and utility partitions)
- Boot volume (executing operating system)
- Services application volumes (boot, system, and automatic startup)
- System State devices and volumes (including Active Directory, System Files, etc.)

## About the Backup Exec Shadow Copy Components file system

The Backup Exec Shadow Copy Components file system uses Microsoft's Volume Shadow Copy Service to protect critical operating system and application service data, and third-party application and user data on Windows Server 2003/2008 computers.

Volume Shadow Copy Service allows a computer to be backed up while applications and services are running by providing a copy of a volume when a backup is initiated. Applications do not need to be shut down to ensure a successful volume backup. Volume Shadow Copy Service enables third party vendors to create snapshot plug-ins, or Writers, for use with this shadow copy technology.

A Writer is specific code within an application that participates in the Volume Shadow Copy Service framework to provide point-in-time, recovery-consistent operating system and application data. Writers appear as Shadow Copy Components, which are listed as data in backup and restore selections.

Only Writers that have been tested for use with Backup Exec are available for selection in the backup selections. Other Writers may be displayed in the selections, but they cannot be selected for backup.

If you select a volume that contains Shadow Copy data for backup, Backup Exec determines which Shadow Copy files should not be included in a volume level backup. These files will be automatically excluded for backup by a feature called Active File Exclusion. If this exclusion did not happen during a non-snapshot backup, these files would appear as in use - skipped. If this exclusion did not happen during a snapshot backup, the files would be backed up in a possible inconsistent state, which could create restore issues.

The Windows SharePoint Services feature pack utilizes a SQL (MSDE) instance called SHAREPOINT as a repository for shared information and collaboration data. On Windows Server 2003/2008, in the absence of a Symantec SQL Agent installation, the SQL SHAREPOINT instance can be protected by the Shadow Copy Components file system. If the SQL Agent is installed, then the SQL SHAREPOINT instance can be protected by the SQL Agent.

---

**Note:** If Windows SharePoint Services is installed using an instance name other than the default SHAREPOINT instance name, then it cannot be protected by the Shadow Copy Components file system. In that case, the Symantec SQL Agent must be used to protect the SQL SHAREPOINT instance.

---

Windows Small Business Server 2003 Standard and Premium contain a SQL (MSDE) instance called SBSMONITORING as a repository for server-related activity data. In the absence of a Symantec SQL Agent installation, the SQL SBSMONITORING instance can be protected by the Shadow Copy Components file system. If the SQL Agent is installed, then the SQL SBSMONITORING instance can be protected by the SQL Agent.

## About managing Microsoft Virtual Hard Disk (VHD) files in Backup Exec

Microsoft Windows 2008 R2 gives users the ability to create native Virtual Hard Disk (VHD) files. VHD files are virtual hard disks contained in a single file. For more information about VHD files, see your Microsoft Windows documentation.

Backup Exec gives you the ability to back up and restore native VHD files. If a native VHD file is not mounted, you can back up the volume on which it resides normally.

If a native VHD file is mounted to a drive letter or to an empty folder path, the file is skipped during backup jobs. You cannot include a mounted VHD as part of your backup selections. To back up the data in a mounted VHD file, select its mount point in the backup selections.

See [“About backing up data”](#) on page 155.

You can restore native VHD files as part of any normal restore job. You can also redirect a restore job to a native VHD if you use Microsoft Windows 2008 R2. When you redirect a restore job to a native VHD, Backup Exec creates a VHD file that expands dynamically as you save data to it. The file expands until it reaches 2040 GB, which is the maximum size for a native VHD file. You can create one VHD file with data from all redirected backup sets or you can create a VHD file for each backup set.

## About pre/post commands

You can set defaults for the commands you want to run before or after all backup jobs. If the default options are not appropriate for a particular job, you can override the default options when you create the job.

Conditions that you can set for these commands include the following:

- Run the backup job only if the pre-command is successful
  - Run the post-command only if the pre-command is successful
  - Run the post-command even if the backup job fails
  - Allow Backup Exec to check the return codes (or exit codes) of the pre- and post-commands to determine if the commands completed successfully
- If the pre- or post-command returns an exit code of zero, Backup Exec considers the job to have completed successfully. Backup Exec considers any non-zero exit codes to mean that the job encountered an error.

See [“Pre/post commands options”](#) on page 202.

If it is critical that the job does not run if the pre-command fails, configure Backup Exec to check the return codes. Backup Exec uses the return codes to determine if the pre-command failed or completed successfully.

For example, if a pre-command that shuts down a database before a backup is run fails, the database could be corrupted when the backup runs. In this situation, it is critical that the backup job does not run if the pre-command fails.

If Backup Exec is configured to check the return codes and the post-command returns a non-zero code, the job log reports that the post-command failed. You may have also selected to run the job only if the pre-command is successful. Even if both the pre-command and the job run successfully, Backup Exec marks the job as failed if the post-command fails.

For example, the pre-command can run successfully and shut down the database. The backup job can also run successfully. But if the post-command cannot restart the database, Backup Exec marks the job and the post-command as failed in the job log.

If you select the option **On each server backed up**, the pre- and post-command selections apply to each server independently. The pre- and post-commands are run and completed for one server at a time before they are run on the next selected server.

## How to restore individual items by using Granular Recovery Technology

You can use Granular Recovery Technology (GRT) to restore certain individual items from backup sets. For example, you can use the Agent for Microsoft Exchange Server to restore an email from a backup without having to restore the entire mailbox. Or, you can use the Agent for Microsoft SharePoint to restore a list without restoring the entire site.

To restore individual items, the Granular Recovery Technology feature must be enabled when you create a backup job.

GRT is enabled by default for backups for the following agents:

- Agent for Microsoft Active Directory
- Agent for Microsoft Exchange Server
- Agent for Microsoft SharePoint
- Agent for VMware and Hyper-V

You can restore either full backup sets or individual items from GRT-enabled backups.

By default, the Agent for VMware and Hyper-V uses Granular Recovery Technology to protect files and folders at a granular level. You can also enable the granular recovery of Microsoft Exchange, SQL, SharePoint, and Active Directory application data that resides on virtual machines.

When you enable granular recovery for Exchange or SharePoint backups, the catalog operation runs after the backup operation. The catalog operation runs once every 24 hours, even if you schedule more than one GRT-enabled backup job to run in the same period. Because the catalog operation runs at a different time, the GRT-enabled backup job does not block another scheduled GRT-enabled backup job from starting on time. When you view the server details, the catalog operation appears in the **Jobs** list and **Job History** separately from the backup operation. Separate backup and catalog operations for a GRT-enabled backup are not supported for Exchange and SharePoint databases that are on virtual machines.

The following table lists the individual items you can restore for each agent.

**Table 18-3** Individual items that can be recovered for each agent

Agent	Individual items
Agent for Microsoft Active Directory	You can restore the following individual items: <ul style="list-style-type: none"> <li>■ Active Directory objects and attributes</li> <li>■ Active Directory Application Mode (ADAM) and Active Directory Lightweight Directory Services (AD LDS) objects and attributes</li> </ul>
Agent for Microsoft Exchange Server	You can restore the following individual items: <ul style="list-style-type: none"> <li>■ Mailboxes</li> <li>■ Mail messages and their attachments</li> <li>■ Public folders</li> <li>■ Calendar items</li> <li>■ Contacts</li> <li>■ Notes</li> <li>■ Tasks</li> </ul>

**Table 18-3** Individual items that can be recovered for each agent (*continued*)

Agent	Individual items
Agent for Microsoft SharePoint	<p>The following are examples of the individual items that can be restored:</p> <ul style="list-style-type: none"> <li>■ Site collections</li> <li>■ Sites or subsites</li> <li>■ Document or picture libraries</li> <li>■ Lists</li> <li>■ Individual list items</li> <li>■ Documents, pictures, or other files that are stored in libraries</li> </ul>
Agent for VMware and Hyper-V	<p>You can restore drives, folders, and files from virtual machines that run a Windows operating system.</p> <p>You can also enable the granular recovery of Microsoft Exchange, SQL, SharePoint, and Active Directory application data that resides on virtual machines:</p> <p>See <a href="#">“How Backup Exec backs up Microsoft application data on virtual machines”</a> on page 788.</p>

When you run a GRT-enabled backup job, Backup Exec creates media with an IMG prefix (for example, IMG00001). IMG media is a specific media type that Backup Exec creates only for GRT-enabled backup operations. When you run a GRT-enabled backup job, the IMG media stores the backup data.

---

**Note:** Disk storage does not support encryption for GRT-enabled jobs.

---

You should consider which device you use for GRT-enabled backups before you begin. You should also consider any special requirements for the type of data you back up.

See [“Recommended devices for backups that use Granular Recovery Technology”](#) on page 545.

See [“About requirements for jobs that use Granular Recovery Technology”](#) on page 547.

## Recommended devices for backups that use Granular Recovery Technology

Symantec recommends that you select a disk storage device for any backups that are enabled for Granular Recovery Technology (GRT). The disk storage device

should be on a volume that does not have file size limitations. An NTFS drive is an example of a volume without file size limitations. Some examples of volumes that have file size limitations include FAT and FAT32 volumes.

If you must use a disk storage device on a volume with file size limitations, Backup Exec requires a staging location. Backup Exec temporarily stores a small amount of metadata in the staging location during the backup job. It deletes the data from the staging location when the backup is finished. The staging location is not necessary, however, if you use a disk storage device on a volume without file size limitations as the destination.

The staging location's default path is C:\temp.

The volume that is used for a staging location for backup jobs should meet the following requirements:

- It is local to the Backup Exec server
- It does not have any file size limitations

Additionally, Symantec recommends the following to avoid disk space problems:

- It should not be a system volume
- It should have at least 1 GB of available space

Backup Exec also uses a staging location to restore GRT-enabled data from a tape or from a disk storage device on volumes with file size limitations. The staging location must be on a volume that does not have file size limitations and is local to the Backup Exec server. The staging location is not necessary if you restore GRT-enabled data from disk storage on a volume without file size limitations, such as NTFS.

Backup Exec uses the staging area differently for the following types of restores:

**Table 18-4** Staging processes

Location of data to be restored	Staging process
Tape	<p>Backup Exec copies the entire backup set or sets to the staging area. The staging area must have enough disk space for the entire backup set or sets from which you want to restore an individual item.</p> <p>Before you use a tape device for a GRT-enabled backup, ensure that sufficient disk space is available to perform a restore.</p> <p>Backup Exec deletes the data from the staging area when the restore job is complete.</p>

**Table 18-4** Staging processes (*continued*)

Location of data to be restored	Staging process
Disk storage device that is on a volume with file size limitations (such as FAT or FAT32)	<p>Backup Exec must copy a small amount of metadata that is associated with the backup set to the staging area to complete the restore.</p> <p>Backup Exec deletes the data from the staging area when the restore job is complete.</p>

The staging location's default path is C:\temp. You can change the default backup and restore staging locations in the Backup Exec settings.

See [“About global Backup Exec settings”](#) on page 463.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“About requirements for jobs that use Granular Recovery Technology”](#) on page 547.

## About requirements for jobs that use Granular Recovery Technology

Keep in mind the following requirements when you use Granular Recovery Technology (GRT) with the agents listed:

**Table 18-5** Granular Recovery Technology requirements

Agent	Restrictions
Agent for Microsoft Active Directory	You can run only full backups for GRT-enabled jobs.
Agent for Microsoft Exchange Server	<p>Backup Exec must have access to a uniquely named mailbox within the Exchange organization for backup and restore of the Information Store.</p> <p>See <a href="#">“Requirements for accessing Exchange mailboxes”</a> on page 845.</p>
Agent for Microsoft SharePoint	You must have a current version of the Agent for Windows installed on all of the servers that participate in the SharePoint farm.

**Table 18-5** Granular Recovery Technology requirements (*continued*)

Agent	Restrictions
Agent for VMware and Hyper-V	You can recover only individual items to virtual machines that run a Windows operating system.  By default, the Agent for VMware and Hyper-V uses Granular Recovery Technology to protect files and folders at a granular level. You can also enable the granular recovery of Microsoft Exchange, SQL, SharePoint, and Active Directory application data that resides on virtual machines.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“Recommended devices for backups that use Granular Recovery Technology”](#) on page 545.

## About specifying backup networks

The backup network feature lets you direct any primary backup traffic that Backup Exec generates to a specific local network. Directing backup jobs to a specified local network isolates the backup data so that other connected networks are not affected when backup operations are performed. You also can use a backup network when you restore data. The feature is enabled on the Backup Exec server and lets you protect all the remote computers that reside on the specified local network.

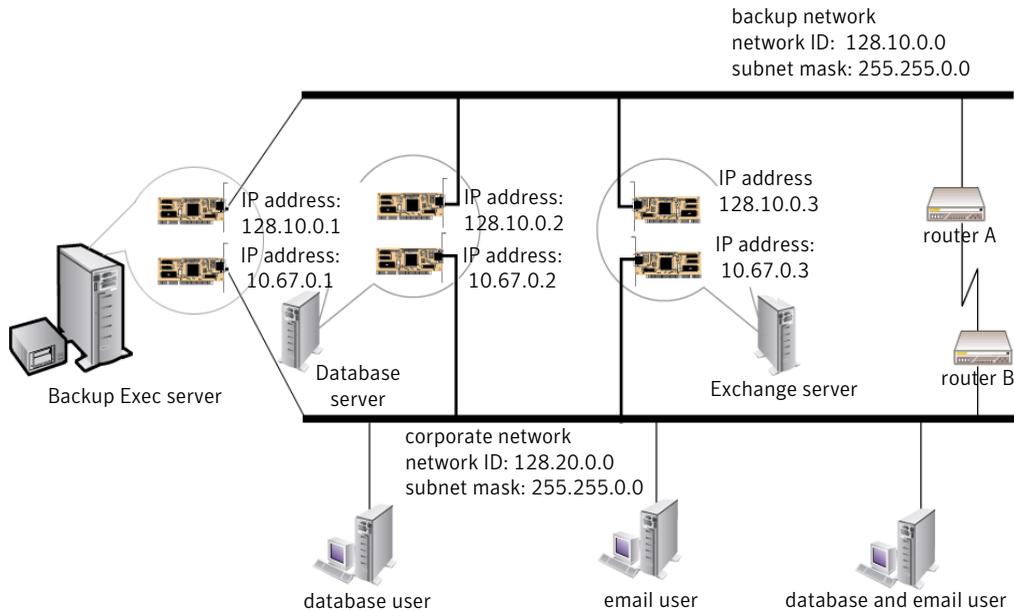
See [“Network options”](#) on page 195.

When you specify a backup network and submit a job, Backup Exec verifies that the remote computer is on the same subnet as the selected interface on the Backup Exec server. If the remote computer is on the selected subnet, then the backup operation is performed.

If the remote computer is not on the selected subnet, then the job fails. However, you can set up Backup Exec to use any available network to back up remote computers.

The following diagram shows an example of a backup network configuration.

**Figure 18-1** Example of backup network



In the example, the database server and mail server are connected to both the backup network and the corporate network.

When the Backup Exec server performs backup operations, the backup data uses either the backup network or the corporate network to back up the database server. If the backup data goes through the corporate network, the amount of time it takes to back up the database server increases. The amount of time increases because the network route between the two computers is longer. Users may experience network latencies when they access the mail server since there is an increase in network traffic.

In contrast, if you specify a backup network and you back up the database server, the backup data traffic is isolated to the backup network. Any users accessing the mail server are not affected. The backup network is used to perform all backup operations, unless the remote computer is not connected to the backup network.

To back up any remote computers that are not connected to the backup network, choose to use any available network route. Choosing any available network lets you back up the remote computer even though it does not reside on the backup network.

See [“About using Backup Exec with firewalls”](#) on page 472.

See [“Browsing systems through a firewall”](#) on page 474.

## About using IPv4 and IPv6 in Backup Exec

Backup Exec supports versions 4 and 6 of the Internet Protocol (IP), which are commonly referred to as IPv4 and IPv6. You can use IPv4 and IPv6 in backup and restore networks. Support for IPv6 is dependent upon operating system support for the protocol, as well as proper network configuration.

You can use Backup Exec in a mixed IPv4/IPv6 environment or an IPv4-only environment.

Enter an IPv4 or IPv6 address for a computer anywhere that you can enter a computer name in Backup Exec, except in the following locations:

- User-defined selections.
- Clusters. Microsoft Windows does not support an IPv6 address as a clustered computer.
- The Connect to Backup Exec Server dialog box.

A Backup Exec agent that supports IPv6 can be backed up or restored using IPv6 only from a Backup Exec server that is IPv6-compliant.

## About using Backup Exec with Symantec Endpoint Protection

You can use Symantec Endpoint Protection version 11.0 or later with Backup Exec to provide extra security when the threat of viruses or malware is high. Symantec Endpoint Protection uses a ThreatCon level to provide an overall view of global Internet security. Symantec's ThreatCon levels are based on a 1-4 rating system, with level 4 being the highest threat level.

You can find more information about Symantec ThreatCon levels at the following URL:

<http://www.symantec.com>

You can configure Backup Exec to automatically run a backup job when the ThreatCon reaches a level that you specify. You may want to configure special jobs for your most crucial data, for example. This strategy helps make sure that your vital data is safely backed up as soon as global threats are detected.

You should consider the types of jobs that you want to trigger automatically and the potential effect they can have on your system resources. The ThreatCon level is updated frequently and it can be raised at any time without warning. If you configure large or resource-intensive jobs to launch automatically, they may interfere with your normal business operations.

The Backup Exec server must be connected to the Internet to monitor the ThreatCon level. If the Backup Exec server is not connected to the Internet, backup jobs are not triggered when the ThreatCon level elevates.

See the *Administrator's Guide for Symantec Endpoint Protection* for more information about Symantec Endpoint Protection.

See [“Setting default backup job settings”](#) on page 456.

See [“Security options”](#) on page 201.

## About encryption

Backup Exec provides you with the ability to encrypt data. When you encrypt data, you protect it from unauthorized access. Anyone that tries to access the data has to have an encryption key that you create. Backup Exec provides software encryption, but it also supports some devices that provide hardware encryption with the T10 standard.

Backup Exec supports two security levels of encryption: 128-bit Advanced Encryption Standard (AES) and 256-bit AES. The 256-bit AES encryption provides a stronger level of security because the key is longer for 256-bit AES than for 128-bit AES. However, 128-bit AES encryption enables backup jobs to process more quickly. Hardware encryption using the T10 standard requires 256-bit AES.

See [“About software encryption”](#) on page 551.

See [“About hardware encryption”](#) on page 552.

See [“Encryption keys”](#) on page 552.

## About software encryption

When you install Backup Exec, the installation program installs encryption software on the Backup Exec server and on any remote computers that use a Backup Exec agent. Backup Exec can encrypt data at a computer that uses a Backup Exec agent, and then transfer the encrypted data to the Backup Exec server. Backup Exec then writes the encrypted data on a set-by-set basis to tape or to a backup-to-disk folder.

Backup Exec encrypts the following types of data:

- User data, such as files and Microsoft Exchange databases.
- Metadata, such as file names, attributes, and operating system information.
- On-tape catalog file and directory information.

Backup Exec does not encrypt Backup Exec metadata or on-disk catalog file and directory information.

You can use software compression with encryption for a backup job. First Backup Exec compresses the files, and then encrypts them. However, backup jobs take longer to complete when you use both encryption compression and software compression.

Symantec recommends that you avoid using hardware compression with software encryption. Hardware compression is performed after encryption. Data becomes randomized during the encryption process. Compression does not work effectively on data that is randomized.

See “[About encryption](#)” on page 551.

## About hardware encryption

Backup Exec supports hardware encryption for any storage devices that use the T10 encryption standard. When you use hardware encryption, the data is transmitted from the host computer to the target device and then encrypted on the device. Backup Exec manages the encryption keys that are used to access the encrypted data.

Backup Exec only supports approved devices for T10 encryption.

You can find a list of compatible devices at the following URL:

<http://entsupport.symantec.com/umi/v-269-2>

See “[About encryption](#)” on page 551.

## Encryption keys

You can set a default encryption key to use for all backup jobs. However, you can override the default key for a specific backup job. When you run a duplicate backup job, any backup sets that are already encrypted are not re-encrypted. However, you can encrypt any unencrypted backup sets.

If you use encryption for synthetic backups, all of the associated backups must use the same encryption key. Do not change the encryption key after the baseline is created. The encryption key that you select for the baseline backup is automatically applied to all associated backups.

When you select encrypted data for restore, Backup Exec verifies that encryption keys for the data are available in the database. If any of the keys are not available, Backup Exec prompts you to recreate the missing keys. If you delete the key after you schedule the job to run, the job fails.

If Backup Exec cannot locate an encryption key while a catalog job is running, Backup Exec sends an alert. You can then recreate the missing encryption key if you know the pass phrase.

If you use encryption keys with the Simplified Disaster Recovery option, special considerations apply.

See [“About encrypted backup sets and the Recover This Computer Wizard”](#) on page 720.

See [“About encryption”](#) on page 551.

See [“Setting default backup job settings”](#) on page 456.

See [“About encryption key management”](#) on page 477.

## About restricted keys and common keys in encryption

Backup Exec has the following types of encryption keys:

**Table 18-6** Types of encryption keys

Key type	Description
Common	Anyone can use the key to encrypt data during a backup job and to restore encrypted data.
Restricted	Anyone can use the key to encrypt data during a backup job, but users other than the key owner must know the pass phrase. If a user other than the key owner tries to restore the encrypted data, Backup Exec prompts the user for the pass phrase. If you cannot supply the correct pass phrase for the key, you cannot restore the data.

## About pass phrases in encryption

Encryption keys require a pass phrase, which is similar to a password. Pass phrases are usually longer than passwords and are comprised of several words or groups of text. A good pass phrase is between 8 and 128 characters. The minimum number of characters for 128-bit AES encryption is eight. The minimum number of characters for 256-bit AES encryption is 16. Symantec recommends that you use more than the minimum number of characters.

---

**Note:** Hardware encryption that uses the T10 standard requires 256-bit AES. Backup Exec does not let you enable hardware encryption for a job unless it uses at least a 16-character pass phrase.

---

Also, a good pass phrase contains a combination of upper and lower case numbers, letters, and special characters. You should avoid using literary quotations in pass phrases.

A pass phrase can include only printable ASCII characters, which are characters 32 through 126. ASCII character 32 is the space character, which is entered using the space bar on the keyboard. ASCII characters 33 through 126 include the following:

!"#\$%&'()\*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNPOQRSTUVWXYZ

[]^\_`abcdefghijklmnopqrstuvwxyz{|}~

See “[About encryption key management](#)” on page 477.

# Reports

This chapter includes the following topics:

- [About reports in Backup Exec](#)
- [About report groups](#)
- [Viewing the list of available reports in a report group](#)
- [Running a report](#)
- [Saving a report](#)
- [Printing a report from the Backup Exec Report Viewer](#)
- [Additional settings for standard reports](#)
- [Viewing a scheduled report](#)
- [Editing a scheduled report](#)
- [Copying a custom report](#)
- [Re-running a completed report](#)
- [Deleting a custom or scheduled report](#)
- [About scheduling report jobs and setting notification recipients](#)
- [About custom reports in Backup Exec](#)
- [Creating a custom report](#)
- [Copying custom reports](#)
- [Editing custom reports](#)
- [Deleting custom reports](#)

- [Editing application settings for reports](#)
- [Viewing report properties](#)
- [Report properties](#)
- [Available reports](#)

## About reports in Backup Exec

Backup Exec includes standard reports that show detailed information about your system. When generating many of the reports, you can specify settings that serve as filter parameters or a time range for the data that you want to include in the report. You can then run and view the report immediately, or you can create a new scheduled report job that saves the report data in the **See Upcoming** report group. You can also view general properties for each report.

Backup Exec also provides the following:

- The ability to schedule a report to run at a specified time or to specify a recurring schedule for the report to run.
- The ability to have Backup Exec distribute reports through notification.

To run reports across multiple Backup Exec servers, you must install the Backup Exec Enterprise Server Option, even if you are not operating in a shared storage environment.

Reports can be viewed and printed in the following formats:

- PDF
- HTML
- XML
- Microsoft Excel (XLS)
- Comma Separated Value (CSV)

To properly format integrated Backup Exec reports, you must configure a default printer using the Windows Control Panel Printers applet. This is required even if you do not have a printer attached to your system.

For information on configuring a printer by using the Windows Control Panel Printers applet, see your Microsoft Windows documentation.

See [“Viewing the list of available reports in a report group”](#) on page 558.

See [“Running a report”](#) on page 558.

See [“About scheduling report jobs and setting notification recipients”](#) on page 566.

See [“Available reports”](#) on page 589.

## About report groups

Reports are organized under the **Reports** tab, in groupings listed under **Report Groups**.

The following table describes report groups:

**Table 19-1** Report groups

<b>Report group</b>	<b>Description</b>
<b>See Completed</b>	Contains scheduled reports that have completed running.  You can view the report again by double-clicking the report name.
<b>See Upcoming</b>	Contains reports that have been scheduled to run on a specific date and at a specific time.
<b>Custom</b>	Contains custom reports that you have created by using <b>New Custom Report</b> .
<b>Archive</b>	Contains the reports that provide information about the Backup Exec activities that are related to the Backup Exec Archiving Option.
<b>Configuration</b>	Contains the reports that provide information about configuration changes and statuses of Backup Exec features and options.
<b>Jobs</b>	Contains the reports that provide information about various Backup Exec job-related activities.
<b>Media</b>	Contains the reports that provide information about the various types of media that Backup Exec uses.
<b>Devices</b>	Contains the reports that provide information about the various types of devices that Backup Exec uses.

**Table 19-1** Report groups (*continued*)

Report group	Description
Alerts	Contains the reports that provide historical information about the alerts that Backup Exec generates.

## Viewing the list of available reports in a report group

Use the following steps to view the list of available reports in each of the report groups.

See [“Available reports”](#) on page 589.

### To view the list of available reports in a report group

- 1 On the **Reports** tab, under **Report groups**, click a report group.
- 2 To sort the list of available reports, click the column heading on which you want to sort.

## Running a report

When you run a report, you can specify the criteria that is used to determine the items that will be included in the report. The settings, or parameters, available for you to select depend on the type of data that can be included in the report. After the report is generated, only the items that match the criteria appear in the report.

See [“Saving a report”](#) on page 559.

See [“Printing a report from the Backup Exec Report Viewer”](#) on page 560.

See [“About scheduling report jobs and setting notification recipients”](#) on page 566.

See [“Available reports”](#) on page 589.

### To run a report

- 1 From the **Reports** tab, under **Report Groups**, click the report group for the report you want to run.
- 2 Right-click the report you want to run, and then click **Run Now**.

- 3 If the **Run Report Now - <report\_name>** properties page appears, select the appropriate settings, or filter parameters, for the data you want to include in the report, and then click **OK**.

Only filter parameters that are available for a report appear. Select the appropriate options.

See [“Additional settings for standard reports”](#) on page 561.

The report appears and displays data based on the criteria you set when you ran the report.

- 4 After you have finished viewing the report, click **Close**.

Backup Exec automatically deletes the report when you close the Report Viewer.

## Saving a report

Use the following steps to save a report.

See [“Printing a report from the Backup Exec Report Viewer”](#) on page 560.

### To save a report

- 1 On the report, in the Report Viewer, click **Save As**.
- 2 When prompted, enter the file name and location where you want to save the report.
- 3 In the **Save as type** box, select a format in which to save the report.  
When you save a report in HTML format, both the HTML file and a .GIF image file are saved.
- 4 Click **Save**.

## Saving a scheduled report to a new location upon completion

You can specify a location where a scheduled report that has run is saved. Backup Exec saves both the images and report pages that enable you to view the saved report.

See [“Printing a report from the Backup Exec Report Viewer”](#) on page 560.

### To save a scheduled report to a new location upon completion

- 1 From the **Reports** tab, under **Report Groups**, click **See Completed**.
- 2 Double-click a completed report that you want to save to a new location.

- 3 Click **Save As**.
- 4 Enter the file name and location where you want to save the report and then click **Save**.

## Printing a report from the Backup Exec Report Viewer

You can print reports from a locally-attached printer or a network printer. To print a report, the printer must be configured to print in the landscape mode.

See [“Saving a report”](#) on page 559.

See [“Printing a report that is saved in PDF format”](#) on page 560.

See [“Printing a report that is saved in HTML format”](#) on page 561.

### To print a report from the Backup Exec Report Viewer

- 1 Run a report.  
See [“Running a report”](#) on page 558.
- 2 On the **Report Viewer**, click **Print**.
- 3 Read the message about printing options and then click **OK**.
- 4 Select a printer from the Windows **Print** dialog box.
- 5 Click **Print**.

## Printing a report that is saved in PDF format

Use the following steps to print a report that you saved in PDF format.

---

**Note:** You must have the Adobe Reader installed on the computer where you want to print a report that you saved in PDF format.

---

See [“Printing a report that is saved in HTML format”](#) on page 561.

See [“Saving a report”](#) on page 559.

### To print a report that is saved in PDF format

- 1 Navigate to the folder where you saved the report in PDF format.
- 2 Open the report by double-clicking the report's PDF icon.
- 3 From the Adobe Reader menu bar, click **File > Print**.

## Printing a report that is saved in HTML format

Use the following steps to print a report that you saved in HTML format.

See [“Printing a report that is saved in PDF format”](#) on page 560.

See [“Saving a report”](#) on page 559.

### To print a report that is saved in HTML format

- 1 Navigate to the location where you saved the HTML report.
- 2 Double-click the folder name of the report that you saved.
- 3 Right-click the HTML file named <name of report>\_.htm.  
 For example, Media Required for Recovery.htm
- 4 On the shortcut menu, click **Print**.
- 5 Select a printer from the Windows **Print** dialog box.
- 6 Click **Print**.

## Additional settings for standard reports

You can set additional report settings when you run a report or create a new report job.

---

**Note:** Only settings that are available for a report appear.

---

See [“Running a report”](#) on page 558.

The following table describes the settings you can set for a report:

**Table 19-2** Additional settings for standard reports

Item	Description
<b>Media sets</b>	<p>Filters the report based on media set names. Media sets include all the media that is inserted into the storage device.</p> <p>Options include the following:</p> <ul style="list-style-type: none"> <li>■ Backup Exec and Windows NT Backup Media</li> <li>■ Cleaning Media</li> <li>■ Foreign Media</li> <li>■ Keep Data for 4 Weeks</li> <li>■ Keep Data Infinitely - Do Not Allow Overwrite</li> <li>■ Retired Media</li> <li>■ Scratch Media</li> </ul>
<b>Backup Exec servers</b>	<p>Filters the report based on Backup Exec server names. The Backup Exec server is the server on which Backup Exec is installed. This setting is only available if the Enterprise Server Option is installed.</p>
<b>Job status</b>	<p>Filters the report based on job status.</p>
<b>Backed up servers</b>	<p>Filters the report based on specific backed up server names. A backed up server is the server that is being backed up.</p>
<b>Vault</b>	<p>Filters the report based on specific vault names. A media vault is a virtual representation of the actual physical location of media.</p> <p>See <a href="#">“About media vaults”</a> on page 384.</p>

**Table 19-2** Additional settings for standard reports (*continued*)

Item	Description
<b>Ranges</b>	<p>Filters the report based on the time range for the data that you want to include in the report. If range parameters are not available for a report, you will not be able to select the parameter.</p> <p>Range parameters or options available include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Days.</b> Enables the date filter. <ul style="list-style-type: none"> <li>- <b>Number of days before the day the report runs.</b> Specifies the number of days prior to the current day to begin the filter process on the data to be included in the report. You can enter a minimum of 0 and a maximum of 32,000 days.</li> <li>- <b>Number of days after the day the report runs.</b> Specifies the number of days after the current day to begin the filter process on the data to be included in the report. You can enter a minimum of 0 and a maximum of 32,000 days.</li> </ul> </li> <li>■ <b>Hours.</b> Enables the hours filter. <ul style="list-style-type: none"> <li>- Number of hours within time report. Specifies the number of hours either before or after the present hour to filter the data to be included in the report. The time frame depends on the type of report. You can enter a minimum of 0 and a maximum of 32,000 hours.</li> </ul> </li> <li>■ <b>Event count.</b> Enables the event count filter. <ul style="list-style-type: none"> <li>- Maximum number of events to include. Specifies the number of events to include in the report. Events generate alerts and originate from one of the following sources: system, job, media, or device. You can enter a minimum of 0 and a maximum of 32,000 events. Entering a value of zero for the range parameter does not limit the amount of data included in the report; this can result in an extensive report.</li> </ul> </li> </ul>

## Viewing a scheduled report

The reports that finish running based on a schedule appear in the **See Completed** report group.

To view the completed reports, use the following steps.

See [“Saving a report”](#) on page 559.

See [“Editing a scheduled report”](#) on page 564.

See [“Re-running a completed report”](#) on page 565.

See [“Copying a custom report”](#) on page 564.

See [“Deleting a custom or scheduled report”](#) on page 565.

**To view a report a scheduled report**

- 1 On the **Reports** tab, under **Report Groups**, click **See Completed**.
- 2 Double-click the report that you want to view.

## Editing a scheduled report

Use the following steps to edit the properties of a scheduled report before it runs.

See [“Viewing a scheduled report”](#) on page 563.

See [“Re-running a completed report”](#) on page 565.

See [“Copying a custom report”](#) on page 564.

See [“Deleting a custom or scheduled report”](#) on page 565.

**To edit a scheduled report**

- 1 On the **Reports** tab, under **Report Groups**, click **See Upcoming**.
- 2 Right-click a report you want to edit, and then click **Edit**.
- 3 Edit the report properties and then click **OK**.

## Copying a custom report

You can make one or more copies of a custom report. Each copy of the custom report resides in the Custom report group, along with the original custom report.

See [“Viewing a scheduled report”](#) on page 563.

See [“Editing a scheduled report”](#) on page 564.

See [“Deleting a custom or scheduled report”](#) on page 565.

Use the following steps to copy a custom report.

**To copy a custom report**

- 1 On the **Reports** tab, under **Report Groups**, click **Custom**.
- 2 Right-click a custom report that you want to copy, and then click **Copy**.
- 3 Type a name for the report, and then click **OK**.

The copy of the custom report appears in the **Custom** report group.

## Re-running a completed report

You can run reports that appear in the **See Completed** report group multiple times.

See [“Viewing a scheduled report”](#) on page 563.

See [“Editing a scheduled report”](#) on page 564.

See [“Copying a custom report”](#) on page 564.

See [“Deleting a custom or scheduled report”](#) on page 565.

To re-run a completed report, use the following steps.

### To re-run a completed report

- 1 On the **Reports** tab, under **Report Groups**, click **See Completed**.
- 2 Right-click a report, and then click **Retry Report Now**.  
Backup Exec creates and runs another iteration of the report.
- 3 To view the report again, double-click the new report.

## Deleting a custom or scheduled report

Reports that you create using the **Run now** option are automatically deleted after you view the report. However, custom reports or scheduled reports can be deleted at your convenience.

---

**Note:** Default Backup Exec reports cannot be deleted.

---

Use the following steps to delete a report.

See [“Viewing a scheduled report”](#) on page 563.

See [“Editing a scheduled report”](#) on page 564.

See [“Copying a custom report”](#) on page 564.

### To delete a report

- ◆ Under **Report Groups**, do one of the following:

To delete a custom report

Do the following in the order listed:

- Click **Custom**.
- Right-click a custom report, and then click **Delete**.

To delete a schedule report

Do the following in the order listed:

- Click **See Upcoming**.
- Right-click a scheduled report, and then click **Delete**.

To delete a completed report

Do the following in the order listed:

- Click **See Completed**.
- Right-click a completed report, and then click **Delete**.

## About scheduling report jobs and setting notification recipients

You can create a report job and schedule it to run at a specific time or specify a recurring schedule for a report to run. After you schedule the report to run, the report resides in **See Upcoming**, under **Report Groups** until it runs. After the report runs, Backup Exec moves the report into the report group named **See Completed**.

You can edit or delete any report that is found in the report group, **See Upcoming** by right-clicking the report name. You can also override the defined schedule and run the report immediately.

See [“Running a report”](#) on page 558.

See [“Schedule options”](#) on page 188.

You can also assign notification recipients to the report job just as you would for other Backup Exec jobs, such as backups and restores.

See [“Configuring an individual recipient for alert notifications”](#) on page 293.

## About custom reports in Backup Exec

You can create reports that contain information to meet the specific requirements of your organization. You choose the data to include in the report, and then determine how the data is filtered, sorted, and grouped. In addition, you can set up pie graphs and bar graphs to graphically represent the report data.

You can customize the look of the reports by doing the following:

- Adding a customized logo to the report
- Changing the color of the banner

- Adding text to the footer

See [“Creating a custom report”](#) on page 567.

## Creating a custom report

You can create reports that contain information to meet the specific requirements of your organization.

### To create a custom report

- 1 On the **Reports** tab, click **New Custom Report**.
- 2 On the **Custom Report** dialog box, type a name and description for the report.
- 3 If you do not want this report to include the default header and footer settings, uncheck **Use header and footer settings specified in Backup Exec Settings**.
- 4 In the left pane, click **Field Selection**.
- 5 In the **Category** box, select a group for which for which you want to create a report.

See [“Available groups from which to select fields for custom reports”](#) on page 579.

- 6 For additional field selections, click **Show advanced fields**.
- 7 Select the fields that you want on the report.  
 See [“Field selection options for custom reports”](#) on page 569.
- 8 To adjust the width of the column for a field, do the following in the order listed:
  - Click the field name in the **Fields selected for the report** list.
  - In the **Column width** box, type the new width.
  - Click **Set**.
- 9 Do any of the following:

To set filter criteria for the report	In the left pane, click <b>Filters</b> . See <a href="#">“Setting filters for custom reports”</a> on page 574.
---------------------------------------	---

To group fields for the report	Do the following in the order listed: <ul style="list-style-type: none"> <li>■ In the left pane, click <b>Grouping</b>.</li> <li>■ Complete the appropriate grouping options. See <a href="#">“About grouping fields in custom reports”</a> on page 577.</li> </ul>
--------------------------------	---

- To sort fields for the report

Do the following in the order listed:

  - In the left pane, click **Sorting**.
  - Complete the appropriate sorting options.  
 See [“Sort options for custom reports”](#) on page 580.
- To set graph options for the report

Do the following in the order listed:

  - In the left pane, click **Graph Options**.
  - Complete the appropriate graphing options.  
 See [“Graph options for custom reports”](#) on page 582.
- To preview the report

In the left pane, click **Preview**.
- To finish and close the report

Click **OK**.

## Custom report name and description options

You can give a report that you create a unique name. You can also enter a detailed description of the report.

See [“Creating a custom report”](#) on page 567.

**Table 19-3** Custom report name and description options

Item	Description
<b>Name</b>	Indicates a unique name for the report. All custom reports must be named.
<b>Description</b>	Indicates the description of the report.
<b>Use header and footer settings specified in Backup Exec Settings</b>	<p>Enable this option to display header and footer information in custom reports.</p> <p>This option uses the default header and footer settings that you specified for all reports.</p> <p>Click the Backup Exec button, select <b>Configuration and Settings</b>, select <b>Backup Exec Settings</b>, and then select <b>Reports</b>.</p> <p>See <a href="#">“Editing application settings for reports”</a> on page 586.</p>

## Field selection options for custom reports

Select the fields that you want to include in the report. Fields are displayed in the order you place them in the **Fields selected for the report** box. All fields are positioned horizontally, from left to right. The first field in the list appears on the left side of the report.

See [“Creating a custom report”](#) on page 567.

**Table 19-4** Field selection options

Item	Description
<b>Catagory</b>	<p>Lets you select fields for a custom report that are based on Backup Exec functionality. Field categories include the following:</p> <ul style="list-style-type: none"> <li>■ Alerts Group</li> <li>■ Device Group</li> <li>■ Job Group</li> <li>■ Job History Group</li> <li>■ Media Group</li> </ul> <p>See <a href="#">“Available groups from which to select fields for custom reports”</a> on page 579.</p>
<b>Available fields</b>	<p>Shows the list of available fields for each category.</p> <p>By default, Backup Exec displays only the basic fields for each category. The basic fields include those fields that are most likely to be used in a report. To show all available fields, check <b>Show advanced fields</b></p> <p>To select consecutive fields, click the first item, press and hold SHIFT, and then click the last item. To randomly select fields, press and hold CTRL, and then click each item.</p> <p>To move the selected fields to the <b>Fields selected for the report</b> box, click &gt;&gt;.</p>

**Table 19-4** Field selection options (*continued*)

Item	Description
<b>Fields selected for the report.</b>	<p>Shows the fields that are selected for display on the report.</p> <p>Fields are displayed on the report based on the order in which they appear in the box titled <b>Fields selected for the report</b>. The first field in the list appears on the left side of the report.</p> <p>Click <b>Move UP</b> or <b>Move Down</b> to reposition the fields on the report.</p> <p>To remove a field, double click the item.</p>

## About filter criteria and filter expressions for custom reports

Filters let you customize reports to include only the information that meets specific criteria.

For example, you can use filters to find the following:

- Jobs that contain a specific word
- Alerts that occurred on a specific day
- Media that are in a specific location

You use filter criteria to create filter expressions. You can use one or multiple filter expressions. A filter expression consists of a field name, an operator, and a value.

The following filter expression finds all alerts for errors:

**Table 19-5** Filter expression for finding alerts for errors

Filter type	Data
<b>Field name</b>	Alert Type
<b>Operator</b>	= (Equal)
<b>Value</b>	Errors

If you want the report to include only alerts for errors that occurred on a specific day, add another filter expression for the date and time.

The following filter expression finds alerts on a specific day:

**Table 19-6** Filter expression for finding alerts on a specific day

Filter type	Data
Field name	Date Entered
Operator	=(Equal)
Value	06/03/2011   <time>

See [“Filter expressions for defining custom reports”](#) on page 571.

See [“Setting filters for custom reports”](#) on page 574.

See [“About grouping fields in custom reports”](#) on page 577.

See [“About sorting fields in custom reports”](#) on page 579.

See [“Setting graph options in custom reports”](#) on page 581.

## Filter expressions for defining custom reports

You can create a filter by defining one or more filter expressions

See [“Setting filters for custom reports”](#) on page 574.

**Table 19-7** Filter expressions for defining custom reports

Item	Description
Show advanced fields	Check <b>Show advanced fields</b> to see all of the fields that are available for filtering. By default, only the most common fields display.
Field name	Select the field on which you want to filter.

**Table 19-7** Filter expressions for defining custom reports (*continued*)

Item	Description
Operator	

**Table 19-7** Filter expressions for defining custom reports (*continued*)

Item	Description
	<p>Select the appropriate operator for this filter. Operators determine how the field name and the value are linked. The following operators are available in Backup Exec, but the list that displays varies depending on the type of field you selected in Field name:</p> <ul style="list-style-type: none"> <li>■ = (Equal). The field name must equal the value.</li> <li>■ &lt;&gt; (Not Equal). The field name must not equal the value.</li> <li>■ &gt; (Greater Than). The field name must be larger than the value.</li> <li>■ &gt;= (Greater Than or Equal). The field name must be larger than or equal to the value.</li> <li>■ &lt; (Less Than). The field name must be smaller than the value.</li> <li>■ &lt;= (Less Than or Equal). The field name must be smaller or equal to the value.</li> <li>■ \$ (Contains). The field name contains the text entered in the Value field.</li> <li>■ NOT\$ (Contains). The field name does not contain the text entered in the Value field.</li> <li>■ IN LAST. A date or time window that is relative to the time that you create the report. This operator defines dates and times prior to the time when the report is created. This operator is available only for date and time fields.</li> </ul> <p>If you enter hours in the Value field you receive more specific results than if you enter days. The Day value is calculated beginning at midnight (00:00) yesterday and ending at the time when the report runs.</p> <p>For example, if you enter 1 day in the Value field and the report runs at 23:59 today, the report includes results for the last 47 hours and 59 minutes. However, if you enter 24 hours, you receive information for exactly 24 hours prior to</p>

**Table 19-7** Filter expressions for defining custom reports (*continued*)

Item	Description
	<p>the time when the report runs.</p> <ul style="list-style-type: none"> <li>■ IN NEXT. A date or time window that is relative to the time that you create the report. This operator defines dates and times after the time when the report is created. For example, to find backup jobs that are scheduled to occur during the next three days, select this operator, and then enter 3 days in the Value field. This is available only for date and time fields.</li> </ul>
<b>Value</b>	<p>Type or select the value on which you want to filter. The type of value that you can enter varies depending on the type of field name that you select. For example, if you select Next Due Date in the Field name, Backup Exec displays date and time values.</p>

## Setting filters for custom reports

Use the following steps to set filters for custom reports that you want to create.

### To set filters for custom reports

- 1 On the Reports tab, under **Report groups**, click **Custom Reports**.
- 2 In the reports list, right-click the report that you want to filter and then click **Edit**.
- 3 In the left pane, click **Filters**.
- 4 Create a filter by defining one or more filter expressions.  
 See [“Filter expressions for defining custom reports”](#) on page 571.
- 5 Click **Add**.
- 6 Repeat steps 4 and 5 to add more filters.
- 7 To combine sets of filter expressions, do any of the following:

To combine two filter expressions so that both expressions must be true for the result to be true

Click **AND**.

For example, to find all backup jobs that failed, add the following expressions:

- Status = Failed
- Type = Backup

After you set up the expressions, do the following:

- Click **AND** to combine the two expressions.

The combined expression is:

Status = Failed AND Type = Backup

To combine two filter expressions so that one of the expressions must be true for the result to be true

Click **OR**.

For example, to find jobs that either failed or were canceled, add the following expressions:

- Status = Failed
- Status = Canceled

After you set up the expressions, do the following:

- Click **OR** to combine Status = Failed with Status = Canceled.

The combined expression is:

Status = Failed OR Status = Canceled

To combine two filter expressions into a single expression

Click **() +**

For example, to find backup jobs and restore jobs that failed, add the following expressions:

- Status = Failed
- Type = Backup
- Type = Restore

After you set up the expressions, do the following:

- Use **OR** to combine Type = Backup with Type = Restore.
- Press and hold **Ctrl** while you click Type = Backup and Type = Restore.
- Click **() +** to combine Type = Backup with Type = Restore.
- Use **AND** to combine Status = Failed with (Type = Backup OR Type = Restore).

The combined expression is:

Status = Failed AND (Type = Backup OR Type = Restore)

To separate two filter expressions that were combined into a single expression

Click **()** -

For example, if you used **() +** to combine **Type = Backup** with **Type = Restore**, it is displayed on the Filters dialog box like this:

**(Type = Backup OR Type = Restore)**

To make the combined expression into two individual expressions, do the following:

- Press and hold **Ctrl** while you click both **Type = Backup** and **Type = Restore**.
- Click **()** -

After you separate the expressions, they are displayed without the parentheses.

- 8 To change any of the expressions, do the following in the order listed:
  - In the Filter criteria box, select the expression that you want to change.
  - Click **Edit**.
  - In the Filter expression area, edit the expression's values.
  - Click **Update**.
- 9 To remove an expression, select the expression, and then click **Remove**.
- 10 Do any of the following:

To group fields for the report

Do the following in the order listed:

- In the left pane, click **Grouping**.
- Complete the appropriate grouping options.  
See [“Grouping options for custom reports”](#) on page 578.

To sort fields for the report

Do the following in the order listed:

- In the left pane, click **Sorting**.
- Complete the appropriate sorting options.  
See [“Sort options for custom reports”](#) on page 580.

To set graph options for the report

Do the following in the order listed:

- In the left pane, click **Graph Options**.
- Complete the appropriate graphing options.  
See [“Graph options for custom reports”](#) on page 582.

To preview the report

In the left pane, click **Preview**.

To finish and close Click **OK**.  
the report

## About grouping fields in custom reports

You can group a custom report by up to three of the fields that you have chosen for the report. Grouping fields creates sections on the report. For example, if you group by Backup Exec server, Backup Exec creates a section for each Backup Exec server that matches the filter criteria. Under each Backup Exec server's section, the report displays the data that corresponds to the remaining fields that you selected for the report.

A report must have at least one field that is not grouped. For example, if you select three fields in the report, you can group only two of the fields. If you group all of the fields, no data appears on the report because all of the data is listed in the group section titles. In addition, you must have at least four fields on the report to use all three grouping fields.

After you select a field on which to group the report, you can group the data for that field in ascending or descending order. Ascending order lists numbers from smallest to largest and lists letters in alphabetical order. Descending order lists numbers from largest to smallest and lists letters in reverse alphabetical order. For example, if you group by a date field in ascending order, the report data is grouped by date, starting with the earliest date.

See [“Grouping fields in custom reports”](#) on page 577.

### Grouping fields in custom reports

Use the following steps to group fields in custom reports.

See [“About grouping fields in custom reports”](#) on page 577.

#### To group fields in custom reports

- 1 On the **Reports** tab, under **Report Groups**, click **Custom**.
- 2 In the list of custom reports, right-click the report that contains the fields you want to group, and then select **Edit**.
- 3 In the left pane, click **Grouping**.
- 4 Select the appropriate options.  
See [“Grouping options for custom reports”](#) on page 578.
- 5 In the **Group by** box, select the name of the field on which you want to group data.

- 6 Click **Ascending** to group the information in ascending order or click **Descending** to group the information in descending order.
- 7 If you want to group on additional fields, in the **Then group by** box, repeat step 5 and step 6.
- 8 Do any of the following:

To sort fields for the report      Do the following in the order listed:

- In the left pane, click **Sorting**.
- Complete the appropriate sorting options.  
 See [“About sorting fields in custom reports”](#) on page 579.

To set graph options for the report      Do the following in the order listed:

- In the left pane, click **Graph Options**.
- Complete the appropriate graphing options.  
 See [“Setting graph options in custom reports”](#) on page 581.

To preview and test the report      In the left pane, click **Preview**.

To finish and close the report      Click **OK**.

## Grouping options for custom reports

You can group report information in ascending or descending order based on the fields that you selected for the report.

See [“About grouping fields in custom reports”](#) on page 577.

**Table 19-8**      Group options for custom reports

Item	Description
<b>Group by</b>	Groups the report information based on the fields that you select for the report.
<b>Ascending</b>	Groups the report information in ascending order. Ascending order lists numbers from smallest to largest and lists letters in alphabetical order.

**Table 19-8** Group options for custom reports (*continued*)

Item	Description
<b>Descending</b>	Groups the report information in descending order. Descending order lists numbers from largest to smallest and lists letters in reverse alphabetical order.
<b>Then group on</b>	Lets you group on additional report fields.

## Available groups from which to select fields for custom reports

Select a group for which for which you want to create a report.

See [“Creating a custom report”](#) on page 567.

**Table 19-9** Group selections for creating reports

Group	Description
<b>Alerts Group</b>	Includes fields for information such as the alert message text, the alert title, when the alert was created, and the name of the responder.
<b>Job History Group</b>	Includes fields for information such as the backup rate, the device used, errors, and media.
<b>Job Group</b>	Includes fields for information such as the the job name and the due date.
<b>Media Group</b>	Includes fields for information such as the backup set date and time, the backup type, the date allocated and modified, and the media set name.
<b>Device Group</b>	Includes fields for information such as the number of bytes that were read or written, number of hours the device was in use, and the number of errors on the device.

## About sorting fields in custom reports

You can sort a custom report by up to three of the fields that you have chosen for the report. When you sort on fields, Backup Exec arranges all of the data that matches the sort criteria together in the report. For example, if you sort on the

Backup Exec server field in ascending order, all data for Backup Exec server A displays first, followed by all data for Backup Exec server B, and so on. Ascending order lists numbers from smallest to largest and lists letters in alphabetical order. Descending order lists numbers from largest to smallest and lists letters in reverse alphabetical order.

See [“Sorting fields in custom reports”](#) on page 580.

## Sorting fields in custom reports

Use the following steps to sort fields in custom reports.

See [“About sorting fields in custom reports”](#) on page 579.

### To sort fields in custom reports

- 1 On the navigation bar, click **Reports**.
- 2 In the tree view, click **Custom Reports**.
- 3 In the reports list, click the report that contains the fields you want to sort.
- 4 In the task pane, click **Edit**.
- 5 On the properties pane, under **Report Definition**, click **Sorting**.
- 6 Select the appropriate sort options.  
See [“Sort options for custom reports”](#) on page 580.
- 7 Do any of the following:

To set graph options for the report

Do the following in the order listed:

- In the left pane, click **Graph Options**.
- Complete the appropriate graphing options.

See [“Setting graph options in custom reports”](#) on page 581.

To preview the report

In the left pane, click **Preview**.

To finish and close the report Click **OK**.

## Sort options for custom reports

You can sort report information in ascending or descending order based on the fields that you selected for the report.

See [“About sorting fields in custom reports”](#) on page 579.

See [“Sorting fields in custom reports”](#) on page 580.

**Table 19-10** Sort options for custom reports

Item	Description
<b>Sort on</b>	Sorts the report information based on the fields that you select for the report.
<b>Ascending</b>	Sorts the report information in ascending order. Ascending order lists numbers from smallest to largest and lists letters in alphabetical order.
<b>Descending</b>	Sorts the report information in descending order. Descending order lists numbers from largest to smallest and lists letters in reverse alphabetical order.
<b>Then sort on</b>	Lets you sort on additional report fields.

## Setting graph options in custom reports

You can include a pie graph or a bar graph in custom reports.

You must select at least two fields on the **Field Selection** dialog box to create a pie graph, and at least three fields to create a bar graph.

### To set graph options in custom reports

- 1 On the **Reports** tab, click **New Custom Report**.
- 2 Type a name and description for the report, and then select at least two fields on the **Field Selection** dialog box to create a pie graph. Select at least three fields to create a bar graph.
- 3 Click **Graph Options**.
- 4 In the **Graph type** box, select the type of graph that you want to create. Choices include **Pie** or **Bar**.
- 5 Complete the options for a pie graph or a bar graph.  
 See [“Graph options for custom reports”](#) on page 582.
- 6 Do any of the following:
  - To preview the report Click **Preview**.
  - To finish and close the report Click **OK**.

## Graph options for custom reports

You can include either a pie chart or a bar chart in a custom report. After you select the graph type, you can select specific options for the graph.

See [“Setting graph options in custom reports”](#) on page 581.

The following table describes the available pie chart options.

**Table 19-11** Pie graph options for custom reports

Item	Description
<b>Category field (pie section per value)</b>	Specifies the field for which you want to display sections in the pie chart. Choices include the following: <ul style="list-style-type: none"> <li>■ <b>Backup Rate</b></li> <li>■ <b>Corrupt Files</b></li> <li>■ <b>Device Name</b></li> </ul>
<b>Data field</b>	Specifies the field for which you want to calculate values. Choices include the following: <ul style="list-style-type: none"> <li>■ <b>Backup Rate</b></li> <li>■ <b>Corrupt Files</b></li> <li>■ <b>Device Name</b></li> </ul>

**Table 19-11** Pie graph options for custom reports (*continued*)

Item	Description
<b>Aggregation function</b>	<p>Selects the way that you want Backup Exec to calculate the values that are generated for the Data field.</p> <p>Choices include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Minimum.</b> Calculates the lowest value. This is available for numeric fields only.</li> <li>■ <b>Maximum.</b> Calculates the highest value. This is available for numeric fields only.</li> <li>■ <b>Average.</b> Calculates the average value. This is available for numeric fields only.</li> <li>■ <b>Count.</b> Calculates the number of values. This option is the only available option for non-numeric fields, such as text fields or date fields. However, it is also available for numeric fields.</li> <li>■ <b>Sum.</b> Calculates the sum of the values. This is available for numeric fields only.</li> </ul>

The following table describes the available bar graph options

**Table 19-12** Bar graph options for custom reports

Item	Description
<b>Vertical axis title</b>	<p>Specifies the title that you want to display to the left of the graph. The title appears vertically in the report and has a 50-character limit.</p>

**Table 19-12** Bar graph options for custom reports (*continued*)

Item	Description
<b>Series field (bar per value)</b>	<p>Specifies the field that contains the values that you want to display on the horizontal bars of the graph. Backup Exec creates a legend for the values.</p> <p>Choices include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Backup Rate</b></li> <li>■ <b>Corrupt Files</b></li> <li>■ <b>Device Name</b></li> </ul>
<b>Category field (set of series bars per value)</b>	<p>Specifies the field that contains the information for which you want to group information along the left side of the graph.</p> <p>Choices include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Backup Rate</b></li> <li>■ <b>Corrupt Files</b></li> <li>■ <b>Device Name</b></li> </ul>
<b>Data field</b>	<p>Specifies the field that you want to display below the graph.</p> <p>Choices include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Backup Rate</b></li> <li>■ <b>Corrupt Files</b></li> <li>■ <b>Device Name</b></li> </ul>
<b>Horizontal axis title</b>	<p>Specifies the title that you want to display below the graph.</p>

**Table 19-12** Bar graph options for custom reports (*continued*)

Item	Description
<b>Aggregation function</b>	<p>Selects the way that you want Backup Exec to calculate the values that are generated for the Data field.</p> <p>Choices include the following:</p> <ul style="list-style-type: none"> <li>■ <b>Minimum.</b> Calculates the lowest value. This is available for numeric fields only.</li> <li>■ <b>Maximum.</b> Calculates the highest value. This is available for numeric fields only.</li> <li>■ <b>Average.</b> Calculates the average value. This is available for numeric fields only.</li> <li>■ <b>Count.</b> Calculates the number of values. This option is the only available option for non-numeric fields, such as text fields or date fields. However, it is also available for numeric fields.</li> <li>■ <b>Sum.</b> Calculates the sum of the values. This is available for numeric fields only.</li> </ul>

## Previewing custom reports

Use the preview feature to verify that you created a custom report correctly.

### To preview custom reports

- 1 On the **Reports** tab, click **New Custom Report**.
- 2 Add a report name and then set the report settings desired.
- 3 Click **Preview**.
- 4 Click **OK**.

## Copying custom reports

You can create a copy of a custom report, and then modify the copy.

#### To copy custom reports

- 1 On the **Reports** tab, under **Report Groups**, click **Custom**.
- 2 Right-click the report that you want to copy, and then click **Copy**.
- 3 In the **Name of copy** box, type a unique name for the copied report.
- 4 Click **OK**.

The copied report appears in the list of custom reports.

## Editing custom reports

If the report that you want to edit has been run in a previous report job, the changes you make now may affect the appearance of the reports in job history. Symantec recommends that you copy the report and then edit the copy.

#### To edit custom reports

- 1 On the **Reports** tab, under **Report Groups**, click **Custom**.
- 2 Right-click the report that you want to edit, and then click **Edit**.
- 3 Change the report settings as needed.
- 4 Click **OK**.

## Deleting custom reports

Use the following steps to delete a custom report.

#### To delete custom reports

- 1 On the **Reports** tab, under **Report Groups**, click **Custom**.
- 2 In the reports list, right-click the report that you want to filter, and then click **Delete**.
- 3 Click **Yes**.

## Editing application settings for reports

You can set Backup Exec to display all reports in either HTML or Adobe Portable Document Format (PDF). The default setting is HTML. The format that you select does not affect the format of the reports sent to users with the notification feature.

In addition, you can edit the application settings for the header and footer for all custom reports.

You can do the following:

- Include a logo in the header.
- Choose a color for the banner in the header.
- Include text in the footer.
- Include the time in the footer.

When you choose a color for the banner, you can type the numbers that correspond to the colors (RGB values), or you can select the color from a chart.

**To edit application settings for reports**

- 1 On the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Reports**.
- 3 Complete the appropriate options.  
 See “[Application settings for reports](#)” on page 587.
- 4 Click **OK**.

## Application settings for reports

You can change the application settings for all Backup Exec reports.

See “[Editing application settings for reports](#)” on page 586.

The following table describes the application settings for reports:

**Table 19-13** Application settings for reports

Item	Description
<b>HTML</b>	Specifies that all reports are displayed in HTML format. This is the default setting.
<b>PDF</b>	Specifies that all reports are displayed in Adobe Portable Document Format (PDF).
<b>Maximum number of rows to include in a report</b>	Indicates the maximum number of rows to show in a report.  The default is 10,000 rows.
<b>Show all rows</b>	Displays all rows in a report.
<b>Show distinct rows</b>	Displays only the rows that are unique.
<b>Use custom image file</b>	Uses a customized image file in the header of all custom reports.

**Table 19-13** Application settings for reports (*continued*)

Item	Description
<b>Image file path</b>	Identifies the path to the logo that you want to use in all custom reports.
<b>Red</b>	Specifies the number that corresponds to the value for red.
<b>Green</b>	Specifies the number that corresponds to the value for green.
<b>Blue</b>	Specifies the number that corresponds to the value for blue.
<b>Colors</b>	Indicates a basic color to use for a custom report banner.  You can also create a custom color for a custom report banner.
<b>Text</b>	Indicates the text that you want to display in the footer of custom reports.
<b>Include time</b>	Includes the time when the report runs in the footer of custom reports.

## Viewing report properties

Report properties provide detailed information about each report. The properties can be viewed, but not edited.

### To view report properties

- 1 On the **Reports** tab, under **Report Groups**, select a report group.
- 2 Right-click a report for which you want to view properties, and then click **Properties**.  
See “[Report properties](#)” on page 588.
- 3 Click **OK** after you have finished viewing the properties.  
See “[Running a report](#)” on page 558.

## Report properties

You can view but not edit properties for each report.

See “[Viewing report properties](#)” on page 588.

The following table describes the report properties:

**Table 19-14**      General report properties

Item	Description
<b>Title</b>	Displays the name of the report.
<b>Description</b>	Describes the type of data that is included in the report.
<b>Category</b>	Specifies the classification for the report. Available report categories include the following: <ul style="list-style-type: none"> <li>■ Media</li> <li>■ Media Vault</li> <li>■ Jobs</li> <li>■ Devices</li> <li>■ Configuration</li> <li>■ Alerts</li> <li>■ Template</li> </ul>
<b>Author</b>	Displays the creator of the report.
<b>Subject</b>	Displays the version of the product for which the report was created.
<b>File name</b>	Displays the file name of the report.
<b>File size</b>	Displays the size of the report.
<b>Creation Date</b>	Displays the date and the time that the report was installed on the system.

## Available reports

This section provides detailed information about each report available in Backup Exec. The file name of the report, a description, and the information included in the report are listed for each report. The data included in each report will vary depending on the criteria you selected to include in the report.

The following reports are included in Backup Exec:

**Table 19-15** Backup Exec Reports

Report Name	Description
<b>Alert History</b>	Lists all alerts in the alert history chronologically, displaying the most recent alerts first  See <a href="#">“Alert History report”</a> on page 595.
<b>Alert History by Backup Exec server</b>	Lists all alerts in the alert history grouped and filtered by Backup Exec server, displaying the most recent alerts first.  See <a href="#">“Alert History By Backup Exec Server report”</a> on page 595.
<b>Archive Job Success Rate</b>	Displays the number of archive jobs for the backed up servers that successfully ran.  See <a href="#">“Archive Job Success Rate report”</a> on page 625.
<b>Archive Selections by Archive Rules and Retention Categories</b>	Displays the archive rules and the retention categories that are applied to each archive selection.  See <a href="#">“Archive Selections by Archive Rules and Retention Categories report”</a> on page 625.
<b>Audit Log</b>	Lists the contents of the audit logs for selected servers for the specified time period.  See <a href="#">“Audit Log report”</a> on page 596.
<b>Backup Job Success Rate</b>	Lists the success rate for backup jobs run to back up selected servers.  See <a href="#">“Backup Job Success Rate report”</a> on page 597.
<b>Backup Recommendations</b>	Lists any recommendations that can help you to better manage your backups.  See <a href="#">“Backup Recommendations report”</a> on page 597.
<b>Backup Resource Success Rate</b>	Lists the success rate for backup jobs for specified past number of days for resources on selected servers.  See <a href="#">“Backup Resource Success Rate report”</a> on page 598.
<b>Backup Sets by Media Set</b>	Lists all backup sets by media set.  See <a href="#">“Backup Sets by Media Set report”</a> on page 598.

**Table 19-15** Backup Exec Reports (*continued*)

Report Name	Description
<b>Backup Size by Resource</b>	<p>Lists the backup size for each resource job for up to seven previous runs and then computes the trailing average for up to seven previous runs for each job run.</p> <p>See <a href="#">“Backup Size By Resource report”</a> on page 599.</p>
<b>Daily Device Utilization</b>	<p>Lists the percentage of the storage devices’ capacity that the Backup Exec server uses.</p> <p>See <a href="#">“Daily Device Utilization report”</a> on page 600.</p>
<b>Deduplication device summary</b>	<p>Displays a summary of the deduplication operations for local deduplication storage folders and shared deduplication storage folders.</p> <p>See <a href="#">“Deduplication Device Summary report”</a> on page 602.</p>
<b>Deduplication summary</b>	<p>Displays a deduplication summary for all of the deduplication jobs that run on the Backup Exec server.</p> <p>See <a href="#">“Deduplication Summary report”</a> on page 603.</p>
<b>Device Summary</b>	<p>Lists device usage and error summary for each selected Backup Exec server.</p> <p>See <a href="#">“Device Summary report”</a> on page 601.</p>
<b>Disk Storage Summary</b>	<p>Displays disk-based usage statistics for Backup Exec server disk storage.</p> <p>See <a href="#">“Disk Storage Summary report”</a> on page 603.</p>
<b>Error-Handling Rules</b>	<p>Lists all the defined error-handling rules.</p> <p>See <a href="#">“Error-Handling Rules report”</a> on page 604.</p>
<b>Event Recipients</b>	<p>Lists all events registered by each notification recipient.</p> <p>See <a href="#">“Event Recipients report”</a> on page 605.</p>
<b>Exchange Mailbox Group Archive Settings</b>	<p>Displays the archive settings that are applied to mailbox groups in each domain.</p> <p>See <a href="#">“Exchange Mailbox Group Archive Settings report”</a> on page 626.</p>

**Table 19-15** Backup Exec Reports (*continued*)

Report Name	Description
<b>Failed Archive Jobs</b>	Displays what archive jobs failed recently. See <a href="#">“Failed Archive Jobs report”</a> on page 627.
<b>Failed Backup Jobs</b>	Lists all the failed backup jobs sorted by the resource server and time frame. See <a href="#">“Failed Backup Jobs report”</a> on page 606.
<b>File System Archive Settings</b>	Displays the archive settings that are applied to archive selections for each server. See <a href="#">“File System Archive Settings report”</a> on page 628.
<b>Jobs Summary</b>	Lists all the jobs that ran within the last 72 hours in chronological order. See <a href="#">“Jobs Summary report”</a> on page 607.
<b>Managed Backup Exec Servers</b>	Lists the status and configuration for all Backup Exec servers managed by a central administration server. See <a href="#">“Managed Backup Exec Servers report”</a> on page 608.
<b>Media Audit</b>	Lists the recent media configuration changes. See <a href="#">“Media Audit report”</a> on page 609.
<b>Media Errors</b>	Lists the number of errors that occur on all media. See <a href="#">“Media Errors report”</a> on page 610.
<b>Media Required for Recovery</b>	Lists the media that contain the backup sets for each system backed up on selected servers for the specified time period. This report can be inaccurate if media overwrite settings allow the media to be overwritten. See <a href="#">“Media Required for Recovery report”</a> on page 610.
<b>Media Summary</b>	Lists all the media sets and media used by Backup Exec servers. The current location is given for each media. Also lists usage statistics for media and the location of media within Backup Exec media sets. See <a href="#">“Media Summary report”</a> on page 611.
<b>Media Vault Contents</b>	Lists the media located in each media vault. See <a href="#">“Media Vault Contents report”</a> on page 612.

**Table 19-15** Backup Exec Reports (*continued*)

Report Name	Description
<b>Move Media to Vault</b>	<p>Lists all media that can be moved to a media vault. The media listed are not currently in a media vault and the media's append period has expired.</p> <p>See <a href="#">"Move Media to Vault report"</a> on page 613.</p>
<b>Operations Overview</b>	<p>Lists past and future operations data for user-set period.</p> <p>See <a href="#">"Operations Overview report"</a> on page 614.</p>
<b>Overnight Archive Summary</b>	<p>Displays the status of the archive jobs that ran in the last 24 hours.</p> <p>See <a href="#">"Overnight Archive Summary report"</a> on page 628.</p>
<b>Overnight Summary</b>	<p>Lists the results of backup jobs for each resource during the last 24 hours. This report includes backup jobs that were scheduled to run but did not run. Jobs are given a grace period of 24 hours before being marked as past due.</p> <p>See <a href="#">"Overnight Summary report"</a> on page 616.</p>
<b>Problem Files</b>	<p>Lists all the problem files reported for jobs. The files are grouped by day and resource.</p> <p>See <a href="#">"Problem Files report"</a> on page 617.</p>
<b>Recently Written Media</b>	<p>Lists all media that have been modified in the last 24 hours.</p> <p>See <a href="#">"Recently Written Media report"</a> on page 617.</p>
<b>Resource Protected Recently Report</b>	<p>Lists all job detail statistics and exceptions that occurred on a Backup Exec server for which you run this report.</p> <p>See <a href="#">"Resource Protected Recently report"</a> on page 619.</p>
<b>Resource Risk Assessment</b>	<p>Lists job information for resources on which the last backup job run on the resource failed. The data is filtered by resource server.</p> <p>See <a href="#">"Resource Risk Assessment report"</a> on page 618.</p>

**Table 19-15** Backup Exec Reports (*continued*)

Report Name	Description
<b>Restore Set Details by Resource</b>	Lists all restore sets that ran within the last 72 hours. The sets are grouped by the server and resource.  See <a href="#">“Restore Set Details by Resource report”</a> on page 619.
<b>Retrieve Media from Vault</b>	Lists all reusable media currently in the specified vault.  See <a href="#">“Retrieve Media from Vault report”</a> on page 620.
<b>Robotic Library Inventory</b>	Lists the contents of slots in robotic libraries attached to Backup Exec servers. Usage statistics are provided for each piece of media.  See <a href="#">“Robotic Library Inventory report”</a> on page 621.
<b>Scheduled Server Workload</b>	Lists the estimated scheduled workload for the next 24-hour period by server.  See <a href="#">“Scheduled Server Workload report”</a> on page 622.
<b>Scratch Media Availability</b>	Lists the aging distribution of media. Shows how many media are available for overwrite and when other media will become available for overwrite.  See <a href="#">“Scratch Media Availability report”</a> on page 623.
<b>Test Run Results</b>	Lists the results for the test run jobs set for the selected time period and Backup Exec servers.  See <a href="#">“Test Run Results report”</a> on page 624.
<b>Vault Store Usage Details</b>	Displays the archives that are in each store and the size of each archive.  See <a href="#">“Vault Store Usage Details report”</a> on page 629.
<b>Vault Store Usage Summary</b>	Displays the archived items that are in each vault store and the total size of the vault store.  See <a href="#">“Vault Store Usage Summary report”</a> on page 630.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Alert History report

The Alert History report lists all the alerts in the Alert History chronologically, displaying the most recent alerts first. You can limit the number of alerts that appear in the report by entering range parameters for the Days or Event count options

Information displayed in the Active History report is described in the following table.

**Table 19-16** Alert History report

Item	Description
<b>Time</b>	Date and time the alert occurred.
<b>Received</b>	Time the alert occurred.
<b>Responded</b>	Time the user responded to the alert.
<b>Responding User</b>	User that responded to the alert.
<b>Job Name</b>	The name of the job associated with the alert.
<b>Backup Exec server</b>	Name of the Backup Exec server on which the alert occurred.
<b>Category</b>	Title of the alert, such as Service Start or Job Failed.
<b>Message</b>	Describes the event that caused the alert.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Alert History By Backup Exec Server report report

The Alert History by Backup Exec server report lists all alerts in the alert history grouped and filtered by Backup Exec server, displaying the most recent alerts first. You can limit the amount of data that appears in the report by selecting filter parameters for the Days, Event count or Backup Exec server option.

Information displayed in the Alert History by Backup Exec server report is described in the following table.

**Table 19-17** Alert History by Backup Exec Server report

Item	Description
<b>Backup Exec server</b>	Name of the Backup Exec server on which the alert occurred.
<b>Time</b>	Date and time the alert occurred.
<b>Received</b>	Time the alert occurred.
<b>Responded</b>	Time the user responded to the alert.
<b>Responding User</b>	User that responded to the alert.
<b>Job Name</b>	Name of the job associated with the alert.
<b>Category</b>	Title of the alert, such as Service Start or Job Failed.
<b>Message</b>	Describes the event that caused the alert.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Audit Log report

The Audit Log report lists the contents of the audit logs for the selected servers for the selected time period. You can limit the amount of data that appears in the report by entering filter parameters for the Backup Exec server or Audit Category options and range parameters for the Days and Event count options.

Information displayed in the Audit Log report is described in the following table.

**Table 19-18** Audit Log report

Item	Description
<b>Category</b>	Category in which the change occurred, such as Logon Account, Alerts, or Job.
<b>Date Entered</b>	Time and date the change occurred.
<b>Message</b>	Description of the change made in Backup Exec.
<b>User Name</b>	User that made the change.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Backup Job Success Rate report

The Backup Job Success Rate report lists the success rate for backup jobs run to back up selected servers. You can limit the amount of data that appears in the report by entering filter parameters for the Backed Up Server option and range parameters for the Days option.

Information displayed in the Backup Success Rate report is described in the following table.

**Table 19-19** Backup Success Rate report

Item	Description
<b>Server</b>	Name of the server being backed up.
<b>Date</b>	Date the backup job was processed.
<b>Total Jobs</b>	Total number of jobs processed by the Backup Exec server.
<b>Successful</b>	Total number of jobs successfully performed by the Backup Exec server.
<b>Success Rate</b>	Percentage of successful jobs processed by the Backup Exec server.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Backup Recommendations report

The Backup Recommendations report lists any recommendations that can help you to better manage your backups. The recommendations may include better ways to back up specific types of data or suggestions for how to use Symantec products.

The following table describes the information in the Backup Recommendations report.

**Table 19-20** Backup Recommendations report

Item	Description
<b>Backup Exec server</b>	Name of the Backup Exec server for which the recommendation applies.
<b>Job Name</b>	Name of the job that is associated with the recommendation.

**Table 19-20** Backup Recommendations report (*continued*)

Item	Description
<b>Start Time</b>	Date and time when the job that is associated with the recommendation ran.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Backup Resource Success Rate report

The Backup Resource Success Rate report lists the success rate for backup jobs for a specific number of days for resources on selected servers. You can limit the amount of data that appears in the report by entering range parameters for the Days option.

**Table 19-21** Backup Resource Success Rate report

Item	Description
<b>Resource</b>	Name of the system being backed up.
<b>Date</b>	Date the backup job was processed.
<b>Total Jobs</b>	Total number of jobs that were processed by the Backup Exec server.
<b>Successful</b>	Total number of jobs successfully performed by the Backup Exec server.
<b>Success Rate</b>	Percentage of successful jobs processed by the Backup Exec server.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Backup Sets by Media Set report

The Backup Sets by Media Set report lists all the backup sets by media set. You can limit the amount of data that appears in the report by selecting filter parameters for the Media Set option.

Information displayed in the Backup Sets by Media Sets report is described in the following table.

**Table 19-22** Backup Sets by Media Sets report

Item	Description
<b>Media Set</b>	Name of the media set on which the job ran.
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.
<b>Set</b>	Sequential number for backup sets on the media.
<b>Method</b>	Specific type of backup.
<b>Date / Time</b>	Date and time the data was backed up.
<b>Backup Set Description / Source</b>	Describes the data that was backed up and the location of the data.
<b>Directories</b>	Number of directories backed up.
<b>Files</b>	Number of files backed up.
<b>Size</b>	Amount of data backed up.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Backup Size By Resource report

The Backup Size By Resource report lists the backup size for each resource job for up to seven previous jobs. It also computes the trailing average, which is the average of the amount of data backed up in the seven previous jobs.

You can limit the amount of data that appears in the report by entering filter parameters for the Backed Up Server option.

Information displayed in the Backup Size by Resource report is described in the following table.

**Table 19-23** Backup Size by Resource Job report

Item	Description
<b>Server</b>	Name of the Backup Exec server where the data for the backup job was located.
<b>Resource</b>	Name of the resource backed up.

**Table 19-23** Backup Size by Resource Job report (*continued*)

Item	Description
<b>Job</b>	Name of the backup job.
<b>Job Date and Time Run</b>	Date and time the backup job was processed.
<b>Backup Size</b>	Amount of data backed up.
<b>Trailing Avg</b>	Average amount of data backed up during the seven previous runs.
<b>Difference %</b>	Amount by which the data backed up in the current job differs from the previous backup jobs.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Daily Device Utilization report

The Daily Device Utilization report lists the percentage of the storage devices’ capacity that the Backup Exec server uses.

Information displayed in the Daily Device Utilization report is described in the following table.

**Table 19-24** Daily Device Utilization report

Item	Description
<b>Drive Name</b>	Name of the storage device and the Backup Exec server where the device is located.
<b>Status</b>	<p>Status of the storage device</p> <p>Statuses for storage devices are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Pause</b> The storage device is temporarily stopped.</li> <li>■ <b>Enable</b> The storage device is available for use with Backup Exec. If the storage device is disabled, it is available for use with other applications.</li> <li>■ <b>Online</b> The storage device is available for use.</li> <li>■ <b>Offline</b> Backup Exec cannot access the storage device.</li> </ul>

**Table 19-24** Daily Device Utilization report (*continued*)

Item	Description
<b>Date</b>	Date the storage device was used.
<b>Jobs</b>	Number of jobs processed by the Backup Exec server's storage device.
<b>Size</b>	The amount of data processed by the Backup Exec server's storage device.
<b>Utilization (%)</b>	Percentage of device utilization.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Device Summary report

The Device Summary report lists all the devices for each selected Backup Exec server. You can limit the amount of data that appears in the report by selecting filter parameters for the Backup Exec server option.

Information displayed in the Device Summary report is described in the following table.

**Table 19-25** Device Summary report

Item	Description
<b>Server</b>	Name of the server where the device is located.
<b>Drive Name</b>	Name of the drive in the robotic library.
<b>Target</b>	Address of the storage device that is connected to the Backup Exec server.
<b>State</b>	Device state, such as online.
<b>Created</b>	Date on which the media was created.
<b>Cleaned</b>	Date on which the last cleaning job was run on the drive.
<b>Hours</b>	Hours the device has been in use since the last cleaning job.
<b>Errors</b>	Number of errors occurring since the last cleaning job.
<b>Size</b>	Amount of data read and written since the last cleaning job.
<b>Mounts</b>	Number of mounts occurring since the last cleaning job.

**Table 19-25** Device Summary report (*continued*)

Item	Description
<b>Hours</b>	Total number of hours the device has been in use.
<b>Errors</b>	Total number of errors occurring on the device.
<b>Size</b>	Amount of data read and written to the device.
<b>Mounts</b>	Total number of mounts occurring to the device.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Deduplication Device Summary report

The Deduplication device summary report displays a summary of the deduplication operations for local deduplication storage folders and shared deduplication storage folders.

**Table 19-26** Deduplication device summary report

Item	Description
<b>State</b>	Device state, such as online and enabled.
<b>Created</b>	Date media was created.
<b>Total Capacity</b>	Total capacity of the deduplication storage folder.
<b>Used Capacity</b>	Capacity presently used by the deduplication storage folder.
<b>Available Capacity</b>	Remaining capacity of the the deduplication storage folder.
<b>Percent Full</b>	Percentage of storage space that is available in the deduplication storage folder.
<b>Protected Bytes</b>	Total amount of data that is selected for backup in all jobs using the device before deduplication occurs.
<b>Deduplication Ratio</b>	Ratio of the amount of data before deduplication to the amount of data after deduplication.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Deduplication Summary report

The Deduplication Summary report displays a deduplication summary for all of the deduplication jobs that run on the Backup Exec server.

**Table 19-27** Deduplication Summary report

Item	Description
<b>Job Name</b>	Name of the job.
<b>Start Time</b>	Time of day that Backup Exec attempted to start the job.
<b>Duration</b>	Length of time the operation took to process.
<b>Size</b>	The amount of data processed.
<b>Size/Minute</b>	Number of kilobytes, megabytes, or gigabytes processed per minute.
<b>Scanned Byte Count</b>	Total amount of data that is selected for backup before deduplication occurs.
<b>Stored Byte Count</b>	The amount of unique data is stored after deduplication occurs.
<b>Deduplication Ratio</b>	Ratio of the amount of data before deduplication to the amount of data after deduplication.
<b>Status</b>	Status of the operation, such as Completed (Success), Failed, or Canceled.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Disk Storage Summary report

The Disk Storage Summary report displays disk usage statistics for Backup Exec server disk storage.

**Table 19-28** Disk storage summary report

Item	Description
<b>Device Name</b>	Name of the disk storage device.
<b>State</b>	State of the device. Device states include the following: <ul style="list-style-type: none"> <li>■ On-line</li> <li>■ Enabled</li> <li>■ Off-line</li> <li>■ Paused</li> <li>■ Disabled</li> </ul>
<b>Local Access Path</b>	Path on the disk where backup data is stored.
<b>Total Capacity</b>	Total capacity of the disk.
<b>Used Space</b>	Amount of disk space being used as storage.
<b>Free Space</b>	Amount of disk space remaining.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Error-Handling Rules report

The Error-Handling Rules report lists all error-handling rules and provides details about each rule. You can limit the amount of data that appears in the report by selecting filter parameters for the Backup Exec server.

Information displayed in the Error-Handling Rules report is described in the following table.

**Table 19-29** Error Handling Rules report

Item	Description
<b>Rule Name</b>	Name of the Error-Handling rule.
<b>Notes</b>	Information entered in the Notes section when the error-handling rule was created.

**Table 19-29** Error Handling Rules report (*continued*)

Item	Description
<b>Job Status</b>	<p>Final job status that activates the rule.</p> <p>Possible statuses are as follows:</p> <ul style="list-style-type: none"> <li>■ Error</li> <li>■ Canceled</li> </ul>
<b>Error Category</b>	<p>Category of error for which the rule will be applied.</p> <p>Available error categories include the following:</p> <ul style="list-style-type: none"> <li>■ Device</li> <li>■ Job</li> <li>■ Media</li> <li>■ Network</li> <li>■ Other</li> <li>■ Resource</li> <li>■ Security</li> <li>■ Server</li> <li>■ System</li> </ul>
<b>Enabled</b>	<p>Displays if the rule is enabled or disabled.</p>
<b>Cancel Job</b>	<p>Displays an X if this option is selected for the error-handling rule. The option cancels all jobs after the maximum number of retries have been attempted.</p>
<b>Pause Job</b>	<p>Displays an X if this option is selected for the error-handling rule. The option enables Backup Exec to pause the job until you can manually clear the error.</p>
<b>Retry Job</b>	<p>Displays an X if this option is selected for the error-handling rule. The option enables Backup Exec to retry the job.</p>
<b>Maximum Retries</b>	<p>Number of times the job is to be retried.</p>
<b>Retry Interval (minutes)</b>	<p>Number of minutes the job is to wait before being retried.</p>

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Event Recipients report

The Event Recipient report lists events registered by each notification recipient.

Information displayed in the Event Recipient report is described in the following table.

**Table 19-30** Event Recipients report

Item	Description
<b>Recipient Name</b>	Name of the recipient.
<b>Recipient type</b>	Designates to whom the Event Recipients report is sent, such as an individual recipient or a group of recipients.
<b>Event Type</b>	Alert category or ad hoc job.
<b>Event Name</b>	Detail for the alert category or ad hoc job.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Failed Backup Jobs report

The Failed Backup Jobs report lists all the failed backup jobs. The jobs are sorted by the server and specified time frame. You can limit the amount of data that appears in the report by entering filter parameters for the Backed Up Server option and range parameters for the Days option.

Information displayed in the Failed Backup Jobs report is described in the following table:

**Table 19-31** Failed Jobs report

Item	Description
<b>Resource</b>	Name of the system being backed up.
<b>Start Time</b>	Date and time the backup job started.
<b>Duration</b>	Length of time the operation took to process.
<b>Job Name</b>	Name of job that failed.
<b>Category</b>	Category for the failed job that may be generated by a system, job, media, or device error.
<b>Error Code</b>	Displays the error code that corresponds to the failure.
<b>Description</b>	Describes the event that caused the error.
<b>Status</b>	Status of the operation, such as Error.

**Table 19-31** Failed Jobs report (*continued*)

Item	Description
<b>Device Name</b>	Name of the device on which the job ran.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Jobs Summary report

The Jobs Summary report lists all jobs that have run within the specified time range. The jobs are listed in chronological order. You can limit the amount of data that appears in the report by selecting range parameters for the Hours option.

Information displayed in the Jobs Summary report is described in the following table.

**Table 19-32** Jobs Summary report

Item	Description
<b>Start Time</b>	Date and time the operation started.
<b>Job Name</b>	Name of the completed job.
<b>Duration</b>	Length of time the operation took to process.
<b>Size</b>	The amount of data processed.
<b>Files</b>	Number of files processed.
<b>Directories</b>	Number of directories processed.
<b>Size/Minute</b>	Number of kilobytes, megabytes, or gigabytes processed per minute.
<b>Skipped</b>	Number of files skipped during the operation.
<b>Corrupt Files</b>	Number of corrupt files encountered during the operation.
<b>Files in Use</b>	Number of files in use during the operation.
<b>Status</b>	Status of the operation, such as Completed (Success), Failed, or Canceled.
<b>Type</b>	Lists the type of job that Backup Exec ran within the specified time range.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Managed Backup Exec Servers report

The Managed Backup Exec Servers report lists status and configuration information for all Backup Exec servers managed by Backup Exec. You can limit the amount of data that appears in the report by selecting filter parameters for the Backup Exec server option.

Information displayed in the Managed Backup Exec Servers report is described in the following table.

**Table 19-33** Managed Backup Exec Servers report

Item	Description
<b>Managed Backup Exec server</b>	Name of the managed Backup Exec server.
<b>Status</b>	Status of the server. Possible status includes the following: <ul style="list-style-type: none"> <li>■ Online - available for use.</li> <li>■ Stalled - not responding immediately to messages</li> <li>■ No Comm - communications to the server have been lost for some period of time.</li> </ul>
<b>Stalled</b>	Time limit used for determining Stalled communications status.
<b>No Comm</b>	Time limit used for determining No Comm communications status.
<b>Catalog Location</b>	Location where server keeps catalog information. Possible locations are as follows: <ul style="list-style-type: none"> <li>■ Local - the catalog information is kept on the Backup Exec server itself.</li> <li>■ CASO - the catalog information is kept on the Central Admin Server.</li> </ul>
<b>Logs</b>	When job logs are uploaded from the managed server to the CASO database. Possible upload times are as follows: <ul style="list-style-type: none"> <li>■ timed basis in seconds</li> <li>■ schedule time</li> <li>■ completion of job</li> <li>■ never</li> </ul>

**Table 19-33** Managed Backup Exec Servers report (*continued*)

Item	Description
<b>History</b>	When job history is uploaded from the managed server to the CASO database. Possible upload times are as follows: <ul style="list-style-type: none"> <li>■ timed basis in seconds</li> <li>■ schedule time</li> <li>■ completion of job</li> <li>■ never</li> </ul>
<b>Status</b>	When status is uploaded from the managed server to the CASO database. Possible upload times are as follows: <ul style="list-style-type: none"> <li>■ timed basis in seconds</li> <li>■ schedule time</li> <li>■ completion of job</li> <li>■ never</li> </ul>
<b>Display Alert</b>	Displays Yes if you have configured an alert to be set if time between server clocks exceed a preset value (maximum time difference tolerance).
<b>Sec</b>	Maximum time difference tolerance in seconds set for server.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Media Audit report

The Media Audit report lists the recent configuration changes that you made to your media. You can use filter parameters for the Backup Exec server option to limit the amount of data that appears in the report. You can also enter range parameters for the Days or Event count options.

Information displayed in the Media Audit report is described in the following table.

**Table 19-34** Media Audit report

Item	Description
<b>Date Entered</b>	Time and date the change occurred.

**Table 19-34** Media Audit report (*continued*)

Item	Description
Message	Description of the change that was made to the media.
User Name	User that made the change.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Media Errors report

The Media Errors report lists the number of errors that occur on all media. You can use filter parameters for the Media Set option to limit the amount of data that appears in the report. You can also enter range parameters for the Event count options.

Information displayed in the Media Audit report is described in the following table.

**Table 19-35** Media Errors report

Item	Description
Media Label	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned barcode label.
Total Mounts	Total number of times this media has been mounted.
Total In Use Hours	Total number of hours that this media has been in use.
Total Errors	Total number of system, job, media, and device error alerts.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Media Required for Recovery report

The Media Required for Recovery report lists the media that contain the backup sets for each system backed up on the selected Backup Exec server for the specified time period. However, this report may be inaccurate if media overwrite settings allow the media to be overwritten. You can limit the amount of data that appears in the report by selecting filter parameters for the Backed Up Server option and range parameters for the Days option.

Information displayed in the Media Required for Recovery report is described in the following table.

**Table 19-36** Media Required for Recovery report

Item	Description
<b>Date</b>	Date and time the backup job set was created.
<b>Media Location Name</b>	Name of the storage device where the media that was used for the backup job is stored.
<b>Media Label</b>	Media label assigned by Backup Exec, which is assigned by the administrator or contained on a pre-assigned bar code label.
<b>Backup Method</b>	Specific type of backup. See <a href="#">“About backup methods”</a> on page 528.
<b>Recycle Time</b>	Displays the date and the time after which the media can be overwritten.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Media Summary report

The Media Summary report lists all media sets and media used by Backup Exec servers. Usage statistics are given for each piece of media. You can limit the amount of data that appears in the report by selecting filter parameters for the Media summary option.

Information displayed in the Media Summary report is described in the following table.

**Table 19-37** Media Summary report

Item	Description
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.
<b>Media Type</b>	Type of media cartridge, such as 4mm.
<b>Allocated</b>	Date media was allocated to a media set as a result of an overwrite operation.
<b>Modified</b>	Date data was last written to the media.

**Table 19-37** Media Summary report (*continued*)

Item	Description
<b>Hours</b>	Total number of hours that the media has been in use.
<b>Mounts</b>	Total number of times the media has been mounted.
<b>Soft Errors</b>	Number of recoverable read errors encountered.
<b>Hard Errors</b>	Number of unrecoverable read errors encountered.
<b>Write Size</b>	Amount of data that has been written to the media.
<b>Current Size</b>	Estimate of the amount of data currently on the media.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Media Vault Contents report

The Media Vault Contents report lists all the media in a specified media vault. You can limit the amount of data that appears in the report by selecting filter parameters for the Vault option.

Information displayed in the Media Vault Contents report is described in the following table.

**Table 19-38** Media Vault Contents report

Item	Description
<b>Vault Name</b>	Location of the media.
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.
<b>Overwrite Protection End Date</b>	Date that data on the media may be overwritten.
<b>Vault Media Rule Move Date</b>	Date media can be moved to vault.
<b>Media Set</b>	Name of media set to which the media belongs.
<b>Vault Media Rule Name</b>	Name of vault media rule.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Move Media to Vault report

Lists all media that you can move to a media vault.

The media listed are not currently in a media vault and meet one of the following criteria:

- The media has met or exceeded the vault move date specified for the media containing the media.
- The append period has expired, but the overwrite protection period is still current (allocated).

You can limit the amount of data that appears in the report by entering filter parameters for Backup Exec server and range parameters for the Days option.

Information displayed in the Move Media to Vault report is described in the following table.

**Table 19-39** Move Media to Vault report

Item	Description
<b>Backup Exec server</b>	Name of the Backup Exec server where the data for the backup job was located.
<b>Media Set</b>	Name of the media set.
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.
<b>Location</b>	Location of the media.
<b>Append Period End Date</b>	Last date that data may be added to the media.
<b>Overwrite Protection End Date</b>	Date that data on the media may be overwritten.
<b>Vault Media Rule Move Date</b>	Date media can be moved to vault.
<b>Vault Name</b>	Name of vault to which media is to be moved.
<b>Vault Media Rule Name</b>	Name of vault media rule.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Operations Overview report

The Operations Overview report lists details for past and future Backup Exec operations. You can limit the amount of data that appears in the report by entering range parameters for the Days or Event count options.

Information displayed in the Operations Overview report is described in the following table.

**Table 19-40** Operations Overview report

Item	Description
<b>Job summary for jobs completed in the past x Hours</b>	Details Backup Exec job activity for the specified time period.
<b>Errors</b>	Total number of system, job, media, and device error alerts.
<b>Warnings</b>	Total number of job, media, and device warning alerts.
<b>Information</b>	Total number of system, job, media, and device information alerts.
<b>Attention Required</b>	Total number of alerts that require a response from the user.
<b>Completed (Failed)</b>	Total number of jobs that failed.
<b>Completed (Canceled)</b>	Total number of canceled jobs.
<b>Completed (Success)</b>	Total number of jobs that completed successfully.
<b>Exceptions</b>	Total number of jobs that completed successfully, but may contain one or more skipped files, corrupt files, virus infected files or files in use.
<b>Total Data Backed Up</b>	Total amount of data backed up in kilobytes, megabytes, or gigabytes.
<b>Total Media Used</b>	Total number of media used to back up the completed jobs.
<b>Missed</b>	Total number of missed jobs.

**Table 19-40** Operations Overview report (*continued*)

Item	Description
<b>Recovered</b>	Total number of recovered jobs.
<b>Active Jobs</b>	Total number of active jobs.
<b>Scheduled Jobs</b>	Displays those jobs whose scheduled start times begin within 72 hours of the job being created. Jobs with recurring schedules also appear if their start times begin within 72 hours of the job's last start time.
<b>Jobs On Hold</b>	Total number of jobs on hold.
<b>Job Status</b>	The status of the jobs.
<b>Scratch Media</b>	Total number of scratch media available.
<b>Recyclable</b>	Total number of recyclable media available.
<b>Imported</b>	Number of imported media (media created by a product other than this installation of Backup Exec).
<b>Allocated</b>	Number of allocated media (media belonging to a user media set).
<b>Total Overwritable Media</b>	Total number of overwritable media available.
<b>Total Appendable Media</b>	Total number of appendable media available.
<b>Media Overwrite Protection Level</b>	Displays level of overwrite protection (Full, Partial, None) assigned to the media.
<b>Online Devices</b>	Total number of online devices.
<b>Offline Devices</b>	Total number of offline devices.
<b>Disabled Devices</b>	Total number of disabled devices.
<b>Paused Devices</b>	Total number of paused devices.
<b>Disabled</b>	Lists the name of the devices that are disabled.
<b>Paused</b>	Name of the paused devices.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Overnight Summary report

The Overnight Summary report lists the results of backup jobs for each resource during the last 24 hours. This report includes backup jobs that were due to run but did not run. Jobs are given a grace period of 24 hours before being marked as past due. You can limit the amount of data that appears in the report by entering filter parameters for the Backed Up Server option.

Information displayed in the Overnight Summary report is described in the following table.

**Table 19-41** Overnight Summary report

Item	Description
<b>Resource</b>	System being backed up.
<b>Type</b>	Displays the type of job that Backup Exec runs to produce the Overnight Summary report.  Because the Overnight Summary report lists the results of backup jobs for each resource during the past 24 hours, <b>Backup</b> is always the type of job that appears.
<b>Start time</b>	Date and time the operation started.
<b>Status</b>	Status of the operation.
<b>Error Category</b>	Category for the job that may be generated by a system, job, media, or device error.
<b>Backup Exec server</b>	Name of the Backup Exec server on which the job ran.
<b>Device Name</b>	Name of the device on which the job ran.
<b>Total Tasks</b>	Total number of jobs run within the last 24 hours.
<b>Uncorrected Exceptions</b>	Number of the jobs that fail and were not run again with successful completion.  Some of the archive jobs that ran in the past 24 hour period encountered exceptions. You must resolve the exceptions. Otherwise, the jobs that fail because of the exceptions continue to appear during subsequent 24 hour periods until the exceptions are resolved.
<b>Service Level</b>	Percentage of jobs that ran successfully.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Problem Files report

The Problem Files report lists all the problem files reported for jobs. The files are grouped by day and resource. You can limit the amount of data that appears in the report by selecting filter parameters for the Backed Up Server option and range parameters for the Days option.

Information displayed in the Problem Files report is described in the following table.

**Table 19-42** Problem Files report

Item	Description
<b>Date</b>	Date the problem file was encountered.
<b>Resource</b>	System on which the problem file is located.
<b>Time</b>	Time the problem file was encountered.
<b>Reason</b>	Error code listed in the job log summary.
<b>File Name</b>	Name of the problem file.
<b>Type</b>	Lists the type of job that Backup Exec ran when problematic files were detected.
<b>Backup Exec Server</b>	Name of the Backup Exec server on which the file is located.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Recently Written Media report

The Recently Written Media report lists all the media that has been modified within the specified period. You can limit the amount of data that appears in the report by selecting range parameters for the Hours option.

Information displayed in the Recently Written Media report is described in the following table.

**Table 19-43** Recently Written Media report

Item	Description
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.

**Table 19-43** Recently Written Media report (*continued*)

Item	Description
<b>Location</b>	Location of the media, such as the storage vault name or drive name.
<b>Set</b>	Name of backup set.
<b>Date and Time Modified</b>	Date and time media was last modified.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Resource Risk Assessment report

The Resource Risk Assessment report shows job information for resources on which the last backup job that was run on the resource failed. You can limit the amount of data that appears in the report by selecting filter parameters for the Backed Up Server option.

Information displayed in the Resource Risk Assessment report is described in the following table.

**Table 19-44** Resource Risk Assessment report

Item	Description
<b>Resource</b>	System on which the job ran.
<b>Error Text</b>	Describes the event that caused the job to fail.
<b>Start Time</b>	Time the operation started.
<b>Job</b>	Name of the job that failed.
<b>Error Category</b>	The category for the failed job that may be generated by a system, job, media, or device error.
<b>Backup Exec Server</b>	Name of the Backup Exec server on which the job ran.
<b>Device Name</b>	Name of the device on which the job ran.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Restore Set Details by Resource report

The Restore Set Details by Resource report lists all restore jobs that ran within the specified time range on a selected server. The jobs are grouped by the server and resource. You can limit the amount of data that appears in the report by entering filter parameters for the **Backed Up Server** option and range parameters for the **Hours** option.

Information displayed in the Daily Jobs by Resource report is described in the following table.

**Table 19-45** Resource Set Details by Resource report

Item	Description
<b>Resource</b>	Name of the system being backed up.
<b>Start Time</b>	Date and time the operation started.
<b>Duration</b>	Length of time the operation took to process.
<b>Size</b>	The amount of data processed.
<b>Files</b>	Number of files processed.
<b>Directories</b>	Number of directories processed.
<b>Data/Minute</b>	Amount of data processed per minute.
<b>Skipped</b>	Number of files skipped during the operation.
<b>Corrupt Files</b>	Number of corrupt files encountered during the operation.
<b>Files in Use</b>	Number of files in use during the operation.
<b>Status</b>	Status of the operation, such as Completed.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Resource Protected Recently report

The Resource Protected Recently report lists all job detail statistics and exceptions that occurred on a Backup Exec server for which you run this report.

**Table 19-46** Resource Protected Recently report

Item	Description
<b>Start Time</b>	Date and time the backup job started.
<b>Duration</b>	Amount of time it took to complete the backup job.
<b>Size</b>	Amount of data backed up.
<b>Files</b>	Number of files backed up.
<b>Directories</b>	Number of directories backed up.
<b>Size per Min</b>	Amount of data backed up per minute.
<b>Skipped</b>	Number of files skipped during the backup.
<b>Corrupt Files</b>	Number of corrupt files detected during the backup.
<b>Files in Use</b>	Number of files that were in use during the backup.
<b>Status</b>	Status of the backup job. See <a href="#">“Completed job statuses”</a> on page 263.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Retrieve Media from Vault report

The Retrieve Media from Vault report lists all reusable media currently in a specified media vault. You can limit the amount of data that appears in the report by selecting filter parameters for the **Vault** option.

Information displayed in the Retrieve Media from Vault report is described in the following table.

**Table 19-47** Retrieve Media from Vault report

Item	Description
<b>Cartridge Label</b>	Displays the name of the disk cartridge. Disk cartridge names cannot exceed 128 characters.  You can rename the disk cartridge.  See <a href="#">“Editing disk cartridge properties”</a> on page 317.
<b>Vault Name</b>	Displays the name of the vault where the media is located.
<b>Media Set Name</b>	Displays the name of the media set.
<b>Offsite Return Date</b>	Displays the date that the media was returned to the offsite vault.
<b>Recycle Date</b>	Displays the date after which the media can be overwritten.
<b>No Append Date</b>	Displays the date on which Backup Exec can no longer append data to the media.
<b>Rule Name</b>	Displays the name of vault media rule that is applied to the media.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Robotic Library Inventory report

The Robotic Library Inventory report lists the contents of slots in robotic libraries attached to Backup Exec servers. Usage statistics are provided for each piece of media. You can limit the amount of data that appears in the report by selecting filter parameters for the **Backup Exec server** option.

Information displayed in the Robotic Library Inventory report is described in the following table.

**Table 19-48** Robotic Library Inventory report

Item	Description
<b>Server</b>	Name of the server where the robotic library is located.
<b>Device Name</b>	Name of the robotic library.
<b>Slot</b>	Sequential number of the slot in the robotic library.
<b>Media Label</b>	Media label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned bar code label.

**Table 19-48** Robotic Library Inventory report (*continued*)

Item	Description
<b>State</b>	State of operation of the slot: paused, disabled, enabled, offline, or online.
<b>Modified</b>	Date the media in the slot was last accessed.
<b>Write</b>	Number of bytes that have been written to this media.
<b>Full</b>	Space available on a media; "1" indicates that media is full and "0" indicates that there is space available on the media.
<b>Hours</b>	Total number of hours this media has been in use.
<b>Mounts</b>	Total number of times this media has been mounted.
<b>Append</b>	The time remaining in the media's append period.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Scheduled Server Workload report

The Scheduled Server Workload report displays the estimated scheduled workload for a server during the next 24-hour period or a user-defined time period. The report only displays recurring jobs that have already run at least one time, not jobs scheduled to run once. You can use filter parameters for the **Backup Exec server** option to limit the amount of data that appears in the report. You can also enter range parameters for the **Hours** option.

Information displayed in the Scheduled Server Workload report is described in the following table.

**Table 19-49** Scheduled Server Workload report

Item	Description
<b>Backup Exec server</b>	Name of the Backup Exec server that will process the scheduled jobs.
<b>Job</b>	Name of the job scheduled to run.
<b>Next Due Date</b>	Time and day the next job is scheduled to run.
<b>Backup Size</b>	Estimated amount of data to be processed during the next 24 hours.

**Table 19-49** Scheduled Server Workload report (*continued*)

Item	Description
<b>Total Size</b>	Total amount of data to be processed on the server during the next 24 hours.
<b>Total Size</b>	Total amount of data to be processed on all Backup Exec servers.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Scratch Media Availability report

The Scratch Media Availability report shows the aging distribution of media, how many media are available for overwrite, and when other media will become available for overwrite. You can limit the amount of data that appears in the report by selecting range parameters for the **Days** option.

Information displayed in the Scratch Media Availability report is described in the following table.

**Table 19-50** Scratch Media Availability report

Item	Description
<b>Cartridge Label</b>	Cartridge label assigned by Backup Exec, assigned by the administrator, or contained on a pre-assigned barcode label  You can rename the cartridge.  See <a href="#">“Editing disk cartridge properties”</a> on page 317.
<b>Media Location Name</b>	Name of the storage device that contains the actual media.
<b>Total Capacity</b>	Total native capacity of the scratch media without using compression.
<b>Append Hours Remaining</b>	Capacity of scratch media available for append.
<b>Remaining Capacity</b>	Total amount of remaining native capacity of the scratch media without compression.
<b>Retention Hours Remaining</b>	The amount of time remaining to retain and protect the media from being overwritten.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Test Run Results report

The Test Run Results report displays the results for the test run jobs set for the selected period and the selected Backup Exec servers. You can limit the amount of data that appears in the report by selecting filter parameters for the **Backup Exec server** option and range parameters for the **Hours** option.

Information displayed in the Test Run Results report is described in the following table.

**Table 19-51** Test Run Results report

Item	Description
<b>Backup Exec server</b>	Name of the Backup Exec server on which the job ran.
<b>Job Date and Time Run</b>	Date and time the backup job was processed.
<b>Job Name</b>	Name of the test run job.
<b>Backup Sets</b>	Name of the backup set.
<b>Credential Check</b>	Indicates if the Backup Exec logon account was verified as correct for the resources being backed up.
<b>Backup Size</b>	Size in kilobytes, megabytes, or gigabytes of the backup.
<b>Media Type</b>	Type of media used, such as 4mm.
<b>Device Name</b>	Name of the device, such as the name of the robotic library.
<b>Max Needed</b>	Amount of space needed on the media to run the job.
<b>Online</b>	Capacity of media available in the device to which data can be appended.
<b>Media Total</b>	Total amount of appendable media available to the system.
<b>Online</b>	Capacity of media available in the device to which data can be written.
<b>Media Total</b>	Total amount of overwritable media available to the system.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Archive Job Success Rate report

The Archive Job Success Rate report displays the number of archive jobs for the backed up servers that successfully ran..

**Table 19-52** Archive Job Success Rate report

Item	Description
<b>Date</b>	Displays the date on which archive jobs ran.
<b>Total Jobs</b>	Displays the total number of archive jobs that have run.
<b>Successful</b>	Displays the total number of archive jobs that are successful.
<b>Success Rate</b>	Displays the success rate of the archive jobs in percentages.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Archive Selections by Archive Rules and Retention Categories report

The Archive Selections by Archive Rules and Retention Categories report displays the archive rules and the retention categories that are applied to each archive selection.

**Table 19-53** Archive Selections by Archive Rules and Retention Categories report

Item	Description
<b>Archive Rule</b>	Displays the archive rule that you specify to identify the files and mail messages that are eligible for archiving.
<b>Archive Selection</b>	<p>Displays only the archive selection.</p> <p>In the case of an NTFS archive, the network path appears.</p> <p>In the case of an Exchange mailbox archive, the mailbox group appears along with information about the mailbox group selections.</p>

**Table 19-53** Archive Selections by Archive Rules and Retention Categories report  
(continued)

Item	Description
<b>Archive Type</b>	Displays the type of data that you are archiving. Archive types include: <ul style="list-style-type: none"><li>■ File System Archive</li><li>■ Mailbox Archive</li></ul>
<b>Windows Domain</b>	Displays the Windows domain in which the archived selection resides.
<b>Retention Category</b>	Displays the retention category that applies to the file system selections in the archive job. A retention category specifies the time period for which you want to keep archived items.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Exchange Mailbox Group Archive Settings report

The Exchange Mailbox Group Archive Settings report displays the archive settings that are applied to mailbox groups in each domain.

**Table 19-54** Exchange Mailbox Group Archive Settings

Item	Description
<b>Windows Domain</b>	Displays the name of the Windows domain in which the Exchange server belongs.
<b>Mailbox Group</b>	Displays the name of the mailbox group to be archived.
<b>Archive Rules</b>	Displays the archive rule that is used to archive the mailbox group.

**Table 19-54** Exchange Mailbox Group Archive Settings *(continued)*

Item	Description
<b>Retention Category</b>	<p>Displays the retention category that applies to the mailbox group selections in the archive job.</p> <p>A retention category specifies the time period for which you want to keep archived items.</p>

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Failed Archive Jobs report

The Failed Archive Jobs report displays what archive jobs failed recently.

**Table 19-55** Failed Archive Jobs report

Item	Description
<b>Start Time</b>	Displays the time that the archive job started.
<b>Duration</b>	Displays the amount of time that the archive job took to run.
<b>Job Name</b>	Displays the name of the archive job.
<b>Category</b>	Displays status of the failed archive job.
<b>Error Code</b>	Displays the error code for the error that caused the archive job to fail.
<b>Description</b>	Displays the description of the error that caused the archive job to fail.
<b>Status</b>	Displays the category for the error that may be generated due to system, job, media, or device issues
<b>Device Name</b>	Displays the name of the storage device that processed the archive job.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## File System Archive Settings report

The File System Archive Settings report displays the archive settings that are applied to archive selections for each server.

**Table 19-56** NTFS Archive Settings report

Item	Description
<b>Server</b>	Displays the name of the Windows server from where the data was archived.
<b>Resource</b>	Displays the path of the resource.
<b>Archive Rules</b>	Displays the archive rule that is used to archive the files.
<b>Vault Store</b>	Displays the name of the vault store where the archived files reside.
<b>Retention Category</b>	Displays the retention category that applies to the file selections in the archive job.  A retention category specifies the time period for which you want to keep archived items.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Overnight Archive Summary report

The Overnight Archive Summary report displays the status of the archive jobs that ran in the last 24 hours.

**Table 19-57** Overnight Archive Summary report

Item	Description
<b>Resource</b>	Displays the name of the server that you are protecting.
<b>Type</b>	Displays the type of job that ran in the last 24 hours.
<b>Start Time</b>	Displays date and the time that the archive operation started.
<b>Status</b>	Displays the status of the archive operation.

**Table 19-57** Overnight Archive Summary report (*continued*)

Item	Description
<b>Error Category</b>	Displays the category for the error that may be generated due to system, job, media, or device issues.
<b>Backup Exec server</b>	Displays the name of the Backup Exec server on which the job ran.
<b>Device Name</b>	Displays the name of the device on which the job ran.
<b>Total Tasks</b>	Displays the total number of archive jobs that have run during the preceding 24 hours.
<b>Uncorrected Exceptions</b>	Displays the number of archive jobs that failed because the error condition was never corrected and were not run again with successful completion.
<b>Service Level</b>	Displays the percentage of jobs that ran successfully.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Vault Store Usage Details report

The Vault Store Usage Details report displays the archives that are in each store and the size of each archive.

**Table 19-58** Vault Store Usage Details report

Item	Description
<b>Vault Store</b>	Displays the name of the vault store where the Backup Exec archives are stored.
<b>Archive Name</b>	Displays the name that the Archiving Option gives to the archive.

**Table 19-58** Vault Store Usage Details report (*continued*)

Item	Description
<b>Archive Type</b>	Displays the type of data that you are archiving. Archive types include: <ul style="list-style-type: none"> <li>■ File System Archive</li> <li>■ Mailbox Archive</li> </ul>
<b>Number of Archived Items</b>	Displays number of archived items that are in the vault store.
<b>Total Size</b>	Displays the total size of the archived items in the vault store.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.

## Vault Store Usage Summary report

The Vault Store Usage Summary report displays the archived items that are in each vault store and the total size of the vault store.

**Table 19-59** Vault Store Usage Summary report

Item	Description
<b>Vault Store</b>	Displays the name of the disk-based vault store where the Backup Exec archives are stored.
<b>Database Name</b>	Displays the name of the vault store database that contains the configuration data and information about each of the archives in the partition.
<b>Vault Store Open Partition</b>	Displays the name of the vault store open partition where the Backup Exec archives are stored.
<b>Vault Store Partition Free Size</b>	Displays the amount of available free space in a vault store open partition.
<b>Number of Archives in Vault Store</b>	Displays the total number of existing Backup Exec archives in the vault store.

**Table 19-59** Vault Store Usage Summary report (*continued*)

Item	Description
<b>Total Size</b>	Displays the total size of the existing Backup Exec vault store archives.

See [“Running a report”](#) on page 558.

See [“Creating a custom report”](#) on page 567.



# Disaster preparation and recovery

This chapter includes the following topics:

- About disaster preparation
- About key elements of a disaster preparation plan (DPP)
- Returning to the last known good configuration
- Creating a hardware profile copy
- About using Windows' Automated System Recovery and System Restore to recover a Windows XP or Windows Server 2003 system
- About manual disaster recovery of Windows computers
- About a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)
- Running a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)
- About a disaster recovery operation of a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)
- Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)

## About disaster preparation

Disaster preparation planning is the implementation of strategies and procedures that will minimize damage in the event a catastrophe destroys your data. While precautions can be taken to minimize the effects of this type of occurrence (UPS devices, password protection, and so forth), unfortunately there is nothing that can safeguard your data 100 percent.

The purpose of a Disaster Preparation Plan (DPP) is to return to an operational status as quickly as possible. Backup Exec is a crucial component of the DPP and this section discusses how to apply this powerful data management tool to your DPP.

The following basic methods are available for disaster recovery:

- Automated recovery. Backup Exec's Simplified Disaster Recovery (SDR) option automates the disaster recovery process for Windows computers.
- Manual recovery. You can manually recover both local and remote Windows computers.

See [“About Simplified Disaster Recovery”](#) on page 704.

See [“Returning to the last known good configuration”](#) on page 636.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

## About key elements of a disaster preparation plan (DPP)

The DPP you put in place with your Backup Exec system should be tailored to your network environment.

While environments vary in different organizations, consider the following elements when creating a comprehensive DPP.

**Table 20-1** Key elements of a DPP

Element	Description
Hardware protection	The hardware devices on your network (CPUs, drives, video) are susceptible to damage from many disaster situations. Uninterruptible power supplies (UPS), surge protectors, and security monitoring devices are the equipment most often used today to protect hardware. If you do not already have these items in place, you should consider installing them. The initial investment could be justified many times over in the event of a disaster.

**Table 20-1** Key elements of a DPP (*continued*)

Element	Description
The ability to maintain business operations during a disaster period	Make sure that proper precautions are taken by everyone to implement plans for network interruptions. For example, the phones in the sales department won't stop ringing because the server is down, so orders may have to be handwritten until the server is up again. Each department should work out strategies for such occurrences. If the proper precautions are taken, the server can be rebuilt quickly and operations can still continue.
A sound backup strategy.	A well-designed backup strategy that includes a strong media rotation scheme plays a key role in quickly restoring your file server.
Off-site and duplicate stage backups.	It is imperative that backed up data be moved off-site regularly. If you use disk as your storage medium, consider adding a stage to duplicate backups to other storage. This ensures that if something happens to your facility, all of your backups will not be destroyed. Depending on the importance of your data, you may choose to use several off-site storage facilities. There are companies that provide off-site storage services that pick up and deliver tapes when they are to be rotated.
Effective DPP management	The last element - and possibly the most important - is proper management of your DPP strategy. A person or group of people should be charged with constantly supervising your organization's disaster preparation efforts. Someone should install and maintain hardware protection devices, make sure all departments have a plan if the server goes down temporarily, and make sure that backups are made and rotated off-site regularly. Also, it is a good idea to document your Disaster Preparation Plan for reference purposes.

Backup Exec plays a major role in your DPP by offering an easy, reliable way of backing up and restoring your files. The rest of this chapter describes how to take some precautionary measures to make restoration as straightforward as possible in the event of a disaster.

See [“Backing up data”](#) on page 163.

## Returning to the last known good configuration

Changes to the system configuration may keep the system from booting. If you suspect that boot problems are the result of a configuration change, you may be able to correct the problem by returning to a previous configuration. This method is simple and fast, and in some cases will correct boot problems in a Windows computer.

Any changes made to the system since the last time the configuration was saved are lost.

See [“Creating a hardware profile copy”](#) on page 636.

### To return to a previous configuration

- 1 Restart the system.
- 2 Press <F8> during startup.
- 3 Select one of the following options:

Safe Mode

This option allows you to diagnose and fix system startup problems. For more information, see your Microsoft documentation.

Last Known Good Configuration

This option allows you to return to a previous saved configuration.

## Creating a hardware profile copy

Before making a major hardware change, copy the current hardware profile to a new hardware profile and boot into the new profile before adding or changing the hardware. This way, you can return to the previous configuration if something does not work properly.

See [“Returning to the last known good configuration”](#) on page 636.

### To create a copy of the current hardware profile and make that the preferred boot option

- 1 Right-click the **My Computer** icon.
- 2 Click **Properties** to display the **System Properties** dialog box.
- 3 Click **Hardware**.
- 4 Click **Hardware Profiles**.
- 5 Select the current hardware profile, and then click **Copy**.

- 6 Type the name for the new configuration in the **To** field, and then click **OK**.
- 7 To make the new profile the preferred boot option, select it, and then click the up arrow next to the list box to move the new hardware profile to the top of the box.
- 8 Choose whether Windows is to use the new hardware profile automatically (after a delay) during startup, or if the system should wait indefinitely until the hardware profile is chosen by selecting the appropriate option.
- 9 Click **OK**.

## About using Windows' Automated System Recovery and System Restore to recover a Windows XP or Windows Server 2003 system

The ASR feature, which replaces the Emergency Repair Disk for Windows XP and Windows Server 2003, allows you to restore the operating system to a previous state so that you can start Windows XP Professional or Windows Server 2003 when other recovery methods do not work.

Microsoft recommends using System Restore, which saves only incremental changes and lets you start Windows XP Professional in normal or safe mode, before resorting to ASR. More information about ASR or System Restore is available. See your Microsoft documentation.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

## About manual disaster recovery of Windows computers

If your system is not protected by Simplified Disaster Recovery (SDR), you can manually recover a computer.

See [“Running a manual disaster recovery of a local Windows computer \(includes non-authoritative and authoritative restore of Active Directory for a domain controller\)”](#) on page 639.

If your system is protected by SDR, you should use automated disaster recovery.

See [“About Simplified Disaster Recovery”](#) on page 704.

The manual disaster recovery procedures restore your computer's operating system to its pre-disaster state and restore your data files, except those protected by one of the Backup Exec agents.

You should perform manual disaster recovery in the following situations:

- The Windows operating system has become corrupted and cannot be restored using the Emergency Repair Disks.
- The hard drive containing the Windows operating system has encountered an unrecoverable error that requires reformatting the disk.
- The hard drive that contains the Windows operating system needs to be replaced.

## About a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)

This procedure restores your computer's operating system to a pre-disaster state. It also restores your data files, except for those that are protected by one of the Backup Exec database agents, such as the Agent for Microsoft Exchange Server (Exchange Agent) or the Agent for Microsoft SQL Server (SQL Agent). If any of your data is protected by Backup Exec agents, refer to the section on restoring the data protected by the agent before beginning disaster recovery.

If your system is protected by Simplified Disaster Recovery (SDR), you should use SDR for disaster recovery.

See [“About Simplified Disaster Recovery”](#) on page 704.

The procedure described in the following section allows you to manually recover a computer not protected by SDR.

A storage device such as a tape drive or a robotic library must be attached to the computer that is being recovered.

You will also need the following items:

- A current full backup of the computer to be recovered and any subsequent incremental/differential backups.
- The Windows installation media.
- The Backup Exec installation media.

---

**Note:** If you recover a Windows computer that has BitLocker encryption enabled, you must re-enable BitLocker encryption following the restore.

---

See Microsoft's documentation for more information on BitLocker drive encryption.

See [“Running a manual disaster recovery of a local Windows computer \(includes non-authoritative and authoritative restore of Active Directory for a domain controller\)”](#) on page 639.

See [“About a disaster recovery operation of a remote Windows computer \(includes non-authoritative and authoritative restore of Active Directory for a domain controller\)”](#) on page 643.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

## Running a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)

Use the following steps to manually recover a local Windows computer, which includes non-authoritative and authoritative restore of Active Directory for a domain controller.

**To run a manual disaster recovery of a local Windows computer, which includes non-authoritative and authoritative restore of Active Directory for a domain controller**

### 1 Install the original version of Windows.

This basic Windows installation is necessary to provide Backup Exec with a target to which it can restore the system. The computer name, Windows directory, and the file system (such as NTFS) must be the same as the previous Windows installation. This installation will be overwritten by the backed up version, which will restore your original system configuration, application settings, and security settings.

If you are recovering from an entire hard disk failure, use Windows setup to partition and format the new disk during installation.

Format the partitions with the same file system as before the failure, as follows:

- If the system was in a specific domain or workgroup, do not join the domain or workgroup at this time.

**Running a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)**

- If you are recovering a domain controller, do not perform the domain controller installation process at this time.
- 2 Install Backup Exec to a directory other than where it was originally installed (this is a temporary installation).  
  
Always log on to Windows using the Administrator account or its equivalent during this procedure.
  - 3 Start Backup Exec.
  - 4 If you are using a tape drive, click **Configure Storage** on the **Storage** tab to install the appropriate device driver for the attached tape drive.
  - 5 Click **Inventory and Catalog** on the **Storage** tab to both inventory and catalog the media containing the latest full backup of the computer to be recovered.
  - 6 Restore all the backup sets from the full and incremental backups that contain logical drives on the hard disk. If differential backup sets are to be restored, select only the last differential set.
  - 7 Select the **Backup and Restore** tab, and then click **Restore**.
  - 8 Click **File and folder backups**, and then click **Next**.
  - 9 Select the drives that you want to restore, and then click **Next**.
  - 10 Select **To the original location**, and then click **Next**.
  - 11 Ensure that the option, **Restore over existing files** is selected and then accept the default selections on the **How do you want to maintain file integrity, heirarchy, and security for restored data** panel.
  - 12 Click **Next**.
  - 13 On the **How do you want to restore operating system features?** panel, click **Next**.
  - 14 On the **What additional tasks do you want to perform before and/or after a restore?** panel, click **Next**.
  - 15 Schedule the job to run, and then click **Next**.
  - 16 On the **Restore summary** panel, click **Finish**.
  - 17 After the restore job finishes, next restore the System State.
  - 18 On the **Backup and Restore** tab, click **Restore**.
  - 19 Click **Complete online restore of a computer, or restore system components**, and then click **Next**.
  - 20 Click **Active Directory, ADAM/AD LDS, and /or System State**, and the click **Next**.

- 21 Select the System State that you want to restore, and then click **Next**.
- 22 Restore the System State to its original location.
- 23 Ensure that the option, **Restore over existing files** is selected and then accept the default selections on the **How do you want to maintain file integrity, heirarchy, and security for restored data** panel.
- 24 Click **Next**.
- 25 If you are restoring a computer that is the only domain controller in the domain, or the entire domain is being rebuilt, an this is the first domain controller, select the option **Mark this server as the primary arbitrator for replication when restoring SYSVOL in System State**, and then click **Next**.
- 26 On the **Do you want to recreate deleted objects?** panel, select **No, do not recreate deleted objects**, and then click **Next**.
- 27 On the **What additional tasks do you want to perform before and/or after a restore?** panel, click **Next**.
- 28 Schedule the job to run, and then click **Next**.
- 29 On the **Restore summary** panel, click **Finish**.
- 30 If you are restoring a computer that is the only domain controller in the domain or the entire domain is being rebuilt and this is the first domain controller, reboot the computer after the restore job successfully completes.  
  
Your computer's operating system is now restored to a pre-disaster state. Your data files have been restored, except those protected by Backup Exec database agents.
- 31 Continue with one of the following:

If you are performing an authoritative restore go to step 32.

If you are not performing an authoritative restore the recovery is complete.

- 32 Do the following to change the Backup Exec services to the local system account.
  - Right-click **My Computer** and then select **Manage**.
  - From the left pane of the Computer Management utility, double-click **Services and Applications**.
  - Click **Services**.

**Running a manual disaster recovery of a local Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)**

- In the right pane, double-click each Backup Exec service, and from the Log On tab, change Log on as to use Local System account.
  - Close the Computer Management utility.
- 33** Restart the computer.
- 34** Press **F8** during startup.
- A menu appears that allows you to diagnose and fix system startup problems.
- 35** Select **Directory Services Restore Mode**.
- 36** Start Backup Exec.
- 37** Run the Restore Wizard and select **Complete online restore of a computer, or restore system components**.
- 38** Select System State or Shadow Copy components as the restore selections, and then run the restore job.
- 39** At this point, you can either choose to restore the entire Active Directory, or specific objects from the Active Directory.

Restore the entire Active Directory by performing the following:

- Open a command prompt.
- Type NTDSUTIL and press **Enter**.
- Type Authoritative Restore and press **Enter**.
- Type Restore Database, press **Enter**, click **OK** and then click **Yes**.

See Microsoft's documentation for running NTDSUTIL for Windows Server 2008/2008 R2.

Restore specific objects from the Active Directory by performing the following:

- Open a command prompt.
- Type NTDSUTIL and press **Enter**.
- Type Authoritative Restore and press **Enter**.
- Type Restore Subtree "ou=<OU Name>.dc=<domain name>.dc=<xxx>" (without the quotation marks), and then press **Enter**, where <OU Name> is the name of the organizational unit you want to restore, <domain name> is the domain name the OU resides in, and <xxx> is the top level domain name of the domain controller, such as com, org, or net. You can do this as many times for as many objects you need to restore.

- 40 Once you have finished restoring Active Directory information, exit NTDSUTIL.
- 41 Restart the computer.

## About a disaster recovery operation of a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)

You can perform a disaster recovery on a remote computer that is attached to the Backup Exec server. This procedure restores your computer's operating system to its pre-disaster state. It also restores your data files, except those that you protect with a Backup Exec agent.

If any of your data is protected by Backup Exec agents, review the overview of the agents before you begin disaster recovery.

If your system is protected by Backup Exec Simplified Disaster Recovery (SDR), you should use SDR for disaster recovery.

See [“About Simplified Disaster Recovery”](#) on page 704.

The procedure described in the following section allows you to manually recover a computer not protected by SDR.

You will need the following:

- A current full backup of the computer to be recovered and any subsequent incremental/differential backups.
- The Windows installation media.

Always log on to Windows using the Administrator account or its equivalent during this procedure.

---

**Note:** If you recover a Windows computer that has BitLocker encryption enabled, you must re-enable BitLocker encryption following the restore.

---

See Microsoft's documentation for more information on BitLocker drive encryption.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

## Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)

Use the following steps to run a disaster recovery operation on a remote Windows computer.

### To run a disaster recovery operation on a remote Windows computer

- 1 At the remote computer, install the original version of Windows.

This basic Windows installation is necessary to provide Backup Exec with a target to which it can restore the system. The computer name, Windows directory and the file system (such as NTFS) must be the same as the previous Windows installation. This basic installation will later be overwritten by the backed up version, which will restore your system configuration, application settings, and security settings.

If you are recovering from an entire hard disk failure, use Windows setup to partition and format the new disk during installation.

Format the partitions with the same file system as before the failure, as follows:

- If the system was in a specific domain or workgroup, do not join the domain or workgroup at this time.
- If you are recovering a domain controller, do not perform the domain controller installation process at this time.

- 2 At the Backup Exec server, install the Backup Exec Agent for Windows on the remote computer.

See [“About installing the Agent for Windows”](#) on page 83.

- 3 Start Backup Exec.
- 4 If you are using a tape drive, use the **Configure Storage** on the **Storage** tab to install the appropriate device driver for the attached tape drive.
- 5 Click **Inventory and Catalog** on the **Storage** tab to both inventory and catalog the media containing the latest full backup of the computer to be recovered.
- 6 Restore all the backup sets from the full and incremental backups that contain logical drives on the hard disk. If differential backup sets are to be restored, select only the last differential set.
- 7 Select the **Backup and Restore** tab, and then click **Restore**.

- 8 Click **Complete online restore of a computer, or restore system components**, and then click **Next**.
- 9 Click **File and folder backups**, and then click **Next**.
- 10 Select the drives that you want to restore, and then click **Next**.
- 11 Select **To the original location**, and then click **Next**.
- 12 Accept the default selections on the **How do you want to maintain file integrity, heirarchy, and security for restored data** panel, and then click **Next**.
- 13 On the **How do you want to restore operating system features?** panel, click **Next**.
- 14 On the **What additional tasks do you want to perform before and/or after a restore?** panel, click **Next**.
- 15 Schedule the job to run, and then click **Next**.
- 16 On the **Restore summary** panel, click **Finish**.
- 17 After the restore job finishes, you must restore the System State.
- 18 On the **Backup and Restore** tab, click **Restore**.
- 19 Click **Complete online restore of a computer, or restore system components**, and then click **Next**.
- 20 Click **Active Directory, ADAM/AD LDS, and /or System State**, and the click **Next**.
- 21 Select the System State that you want to restore, and then click **Next**.
- 22 Restore the System State to its original location.
- 23 Ensure that the option, **Restore over existing files** is selected and then accept the default selections on the **How do you want to maintain file integrity, heirarchy, and security for restored data** panel.
- 24 If you are restoring a computer that is the only domain controller in the domain, or the entire domain is being rebuilt an this is the first domain controller, select the option **Mark this server as the primary arbitrator for replication when restoring SYSVOL in System State**, and then click **Next**.
- 25 On the **Do you want to recreate deleted objects?** panel, select **No, do not recreate deleted objects**, and then click **Next**.
- 26 On the **What additional tasks do you want to perform before and/or after a restore?** panel, click **Next**.
- 27 Schedule the job to run, and then click **Next**.
- 28 On the **Restore summary** panel, click **Finish**.

**Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)**

**29** If you are restoring a computer that is the only domain controller in the domain or the entire domain is being rebuilt and this is the first domain controller, reboot the computer after the restore job successfully completes.

Your computer's operating system is now restored to its pre-disaster state. Your data files have been restored, except those protected by Backup Exec database agents.

**30** Continue with one of the following:

If you are performing an authoritative restore go to step 31.

If you are not performing an authoritative restore the recovery is complete.

**31** At the remote server, press **F8** during startup.

A menu appears that allows you to diagnose and fix system startup problems.

**32** Select **Directory Services Restore Mode**.

**33** At the Backup Exec server, start Backup Exec.

**34** Run the Restore Wizard and select **Complete online restore of a computer, or restore system components**.

**35** Select System State or Shadow Copy components as the restore selections, and then run the restore job.

**36** Run the Restore job.

**37** At the remote server, do the following:

**38** At this point, you can either choose to restore the entire Active Directory, or specific objects from the Active Directory:

Restore the entire Active Directory by performing the following:

- Open a command prompt.
- Type NTDSUTIL and press **Enter**.
- Type Authoritative Restore and press **Enter**.
- Type Restore Database, press **Enter**, click **OK** and then click **Yes**.

See Microsoft's documentation for running NTDSUTIL on Windows Server 2008/2008 R2.

Restore specific objects from the Active Directory by performing the following:

- Open a command prompt.

**Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)**

- Type NTDSUTIL and press **Enter**.
  - Type Authoritative Restore and press **Enter**.
  - Type Restore Subtree "ou=<OU Name>.dc=<domain name>,dc=<xxx>" (without the quotation marks), and then press **Enter**, where <OU Name> is the name of the organizational unit you want to restore, <domain name> is the domain name the OU resides in, and <xxx> is the top level domain name of the domain controller, such as com, org, or net. You can do this as many times for as many objects you need to restore.
- 39** Once you have finished restoring Active Directory information, exit NTDSUTIL.
- 40** Restart the computer.

648 | Disaster preparation and recovery

**Running a disaster recovery operation on a remote Windows computer (includes non-authoritative and authoritative restore of Active Directory for a domain controller)**

# Troubleshooting Backup Exec

This chapter includes the following topics:

- [Troubleshooting hardware-related issues](#)
- [How to get more information about alerts and error messages](#)
- [Troubleshooting backup issues](#)
- [Troubleshooting failed components in the SAN](#)
- [How to improve Backup Exec's performance](#)
- [Accessing Symantec Online](#)
- [About the Symantec Knowledge Base](#)
- [About contacting Technical Support](#)
- [About Backup Exec diagnostic tools](#)
- [About the Symantec Backup Exec Support Tool](#)
- [About the Backup Exec diagnostic application](#)
- [Running the begather utility to troubleshoot Backup Exec components on Linux servers](#)
- [Using the Backup Exec Debug Monitor for troubleshooting](#)
- [About the Backup Exec debug tool](#)

# Troubleshooting hardware-related issues

For common hardware-related issues, review the following frequently asked questions:

**Table 21-1** Hardware-related questions

Question	Answer
How do I know if my storage device is supported?	<p>You can find a list of compatible devices at the following URL:</p> <p><a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a></p> <p>If your drive is listed on the hardware compatibility list, run the Configure Storage wizard and install Symantec device drivers.</p> <p>See “<a href="#">About the Configure Storage wizard</a>” on page 145.</p> <p>From the Configure Storage wizard, the Symantec Device Driver Installation wizard finds and installs the most suitable driver for your tape drive.</p>
How can I troubleshoot issues with a robotic library or tape drive?	<p>You can find troubleshooting tips and a video tutorial about configuring and troubleshooting tape drive hardware at the following URL:</p> <p><a href="http://www.symantec.com/business/support/index?page=content&amp;id=TECH24414">http://www.symantec.com/business/support/index?page=content&amp;id=TECH24414</a></p> <p>See “<a href="#">Starting and stopping Backup Exec services</a>” on page 511.</p> <p>See “<a href="#">Deleting a storage device</a>” on page 421.</p>

**Table 21-1** Hardware-related questions (*continued*)

Question	Answer
<p>I'm getting an error "Storage device [device] reported an error on a request to read or write data to or from media. Error reported: Data error (cyclic redundancy check)." What should I do?</p>	

**Table 21-1** Hardware-related questions (*continued*)

Question	Answer
	<p>Many factors can cause the cyclic redundancy check (CRC) error.</p> <p>The following list contains the most common reasons for this error and potential ways to resolve the problem:</p> <ul style="list-style-type: none"> <li>■ Contaminated read and write heads of the tape device. Check with the hardware manufacturer for proper cleaning techniques.</li> <li>■ Bad media. Replace the media. Try a new tape that the hardware manufacturer has certified.</li> <li>■ Tape driver. Load the appropriate Backup Exec tape driver. You can find a list of compatible devices at the following URL: <a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a></li> <li>■ Wide negotiation for the SCSI controller is not configured properly. If the device is a wide (68 pin) SCSI device, then wide negotiation may and should be used. If the device is a narrow (50 pin) SCSI device, disable wide negotiation. Use the manufacturer's SCSI installation program to disable wide negotiation on the SCSI controller card.</li> <li>■ SCSI controller transfer rate is too fast. Use the manufacturer's SCSI installation program to lower the SCSI transfer rate. Check with the manufacturer of the controller and the device for the proper configuration for the SCSI transfer rate.</li> <li>■ SCSI controller synchronous negotiation enabled.</li> </ul>

**Table 21-1** Hardware-related questions (*continued*)

Question	Answer
	<p>Use the manufacturer's SCSI installation program to disable synchronous negotiation on the SCSI controller card. Check with the manufacturer of the controller and the device for the proper configuration for SCSI synchronous negotiation.</p> <ul style="list-style-type: none"> <li>■ Incorrect termination or bad cables. Verify that the SCSI cable is good and that it is configured to provide proper SCSI termination. Do not mix passive and active termination.</li> <li>■ Confirm that the tape drive functions properly. Check with the tape drive manufacturer for diagnostic software to test the condition of the tape drive hardware.</li> <li>■ General SCSI problems. Isolate the tape drive on its own controller card or try a different SCSI card.</li> </ul>
<p>Why does my DLT tape drive pause when it catalogs some tapes?</p>	<p>The DLT tape drive maintains internal information about the tape on a tape directory track. The directory track is updated before the tape is ejected from the drive. If the drive is turned off without ejecting the tape first, this information is lost.</p> <p>Re-generating the tape directory information takes several hours to complete, which makes it seem like the drive is hung. Allow sufficient time for the operation to complete and then eject the tape. Normal operation resumes after the directory track is updated.</p>

**Table 21-1** Hardware-related questions (*continued*)

Question	Answer
A backup to my DLT tape drive is stuck at 99% complete. What should I do?	<p>The backup most likely fails to complete because the storage option <b>Eject media after job completes</b> is selected, and the tape drive does not support the operation. Some tape drives require you to manually remove the tape, such as Digital Linear Tape (DLT), Linear Tape-Open (LTO), Travan, and Onstream drives.</p> <p>To remedy this situation, either uncheck the storage option <b>Eject media after job completes</b>, or configure an automatic response to the active alert.</p> <p>See <a href="#">“Storage options”</a> on page 190.</p> <p>See <a href="#">“Configuring alert categories”</a> on page 286.</p>

## How to get more information about alerts and error messages

Backup Exec generates an error message when a condition occurs that is important enough to warrant your attention, or requires that you submit a response. Most alerts and error messages are self explanatory, but there may be times when you need to get more information to resolve a condition.

You can get more information on Backup Exec alert and error messages in the following ways:

- On the alert message, click the link for more information, or look in the job log and click the UMI link. This code is a hyperlink to the Symantec Technical Support Web site. You can access the technical notes that are related to the alert.  
See [“Linking from the job log to the Symantec Technical Support Web site”](#) on page 266.
- Search the Symantec Technical Support knowledge base for the error.  
See [“Searching the Symantec Knowledge Base”](#) on page 663.

# Troubleshooting backup issues

If you have problems with backing up data, review the following questions.

**Table 21-2** Backup questions

Question	Answer
<p>I am unable to back up certain files on my system that are in use by other processes. Why is that?</p>	<p>For non-snapshot backups, when Backup Exec encounters a file that is in use by another process, it either skips the file or waits for the file to become available. These actions depend on the options for no-snapshot backups that you configure when you create the backup.</p> <p>See <a href="#">“Files and Folders options”</a> on page 204.</p> <p>If you configure Backup Exec to back up open files with a lock, it attempts to open the files in a different mode. It locks these files during backup to prevent other processes from writing to them. Symantec recommends that you close the applications that leave files open so that the files are backed up in a consistent state.</p> <p>To back up open files on Windows computers, use the Advanced Open File options to configure the backups that use snapshot technology.</p> <p>See <a href="#">“Advanced Open File options”</a> on page 199.</p>
<p>Why do the Backup Exec Administration Console continue to own a storage device even when it's not running?</p>	<p>Backup Exec is a client/server application that must always be available to process the jobs that are submitted from both local and remote administrative consoles.</p> <p>The Backup Exec services claim all of the storage devices that are attached to the Backup Exec server whenever the services are running. Backup Exec requires constant control of the storage devices to collect statistics on media and storage device usage, and to provide media overwrite protection when necessary.</p>

**Table 21-2** Backup questions (*continued*)

Question	Answer
<p>When I run a local backup, the total number of bytes backed up by Backup Exec does not match the number of bytes displayed by Windows. Why?</p>	<p>The type of partition for which the system is formatted may cause this problem.</p> <p>If you have a Windows NTFS compressed partition, Backup Exec displays the uncompressed byte count of the files that are backed up. Meanwhile, Windows Explorer displays the compressed byte count of the files on the hard drive. For example, Windows compresses an NTFS partition that contains 1 GB of data to 500 MB. Backup Exec reports that 1 GB of data was backed up, even though Windows Explorer displays that only 500 MB of compressed data exists on the hard drive.</p> <p>If you have a FAT partition, Backup Exec reports the actual number of bytes of the files being backed up while File Manager reports an inflated amount of disk space. For example, a 2 GB FAT partition has a 32-K cluster size and File Manager displays 1.9 GB of used space. Backup Exec reports that 1.4 GB of data was backed up. Assuming that a 50-MB pagefile.sys is excluded from the backup, there is a 450-MB difference in the number of bytes.</p> <p>Converting to NTFS regains disk space since it is more efficient and the default cluster size (automatically set by Windows) in NTFS is less than FAT. Windows lets you specify a cluster size other than the default; however system performance may decrease. For more information, see the Windows documentation.</p>

## Troubleshooting failed components in the SAN

Various problems can occur at any location in a SAN.

For Backup Exec to work properly, a storage device has to be recognized in the following locations:

- The bridge or router must recognize it as a SCSI device
- The operating system must recognize it as a device
- Backup Exec must recognize it as a supported device

In some cases, hardware issues may require you to contact your hardware vendor for technical support.

You may need to replace a component of your SAN, such as a bridge or a switch. For specific steps for replacing your equipment, refer to your hardware vendor’s documentation.

See “[Troubleshooting offline storage devices in a SAN](#)” on page 657.

## Troubleshooting offline storage devices in a SAN

If a device in your SAN has gone offline, follow these steps to determine the source of the problem.

Before you begin troubleshooting, verify that your storage devices are on the Backup Exec supported device list.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

Also, verify that all hardware drivers are up to date and are started. If you find errors with your hardware, contact your hardware vendor for specific instructions.

**Table 21-3** Troubleshooting offline storage devices in a SAN

Step	Action
Step 1	<p>Use the Windows Device Manager to verify that the operating system recognizes the device.</p> <p>If the device is not recognized, you may need to troubleshoot the device.</p> <p>See “<a href="#">Finding hardware errors in a SAN</a>” on page 659.</p>
Step 2	<p>For robotic libraries, verify that robotic library support is installed.</p> <p>See “<a href="#">About the Library Expansion Option</a>” on page 335.</p>

**Table 21-3** Troubleshooting offline storage devices in a SAN (*continued*)

Step	Action
Step 3	<p>Check the system event log for the following errors, which indicate SAN communication errors: SCSI errors 9, 11, and 15, or timeout errors relating to storage. Check the application event log for multiple events 33152. These events indicate SAN communication errors.</p> <p>See <a href="#">“Finding hardware errors in a SAN”</a> on page 659.</p> <p>You may need to contact your hardware vendor.</p>
Step 4	<p>If the library is online, but some or all of the drives are offline, use Backup Exec to initialize the library.</p> <p>See <a href="#">“Initializing a robotic library”</a> on page 426.</p>
Step 5	<p>If initializing the library does not bring the storage devices online, check the library for an error display on the front panel, mechanical problems, or tapes inappropriately in the drives. Correct any errors that you find.</p>
Step 6	<p>If no errors exist on the library or if you corrected the errors and the storage devices are still offline, stop Backup Exec services and then restart.</p> <p>See <a href="#">“Starting and stopping Backup Exec services”</a> on page 511.</p>
Step 7	<p>If restarting the services does not bring the storage devices online, restart the operating system. Be sure that no Backup Exec jobs are running when you restart.</p>

**Table 21-3** Troubleshooting offline storage devices in a SAN (*continued*)

Step	Action
Step 8	<p>If restarting the operating system does not bring the storage devices online, reset the SAN to help identify problem tape storage. Recycling the SAN may also resolve Fibre Channel problems.</p> <p>See <a href="#">“Resetting the SAN”</a> on page 660.</p>

## Finding hardware errors in a SAN

Use the following steps to find the common hardware errors that occur in a SAN. If you find errors with your hardware, contact your hardware vendor for specific instructions.

**Table 21-4** Finding hardware errors in a SAN

Step	Action
Step 1	Verify that the proper device drivers are installed.
Step 2	Verify that the fibre cable is securely connected to the HBA and to the fibre switch.
Step 3	Verify that the fibre connection is properly connected to the robotic library from the fibre switch.
Step 4	Check for a failed hardware component between the server and the fibre switch. Sometimes some of the servers in the SAN recognize the storage device, but other servers do not. If none of the servers in the SAN recognize the storage device, check for a failed hardware component between the fibre switch and the storage device.
Step 5	<p>Reset the SAN, which may identify problem hardware components and may resolve fibre problems.</p> <p>See <a href="#">“Resetting the SAN”</a> on page 660.</p>

## Resetting the SAN

Resetting the SAN involves turning off the components of the SAN, and then powering them on in a specific order.

**Table 21-5**      Resetting the SAN

Step	Action
Step 1	Turn off all servers, robotic libraries, and fibre bridges in the SAN.  In rare cases, you may need to turn off the fibre switch also. If you need to turn off the switch, you should power it on before any other components. Wait for all checks to complete before you turn on the other components.
Step 2	Turn on the robotic library.  See <a href="#">“Initializing a robotic library”</a> on page 426.
Step 3	Verify that the fibre switch recognizes the robotic library.
Step 4	Turn on the central administration server.
Step 5	Verify that the operating system recognizes the robotic library and its drives.
Step 6	Turn on one of the managed Backup Exec servers. Wait for the managed Backup Exec server to start before you turn on the other managed Backup Exec servers.

## Bringing storage devices online after an unsafe device removal event in a SAN

If a storage device is in use by Backup Exec at the time of an unsafe device removal event, the device appears as offline in Backup Exec.

**Table 21-6**      How to bring a device online after an unsafe device removal event

Step	Action
Step 1	Verify that no Backup Exec jobs are running in the SAN.

**Table 21-6** How to bring a device online after an unsafe device removal event  
*(continued)*

Step	Action
Step 2	Use Backup Exec to initialize the robotic library if the library is online but the drives are offline.  See <a href="#">"Initializing a robotic library"</a> on page 426.
Step 3	Stop all Backup Exec services and then restart them if the library is offline or if the drives are offline after initialization.  If the device is not online, you may need to troubleshoot the device.  See <a href="#">"Finding hardware errors in a SAN"</a> on page 659.

## How to improve Backup Exec's performance

To get the best performance from Backup Exec, you should review several factors:

- Data transfer path
- Backup Exec agent performance
- Network performance
- Backup Exec server performance
- Storage device performance

For more information on how to measure and tune the performance of these items, go to the following URL:

<http://entsupport.symantec.com/umi/V-269-38>

## Accessing Symantec Online

You can access Symantec community forums, learn about training courses, and view Symantec Web sites.

**Table 21-7** Symantec Online menu items

Item	Description
<b>Share Your Ideas</b>	Connects you to the SymConnect forum where you can post your ideas for improving Backup Exec.  You can also access SymConnect at the following URL:  <a href="http://www.symantec.com/connect/">http://www.symantec.com/connect/</a>
<b>Education Services</b>	Provides the links to all Symantec Education training and custom learning services.
<b>Backup Exec Training</b>	Provides the links to Backup Exec training courses, certification programs, classroom locations, and other information about training.
<b>Backup Exec Page</b>	Provides the links to resources for Backup Exec.
<b>Symantec Home Page</b>	Connects you to the Symantec Web site.

**To access Symantec Online**

- ◆ Click the Backup Exec button, select **Symantec Online**, and then select the appropriate menu item.

See “[About the Symantec Knowledge Base](#)” on page 662.

## About the Symantec Knowledge Base

The Symantec Knowledge Base is a centralized location where you can find more information about Symantec products. The knowledge base contains information about how to install, upgrade, configure, and use Symantec products. It also contains information about requirements, best practices, and how to troubleshoot problems. The Symantec Knowledge Base is accessible from within Backup Exec.

---

**Note:** You must have an active Internet connection to access the Symantec Knowledge Base.

---

The knowledge base uses a keyword-based search technology. It focuses on the important keywords in a search and compares them to other search phrases to provide the best possible results. You can use Boolean search features and

expression queries to provide search parameters. For best results, focus on a few keywords that best represent your question.

See “[Searching the Symantec Knowledge Base](#)” on page 663.

See “[About contacting Technical Support](#)” on page 663.

## Searching the Symantec Knowledge Base

When you search the knowledge base, a new browser window launches and displays the search results.

See “[About the Symantec Knowledge Base](#)” on page 662.

### To search the Symantec Knowledge Base

- 1 Do either of the following:
  - Click the Backup Exec button, select **Technical Support**, and then select **Search Knowledge Base**.
  - On the **Home** tab, in the **Support** group, ensure that **Technical Support** is checked. Then, in the **Technical Support** panel, click **Symantec Technical Support**.
- 2 Enter a keyword or phrase, and then click the search icon.

## About contacting Technical Support

If you have tried to solve a problem, but still need a resolution, you can use Symantec's **MySupport** to contact Technical Support over the Internet, or by phone.

You can find a list of phone numbers at the following URL:

<http://entsupport.symantec.com/phonesup>

To expedite the Technical Support process, do the following:

- Know your Backup Exec version and revision number.
- Use one of the diagnostic utilities that included with Backup Exec to collect the information that technical support can use to diagnose your issue.

See “[Displaying the Backup Exec version](#)” on page 134.

See “[About the Backup Exec diagnostic application](#)” on page 665.

See “[Accessing Symantec Online](#)” on page 661.

## About Backup Exec diagnostic tools

The following diagnostic tools help to troubleshoot issues in Backup Exec:

**Table 21-8** Backup Exec diagnostic tools

Item	Description
Backup Exec Support Tool	Scans the local computer and generates a report about common issues in your Backup Exec environment.  See <a href="#">“About the Symantec Backup Exec Support Tool”</a> on page 664.
Backup Exec diagnostic application	Gathers the pertinent information about a Windows computer for troubleshooting.  See <a href="#">“About the Backup Exec diagnostic application”</a> on page 665.
Gather utility for Linux servers	Creates and compiles a Packet file. The file contains detailed information about installation, diagnostics, and error reports.  See <a href="#">“Running the begather utility to troubleshoot Backup Exec components on Linux servers”</a> on page 670.
Backup Exec Debug Monitor	Captures the debug output from Backup Exec and saves it into debug logs.  See <a href="#">“Using the Backup Exec Debug Monitor for troubleshooting”</a> on page 670.
Backup Exec debug tool	Generates the diagnostic information about the Backup Exec processes that shut down unexpectedly.  See <a href="#">“About the Backup Exec debug tool”</a> on page 671.

## About the Symantec Backup Exec Support Tool

The Symantec Backup Exec Support Tool is a diagnostic tool that scans the local computer and generates a report about common issues in your Backup Exec environment. You can view the report and try to resolve the issues before you contact Symantec Technical Support. If you cannot resolve the issues, you can choose to collect data to send to Symantec Technical Support.

The report identifies issues with items such as the following:

- Minimum system requirements
- Backup Exec service account
- Backup Exec service account credentials
- Windows Removable Storage service

You can find a description of the report and more information about the report at the following URL:

<http://entsupport.symantec.com/umi/V-370-2378-00002>

You can find more information about the Backup Exec Support Tool at the following URL:

<http://entsupport.symantec.com/umi/V-370-2378-00001>

See “[Running the Backup Exec Support Tool](#)” on page 665.

## Running the Backup Exec Support Tool

You can use the Backup Exec Support Tool to run a system analysis or collect data for technical support. When you run the Backup Exec Support Tool, it automatically checks for an updated version of the tool. If there is a new version, Backup Exec automatically downloads and runs the new version.

You can also find the latest version of the Backup Exec Support Tool at the following URL:

<http://entsupport.symantec.com/umi/V-370-2378-00003>

See “[About the Symantec Backup Exec Support Tool](#)” on page 664.

### To run the Backup Exec Support Tool

- 1 Click the Backup Exec button, select **Technical Support**, and then select **Run the Support Tool to resolve issues**.
- 2 Follow the on-screen prompts.

## About the Backup Exec diagnostic application

Backup Exec includes a diagnostic application (Bediag.exe) that gathers information about a Windows computer for troubleshooting purposes. You can run it from the Backup Exec server, or from a remote computer. This application can be run from within Backup Exec, or it can be run from a command line. The Bediag command line utility is located in the Backup Exec directory on your hard drive (by default, `\Program Files\Symantec\Backup Exec`).

The type of information collected in the bediag.txt file includes the following:

- Account groups, account privileges, and environment settings
- Backup Exec software version and registry information, Backup Exec agent listing, Windows version information, SCSI hardware configuration, SQL Server information, Driver services information, and Windows Services information.
- Server information, supported shared directories, and Windows sockets information.

See [“Generating a diagnostic file for troubleshooting”](#) on page 666.

See [“Generating a diagnostic file on a remote Backup Exec server”](#) on page 669.

See [“Using the command line to generate a diagnostic file for troubleshooting”](#) on page 667.

## Generating a diagnostic file for troubleshooting

You can run the Backup Exec diagnostic application to gather information for troubleshooting. Diagnostic information appears in a text file.

See [“About the Backup Exec diagnostic application”](#) on page 665.

### To generate a diagnostic file for troubleshooting

- 1 Click the Backup Exec button, select **Technical Support**, and then select **Backup Exec Diagnostics**.
- 2 Select the appropriate options.  
See [“Backup Exec Diagnostics”](#) on page 666.
- 3 Click **Run Diagnostics**.
- 4 Click **Close**.

## Backup Exec Diagnostics

You select a server and generate a diagnostic file to gather information for troubleshooting.

See [“Generating a diagnostic file for troubleshooting”](#) on page 666.

**Table 21-9** Backup Exec Diagnostics options

Item	Description
Select Server	Displays the name of the Backup Exec server on which you want to run diagnostics.

**Table 21-9** Backup Exec Diagnostics options (*continued*)

Item	Description
<b>User name</b>	Indicates the user name for an account that has rights on the Backup Exec server.
<b>Password</b>	Indicates the password for an account that has rights the Backup Exec server.
<b>Domain</b>	Indicates the domain in which the Backup Exec server is located.
<b>Select Server</b>	Lets you select a different server on which to run the diagnostic application.
<b>View Last Diagnostics Results</b>	Displays the results of the last diagnostics utility that was run.
<b>Run Diagnostics</b>	Runs the diagnostic application to gather information for troubleshooting purposes.

## Using the command line to generate a diagnostic file for troubleshooting

You can run the Backup Exec diagnostic application from the command line to gather information for troubleshooting.

See [“About the Backup Exec diagnostic application”](#) on page 665.

**To use the command line to generate a diagnostic file for troubleshooting**

- 1 Launch the command prompt.
- 2 Do one of the following:

To generate a diagnostic file for a Backup Exec server      From the directory `Program Files\Symantec\Backup Exec\`, type *bediag [switches] servername* .  
 See [“Command line switches for a diagnostic file”](#) on page 668.

To generate a diagnostic file for a remote computer      From the directory `Program Files\Symantec\Backup Exec\`, type *bediag [switches] workstationname*.  
 See [“Command line switches for a diagnostic file”](#) on page 668.

- 3 Open the "Bediag.txt" from the directory that contains Bediag.exe (by default `Program Files\Symantec\Backup Exec`).

## Command line switches for a diagnostic file

You can add the following switches to gather additional information when you generate a diagnostic file for troubleshooting.

See [“Using the command line to generate a diagnostic file for troubleshooting”](#) on page 667.

**Table 21-10**      Command line switches for a diagnostic file

Switch	Description
/a	Dumps the Agent List.
/b:[server]	Specifies a Backup Exec server to poll for service account information.
/c	Dumps the Backup Exec software configuration from the registry.
/app	Dumps the Application Event log.
/sys	Dumps the system event log.
/bex	Dumps only the Backup Exec entries that are in the Application Event log.
/err	Dumps only the error events from any event log.

**Table 21-10** Command line switches for a diagnostic file (*continued*)

Switch	Description
/recs:n	Dumps only the newest records from given event logs.
	The <code>bex</code> , <code>err</code> , and <code>recs</code> switches must be used with the <code>app</code> switch and the <code>sys</code> switches.
/o:[file]	Specifies the output job log for append.
	Omitting [file] sends output to the screen.
/h	Dumps the SCSI hardware subkey from registry.
/l	Dumps the Lotus Notes information.
/n	Dump Windows Socket Network Protocols.
/p	Dumps the user privileges.
	Dumps the Microsoft SQL Server information.
/s	Dumps the information on Services.
/u	Dumps Microsoft update information.
/v	Dumps Server Information.
/w	Dumps Windows version information.
/x	Dumps Microsoft Exchange Server Information.
/?	Displays usage information.

## Generating a diagnostic file on a remote Backup Exec server

You can run diagnostics on a remote Backup Exec server if the following requirements are met:

- Backup Exec is installed on the remote server.
- Backup Exec services are running.

Diagnostic information appears in a text file.

### To generate a diagnostic file on a remote Backup Exec server

- 1 Click the Backup Exec button, select **Technical Support**, and then select **Backup Exec Diagnostics**.
- 2 Click **Select Server** and select the remote Backup Exec server on which you want to run the diagnostic utility.

- 3 Select the appropriate options.  
See “[Backup Exec Diagnostics](#)” on page 666.
- 4 Click **Run Diagnostics**.
- 5 Click **Close**.

## Running the begather utility to troubleshoot Backup Exec components on Linux servers

The begather utility brings together the files that help you diagnose issues with Backup Exec components on Linux servers. After you run it, the begather utility displays the name of the Packet file that it creates. The files that are gathered contain detailed information regarding installation, diagnostics, and error reporting. Reviewing these files before contacting technical support can reveal the source of the issue. If the solution is not evident based on the gathered files, have the Packet file available when contacting support. The support technician may request an email that contains the Packet file.

### Run the begather utility to troubleshoot Backup Exec components on Linux servers

- 1 Log on as root to the Linux server on which the Backup Exec components are installed.
- 2 Navigate to the following directory:  

```
/opt/VRTSralus/bin
```

For example:

```
cd /opt/VRTSralus/bin
```
- 3 Start the begather utility.  

For example:

```
./begather
```
- 4 Note the location of the Packet file that is displayed on the screen.

## Using the Backup Exec Debug Monitor for troubleshooting

The Backup Exec Debug Monitor, or SGMon, is a diagnostic tool that captures debug output from Backup Exec and saves it in debug logs. SGMon debug logs can help you troubleshoot backup issues. Furthermore, debug logs can help Symantec Technical Support diagnose and repair problems.

When you open SGMon, it automatically captures debug data from Backup Exec's services. To collect debug information while SGMon is closed, enable debug log creation outside of SGMon and specify a directory in which to save the logs.

For more information about how to configure the Debug Monitor and read log files, refer to the help within the Debug Monitor.

**To use the Backup Exec Debug Monitor for troubleshooting**

- ◆ Click the Backup Exec button, select **Technical Support**, and then select **Collect debug output**.

## About the Backup Exec debug tool

Backup Exec includes a debug tool (BEDBG) that generates diagnostic information about the Backup Exec processes that shut down unexpectedly. The diagnostic information helps Symantec Technical Support diagnose and repair the problem. The Backup Exec debug tool runs by default in Backup Exec. The data that the tool gathers is copied into the BEDBG folder which is located in \Program Files\Symantec\Backup Exec.

You can find more information about the Backup Exec debug tool at the following URL:

<http://seer.entsupport.symantec.com/docs/327408.htm>



# Using Backup Exec in cluster environments

This chapter includes the following topics:

- [About Backup Exec and clusters](#)
- [Requirements for clustering Backup Exec in a Microsoft Cluster Server environment](#)
- [How Backup Exec works in a Microsoft Cluster Server environment](#)
- [Requirements for installing Backup Exec on a Microsoft Cluster Server](#)
- [Installing Backup Exec on a Microsoft Cluster Server](#)
- [Upgrading Backup Exec on a Microsoft cluster](#)
- [Installing additional Backup Exec options on a Microsoft cluster](#)
- [Uninstalling Backup Exec from a Microsoft cluster](#)
- [Creating storage device pools for Microsoft Cluster Servers](#)
- [Using checkpoint restart on Microsoft Cluster Server failover](#)
- [Specifying a different failover node](#)
- [Designating a new central administration server in a Microsoft Cluster Server](#)
- [Configurations for Backup Exec and Microsoft Cluster Servers](#)
- [Using the Central Admin Server Option with Microsoft clusters and a storage area network](#)
- [About backing up Microsoft Cluster Servers](#)

- [About restoring data to a Microsoft cluster](#)
- [Disaster recovery of a cluster](#)
- [Restoring the Microsoft Cluster Server data files](#)
- [Recovering all shared disks in a Microsoft cluster](#)
- [Recovering Backup Exec in a Microsoft cluster](#)
- [Changing the Quorum disk signature](#)
- [Manually joining two cluster disk groups and resynchronizing volumes](#)
- [Troubleshooting clusters](#)

## About Backup Exec and clusters

In a server cluster, Backup Exec can protect data on local disks and shared disks, as well as protect Microsoft SQL and Exchange databases that are configured as virtual server applications; that is, they contain an IP address resource, a Network Name resource, and are displayed on the network with a unique server name (the virtual server name). Clustered servers provide high availability of applications and data to users. In a clustered server, several servers (called nodes) are linked in a network, and run cluster software that allows each node access to the shared disks. If a node becomes unavailable, cluster resources migrate to an available node (called failover). The shared disks and the virtual server are kept available. During failover, users experience only a short interruption in service.

---

**Note:** For offhost backups that use the hardware provider in a Microsoft Cluster Server (MSCS) environment, the Backup Exec server and the remote computer must be in different cluster groups. The cluster applications cannot support devices' logical unit numbers (LUNs) that have duplicate signatures and partition layouts, therefore, the snapshots containing the LUNs must be transported to a host, or remote computer, that is outside the cluster.

---

See [“Installing Backup Exec on a Microsoft Cluster Server ”](#) on page 677.

See [“Configurations for Backup Exec and Microsoft Cluster Servers”](#) on page 686.

See [“About backing up Microsoft Cluster Servers”](#) on page 693.

See [“About restoring data to a Microsoft cluster”](#) on page 694.

See [“ Requirements for clustering Backup Exec in a Microsoft Cluster Server environment”](#) on page 675.

See [“Disaster recovery of a cluster”](#) on page 694.

## Requirements for clustering Backup Exec in a Microsoft Cluster Server environment

The following scenarios must be followed if you plan to cluster Backup Exec:

- Symantec highly recommends that you use the default database instance (MSDE) that Backup Exec installs if you plan to cluster Backup Exec.
- Symantec also supports using a remote SQL Server instance to host the Backup Exec database. However, if you plan to use this scenario, review the following: Only one installed instance of Backup Exec can be installed into the remote SQL Server instance on a clustered node. All other installed instances of Backup Exec in the cluster must use the default Backup Exec MSDE database instance.

---

**Note:** You must run the Backup Exec cluster wizard on the cluster node that uses the remote SQL Server instance.

---

If you use **Windows Server 2008** or later and you use a remote, clustered SQL Server instance to host the Backup Exec Database:

- The Backup Exec server must use the same operating system level that is installed on the computer that hosts the remote SQL Server instance.

If you use **Windows Server 2008** or later and you use the **Backup Exec Utility** to reconfigure the clustered Backup Exec installation or the clustered remote SQL Server instance:

- Run the Backup Exec Utility on a computer that uses the same operating system level at the Backup Exec server and the computer that hosts the remote SQL Server instance.

See [“Installing Backup Exec on a Microsoft Cluster Server ”](#) on page 677.

See [“About backing up Microsoft Cluster Servers”](#) on page 693.

## How Backup Exec works in a Microsoft Cluster Server environment

When you install Backup Exec into a Microsoft cluster, you install it as a virtual server application. You assign an IP address resource, a Network Name resource (the virtual server name), and a disk resource to Backup Exec.

When a failover occurs, backup jobs that were running are rescheduled. The Backup Exec services are restarted on a designated failover node, and the backup jobs are restarted by default. Backup Exec provides an additional rule for cluster failover restart called Checkpoint Restart. A checkpoint restart option allows backup jobs to continue from the point at which the jobs were interrupted rather than starting the backup over again, making the backups faster and requiring fewer media. If the rule to retry jobs on a cluster failover is enabled, then an additional option can be specified to do a checkpoint restart when retrying the job. Checkpoint Restart is the only property available for the Cluster Failover Rule. You can change the default so that jobs are not restarted.

When the failed server comes back online, the Microsoft cluster can automatically rebalance the workload in a cluster, called failback, by moving cluster groups back to the server that has rejoined the cluster. However, by design, Backup Exec does not failback. The backup jobs will continue to run on the designated failover node. By continuing to run backup jobs on the designated failover node, any further risk of having to restart the jobs again when the failed server rejoins the cluster is avoided. Then, when it is convenient, you can move the Backup Exec cluster group back to the controlling node.

Specific details of how Backup Exec runs in a cluster vary depending on the configuration you use in the cluster.

See [“Configurations for Backup Exec and Microsoft Cluster Servers”](#) on page 686.

See [“Installing Backup Exec on a Microsoft Cluster Server ”](#) on page 677.

## Requirements for installing Backup Exec on a Microsoft Cluster Server

The following items are required to install Backup Exec on a Microsoft cluster:

- Two-node clusters are supported with Backup Exec on Microsoft Windows Server 2003 Enterprise/DataCenter, and Windows Server 2008 R2 Enterprise/DataCenter.
- Four-node clusters are supported with Backup Exec on Microsoft Windows Server 2008 R2 Enterprise/DataCenter.
- Up to eight-node clusters are supported with Backup Exec on Microsoft Windows Server 2003 DataCenter.
- Backup Exec clusters can be installed on Windows Server 2003/2008 R2 majority node configurations. However, there must be a shared disk in the configuration in order for Backup Exec to share its database files between nodes. In this type of configuration, if the majority of the cluster nodes fail,

then the entire cluster will fail. This configuration normally uses more than two nodes in the cluster configuration.

- The controlling node and designated failover nodes must be online during installation of Backup Exec into the cluster.
- A unique IP address and a unique network name for the Backup Exec virtual server is required during installation.
- During installation of a Backup Exec cluster, the node that runs the installation should own the shared disk. If you use a physical disk resource that belongs to another application, the Backup Exec Cluster Wizard will move all the resources that belong to the other application into the Backup Exec group. It is recommended that Backup Exec not be installed on the cluster quorum.
- An individually licensed copy of Backup Exec, as well as any applicable agents and options, is required for each active node in the cluster as defined in the End User License Agreement. When installing an evaluation version of Backup Exec, a cluster environment is automatically detected and licenses are not required.
- When you install Backup Exec clusters in a Central Admin Server Option (CASO) configuration, all Backup Exec installations must have the same server configuration. Either all nodes should be database servers or all nodes should be managed Backup Exec servers that connect to the central administration server.
- All Backup Exec installations into a cluster must either be part of a single cluster group, or be locally installed on each node. If cluster-aware Backup Exec is installed in a cluster as well as a locally installed version of Backup Exec (not cluster-aware), then you cannot log on to the locally installed Backup Exec server. You can only log on using the Backup Exec virtual server name. To be able to log on to the locally installed Backup Exec server, you must first use the Cluster Configuration Wizard to uninstall cluster-aware Backup Exec from all the nodes in the cluster.
- Use the same account for Backup Exec services on all nodes in the cluster. If nodes in a cluster use Backup Exec and have different accounts, change the services to use the same account.

See [“Installing Backup Exec on a Microsoft Cluster Server”](#) on page 677.

See [“Configurations for Backup Exec and Microsoft Cluster Servers”](#) on page 686.

## Installing Backup Exec on a Microsoft Cluster Server

Symantec does not recommend installing Backup Exec on the same disk that the cluster quorum is installed on. If you have to specify a new drive letter for the

quorum disk during a recovery process, Backup Exec will not recognize the new drive and will not run.

---

**Note:** By default, failover from the controlling node to a designated node occurs in alphabetical order according to the machine name of each node. To change the order in which failover will occur on the designated nodes, rename the machines.

---

The Backup Exec Agent for Windows is automatically installed on all the nodes in the cluster. If this installation of Backup Exec is to be used to back up remote servers outside the cluster, install the Agent for Windows on those remote servers as well.

#### To install Backup Exec on a Microsoft Cluster Server

- 1 Install Backup Exec on all the nodes that you want in the cluster. Use the same installation path for each node.
- 2 From the node that you want to be the active node, start Backup Exec.
- 3 Click the Backup Exec button, select **Configuration and Settings**, and then select **Cluster Configuration Wizard**.
- 4 Follow the instructions on the screen.

On the **Virtual Server Information** screen, Backup Exec automatically displays a default name called BKUPEXECVRS for the virtual server. Type a new default name if you do not want to use the default.

- 5 When the Cluster Configuration Wizard completes, create a storage device pool that contains all the locally attached storage devices on each node to be used when failover occurs. This ensures that jobs can be run on the storage devices that are attached to the failover nodes.

See [“Creating storage device pools for Microsoft Cluster Servers”](#) on page 680.

- 6 Repeat step 5 for all nodes.

See [“About enabling or disabling checkpoint restart ”](#) on page 683.

See [“Configurations for Backup Exec and Microsoft Cluster Servers”](#) on page 686.

See [“Specifying a different failover node”](#) on page 683.

## Upgrading Backup Exec on a Microsoft cluster

You can upgrade Backup Exec on the nodes in a cluster without taking the nodes out of the cluster.

**Table 22-1** Upgrading Backup Exec on a Microsoft cluster

Step	Action
Step 1	Select a node to upgrade and make that node the active Backup Exec cluster node.
Step 2	Run the Backup Exec installation program on the active node.
Step 3	Move the cluster group to the next node you want to upgrade, and then run the Backup Exec installation program on that node. All of the resources except for the disk should be offline when moved over to each node for upgrade.
Step 4	Repeat step 3 for each node in the cluster.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

## Installing additional Backup Exec options on a Microsoft cluster

Install additional Backup Exec options on each node of the cluster. For details on installing each option, see the appropriate section in this guide, or in online Help.

### To install additional Backup Exec options

- 1 On the controlling node, make sure the Backup Exec group is online before you start installing additional options.
- 2 Install the additional options.  
See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.
- 3 After the installation is complete on the controlling node, use the cluster administrator to move the Backup Exec group to the next appropriate node, and repeat step 2.  
Be sure to install the same options with the same settings for each node in the cluster.
- 4 To install the Agent for Oracle on Windows or Linux Servers on other nodes, map a drive to the shared disks where Backup Exec is installed on the cluster, and run SETUP.

See [“Uninstalling Backup Exec from a Microsoft cluster”](#) on page 680.

## Uninstalling Backup Exec from a Microsoft cluster

You use the Cluster Configuration Wizard to remove Backup Exec.

### To uninstall Backup Exec from a cluster

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Cluster Configuration Wizard**.
- 2 Use the wizard to remove cluster-aware Backup Exec from all selected servers.  
  
When unclustering the active node, you can either leave the Backup Exec data on the shared drive or delete it. If you delete the data, you can make the data available on the active node.
- 3 Uninstall Backup Exec from all the nodes.
- 4 After Backup Exec has been uninstalled, move any resource disks from the Backup Exec cluster group to another group, and then delete the Backup Exec cluster group.
- 5 On any node, click **Start**, point to **Settings**, and then click **Control Panel** to uninstall Backup Exec.
- 6 Double-click **Add/Remove Programs**, and then in the list of currently installed programs, select **Symantec Backup Exec (TM) 2012** and click **Change/Remove**.
- 7 Repeat step 5 for all nodes.

See [“Creating storage device pools for Microsoft Cluster Servers”](#) on page 680.

## Creating storage device pools for Microsoft Cluster Servers

When Backup Exec is installed on a cluster, it creates a set of default storage pools for each node in the cluster. If a node has storage devices, those storage devices are automatically assigned to an appropriate device pool, which is also the default destination device on that node when you create backup or restore jobs. However, to allow jobs to run on the storage devices attached to a failover node after a failover occurs, you must create a storage pool that includes the storage devices from all of the nodes. If the cluster is also configured with tape devices on a shared SCSI bus, then add the tape device name used by each node to the storage pool. You must also select this storage pool as the destination device for all jobs that you want to be restarted.

You can create either a single storage pool, or you can create storage pools for device or media types so that when jobs fail over they can be restarted on "like" devices and media.

#### To create a storage pool for a cluster

- 1 From the controlling node, open Backup Exec.
- 2 Create a new storage device pool and add storage devices.  
See [“Creating a storage device pool”](#) on page 405.
- 3 Exit Backup Exec. If there are tape devices on a shared SCSI bus, then add the tape device name used by each node.
- 4 Using the cluster administrator, move the Backup Exec resource group to the next appropriate node.
- 5 Open Backup Exec, add storage devices for this node to the previous storage pool and then exit Backup Exec. If there are tape devices on a shared SCSI bus, then add the tape device name used by each node.
- 6 Repeat step 4 and step 5 for each node in the cluster.

See [“Using checkpoint restart on Microsoft Cluster Server failover”](#) on page 681.

## Using checkpoint restart on Microsoft Cluster Server failover

You can enable or disable checkpoint restart for each backup job run on the cluster (by default, checkpoint restart is enabled). When checkpoint restart is enabled, jobs that were interrupted because of a failover continue from the point of interruption rather than starting over. Files that were already backed up are skipped, and only the remaining files in the job are backed up when the job is restarted. If this option is not selected, jobs are restarted from the beginning.

Checkpoint restart works best for the following file types:

- NTFS
- Exchange mailboxes and public folders
- Exchange 2003 IS with multiple storage groups
- SQL database non-snapshot backups

The following types of files cannot use checkpoint restart:

- System State
- Lotus Domino

- Exchange 2003 IS with one storage group
- NTFS Image sets
- NTFS Snapped volumes
- SQL database snapshot backups
- SQL transaction log backups

Checkpoint restart is not supported by the following:

- Microsoft Windows Vista/Server 2008.
- The offhost backup feature in the Advanced Disk-based Backup Option.
- Incremental backups based on the archive bit.

Jobs that are restarted from the point of failover display a status of 'Resumed' in the Job Monitor.

Before using checkpoint restart, review the following:

- If a resource was completely backed up prior to a cluster failover, that resource is skipped upon checkpoint restart, regardless of whether the backup type or file type of that resource is supported by checkpoint restart. This saves media space and backup time.
- If failover occurs in the middle of backing up a resource, the media that was being used at the time of the failover is left unappendable and new media will be requested upon restart. It is recommended that you select an appropriate media overwrite protection level to ensure that media that was used prior to the failover is not overwritten upon restart.
- The data that is backed up upon restart is part of a different backup set than the data that was backed up prior to the failover. Separate catalog backup set entries are created for the data backed up prior to the failover and after the failover.

In addition, if multiple cluster failovers occur during the backup of a given resource, a different backup set is created each time the job restarts. These multiple backup sets allow potential for duplication of backed up data.

It is important to restore the backup sets in the order in which they were backed up. In addition, you should enable the Restore over existing files option when performing a restore operation on these backup sets to ensure that all the data included in the backup set is completely restored.

- If failover occurs during a post-backup verify job, or a pre-backup or post-backup database consistency check job, that job starts at the beginning after failover.

- Entries for full-volume backups that were interrupted by a cluster failover and resumed from the point of failover do not display in the Simplified Disaster Recovery **Recover This Computer Wizard**. However, you can restore these backup sets manually after you make the initial recovery using the **Recover This Computer Wizard**.
- You can enable the checkpoint restart option for a full backup job that backs up and deletes the files. However, if a cluster failover occurs and the job is resumed, the files are not deleted from the source volume after the backup completes.
- If a failover occurs on a clustered managed Backup Exec server, the job that is recovered resumes on the active cluster node. The job will not be recovered to any other managed Backup Exec servers outside of the Backup Exec cluster.

See [“About enabling or disabling checkpoint restart”](#) on page 683.

## About enabling or disabling checkpoint restart

The Check Point Restart feature is enabled or disabled on a per backup job basis. You can find the option under **Advanced Open File** when you set backup job options for a job.

To apply checkpoint restart to backup jobs, make sure that the **Error-Handling Rule for Cluster Failover** is enabled.

See [“Backing up data”](#) on page 163.

See [“Using checkpoint restart on Microsoft Cluster Server failover”](#) on page 681.

## Specifying a different failover node

You can do the following:

- Change the order in which the nodes fail over.
- Add a failover node to the cluster.
- Remove a failover node from the cluster.

To change the order in which nodes fail over

- By default, in a MSCS cluster, failover from the controlling node to a designated node occurs in alphabetical order according to the machine name of each node. To change the order in which failover will occur on the designated nodes, rename the machines in the order in which they should fail over.

Before you add a node to the Backup Exec cluster configuration, you must install Backup Exec on it. Cluster services for a node should be online before you add or remove it from the cluster.

If you are removing a node, do not run the cluster configuration wizard from the node you want to remove.

#### **To add or remove a failover node**

- 1 On the controlling node, click the Backup Exec button, select **Configuration and Settings**, and then select **Cluster Configuration Wizard**.
- 2 Follow the instructions on the screen to add or remove a node.
- 3 If you have added a failover node, also add any locally attached storage devices that are to be used when failover occurs to the cluster storage pool. This ensures that jobs can be run on the storage devices that are attached to the failover nodes.

If you remove some, but not all, nodes in a cluster, an uninstall of Backup Exec results in a password being requested for the virtual server and the services continuing to run. You must remove Backup Exec from all nodes on the cluster.

See [“Uninstalling Backup Exec from a Microsoft cluster”](#) on page 680.

See [“Specifying a different failover node”](#) on page 683.

See [“Configurations for Backup Exec and Microsoft Cluster Servers”](#) on page 686.

## **Designating a new central administration server in a Microsoft Cluster Server**

To designate a new central administration server for a cluster environment, use BEUtility.exe. BEUtility enables you to do various types of configuration and maintenance operations on your Backup Exec servers.

---

**Note:** In a cluster environment, do not use **Change Service Account** in BEUtility.exe.

---

**To change a Backup Exec cluster from a Database Server to a Member Server**

- 1 Install the new server as a managed Backup Exec server with the Library Expansion Option installed.  
Make sure connections to the Backup Exec cluster and other member servers are working properly.
- 2 Using the cluster administrator, shut down the Backup Exec cluster services.  
Be sure to keep the Disk resource online.
- 3 Move the catalog files from the Backup Exec cluster installation path to the respective installation paths on the new database server.
- 4 Use BEUtility.exe to connect all Backup Exec servers to the new database server and to start all Backup Exec services.
- 5 Stop and restart the Backup Exec Services on the new database server.
- 6 Using the Cluster Administrator, move the Backup Exec resource group to the failover node and make sure services start on that node.
- 7 Use BEUtility.exe to stop and restart the Backup Exec Services on all the member servers of the SAN in order for them to connect to the new database server.

**To change a Backup Exec cluster from a central administration server to a managed Backup Exec server**

- 1 Install the new server as a managed Backup Exec server.  
Make sure connections to the Backup Exec cluster and other managed Backup Exec servers are working properly.
- 2 Using the cluster administrator, shut down the Backup Exec cluster services.  
Be sure to keep the Disk resource online.
- 3 Move the catalog files from the Backup Exec cluster installation path to the respective installation paths on the new central administration server.
- 4 Use BEUtility.exe to connect all Backup Exec servers to the new central administration server and to start all Backup Exec services.
- 5 Stop and restart the Backup Exec Services on the central administration server.

- 6 Using the Cluster Administrator, move the Backup Exec resource group to the failover node and make sure services start on that node.
- 7 Use BEUtility.exe to stop and restart the Backup Exec Services on all the managed Backup Exec servers in order for them to connect to the new central administration server.

See “[Multi-node clusters on a fibre channel SAN with the Central Admin Server Option](#)” on page 691.

## Configurations for Backup Exec and Microsoft Cluster Servers

Backup Exec supports various cluster configurations of between two and eight nodes on a fibre channel SAN, with locally attached storage devices, or with storage devices on a shared SCSI bus. You can use any combination of these configurations.

---

**Note:** If you install the cluster on a private network, use the Cluster Administrator to enable public communication if necessary.

---

If you are using a cluster on a fibre channel SAN or with storage devices on a shared SCSI bus and failover occurs, depending on the capability of your various SAN components, media might be orphaned in the tape drive until the failed node becomes active again.

If end-of-job markers were not written to the media before the failover occurred, the media may be marked as unappendable by the Backup Exec engine when the next append backup job is run. The media remains unappendable until it is overwritten (or erased, or the retention period expires, etc.).

If the storage device is a robotic library, you can review the Robotic Library Inventory report to discover if the media was marked unappendable by the Backup Exec engine. If the Full column reports a 3, the Backup Exec engine has marked the media as unappendable.

To add or remove hot-swappable devices in a cluster, run the Hot-swap Device Wizard on all Backup Exec Cluster nodes. If a server is not updated to recognize a new device, any job that is targeted to that device may fail.

See “[Using the Hot-swappable Device Wizard to add or replace devices](#)” on page 336.

Examples of various cluster configurations are available.

- See “[Two-node cluster with locally attached storage devices](#)” on page 687.
- See “[Two-node cluster with tape devices on a shared SCSI bus](#)” on page 688.

- See [“Configuring a shared SCSI bus for tape devices”](#) on page 689.
- See [“Multi-node clusters on a fibre channel SAN with the Central Admin Server Option”](#) on page 691.

## Two-node cluster with locally attached storage devices

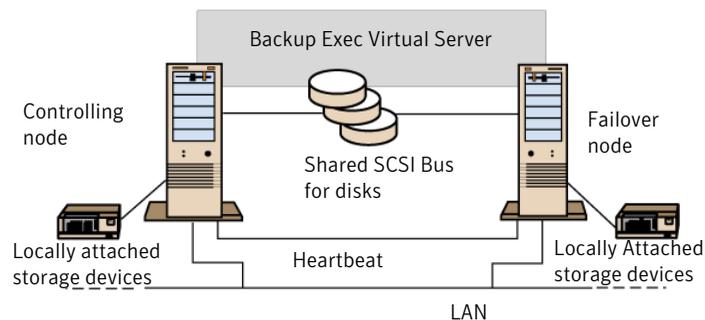
In this configuration, cluster-aware Backup Exec is installed on the controlling node, failover occurs to designated nodes in the cluster, and storage devices are locally attached to each node.

Depending on the type of storage device, each node’s locally attached storage devices are automatically assigned to an appropriate storage device pool that Backup Exec creates. These storage device pools also act as default destination devices on that node when you create backup or restore jobs. You must create a storage pool that includes storage devices on the controlling node and on each failover node in order for jobs to run when failover occurs.

See [“Creating storage device pools for Microsoft Cluster Servers”](#) on page 680.

To restore data in this configuration, move media to the failover node’s locally attached storage device and reinventory the device before starting a restore operation.

**Figure 22-1** Two-node Cluster with Locally Attached Storage Devices



See [“Multi-node clusters on a fibre channel SAN with the Central Admin Server Option”](#) on page 691.

## Two-node cluster with tape devices on a shared SCSI bus

In this configuration, cluster-aware Backup Exec is installed on the controlling node, failover occurs to designated nodes in the cluster, and tape devices are attached to a shared SCSI bus that is separate from any shared SCSI bus for disks.

Because each node creates a unique tape device name for the same device, if the drive is not serialized, this configuration requires you to create a storage pool that includes the tape device name used by each node in order for jobs to run when failover occurs.

See [“Creating storage device pools for Microsoft Cluster Servers”](#) on page 680.

When failover occurs, a SCSI bus reset is issued. Therefore, tape devices and shared drives should not be connected to the same SCSI bus; each should be connected to separate SCSI buses.

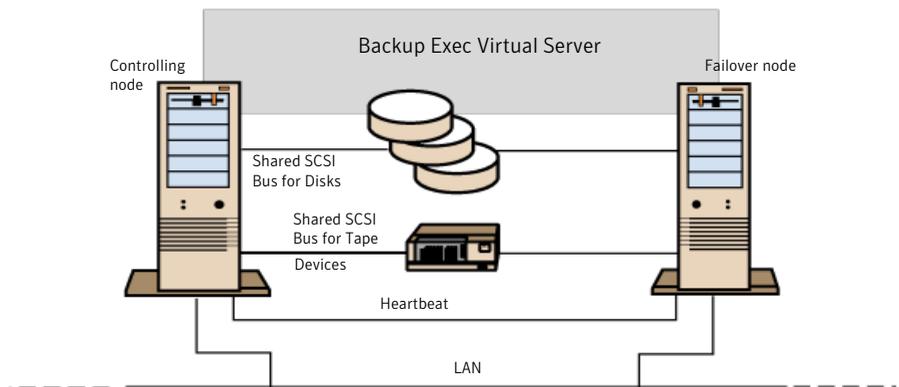
See [“Configuring a shared SCSI bus for tape devices”](#) on page 689.

---

**Note:** If you are using a serialized tape device in a shared SCSI cluster configuration, media that is orphaned in a device because of a failover will be ejected from the tape device. If you are using a tape device that is not serialized, you need to manually eject the media from the device or reboot the device.

---

**Figure 22-2** Two-node cluster with tape devices on a shared SCSI bus



See [“Multi-node clusters on a fibre channel SAN with the Central Admin Server Option”](#) on page 691.

## Configuring a shared SCSI bus for tape devices

Before configuring a shared SCSI bus for tape devices, please read the following carefully.

To configure tape devices on a shared SCSI bus, you must have SCSI cables, SCSI terminators, a SCSI adapter in each cluster node to provide a shared external bus between the nodes, and at least one tape device on the shared bus.

The tape devices must be connected to a bus that uses the same method of transmission that the device does (single-ended or differential). Only one transmission method can be used on a single SCSI bus, however, if the devices use different transmission methods, you can install a signal converter between the devices. A signal converter converts single-ended SCSI signals to differential SCSI signals.

---

**Note:** You must use a signal converter to connect single-ended and differential devices in order to avoid hardware damage.

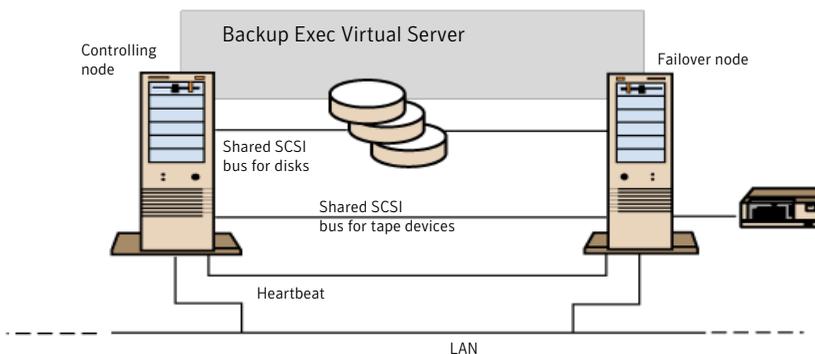
---

You must terminate the SCSI bus at both ends so that commands and data can be transmitted to and from all devices on the bus. Each SCSI bus must have two terminators and they must be at each end of the segment.

If a tape device is in the middle of the bus, remove any internal termination in that device.

If the tape device is at the end of the bus, and the tape device has internal termination, you can use the device's internal termination to terminate the bus.

**Figure 22-3** Example of a shared bus with tape devices at the end of the bus



Following are methods you can use to terminate a bus:

- SCSI adapters. This method is not recommended because if the server is disconnected from the shared bus, or if there is a power supply failure, the bus may not be properly terminated and may be inoperable.
- Pass-through (or feed-through) SCSI terminators. These can be used with SCSI adapters and with some tape devices. If the tape device is at the end of the bus, you can attach a pass-through SCSI terminator to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.

---

**Note:** To ensure termination if a power supply failure occurs, turn off the on-board terminators on the SCSI controller (using the host adapter manufacturer's recommended method) and physically terminate the controller with a terminator.

---

- Y cables. These can be used with some tape devices. If the tape device is at the end of the bus, you can attach a terminator to one branch of a Y cable to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.
- Trilink connectors. These can be used with some tape devices. If the tape device is at the end of the bus, you can attach a terminator to one of the trilink connectors to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.

Besides terminating the bus, Y-cables and trilink connectors also allow you to isolate the devices from the shared bus without affecting the bus termination. You can maintain or remove that device without affecting the other devices on the shared SCSI bus.

### To configure a shared SCSI bus for tape devices

- 1 Install the SCSI controllers for the shared SCSI bus.

Make sure that the SCSI controllers for the shared SCSI bus are using different SCSI IDs. For example, on the controlling node, set the SCSI controller ID to 6 and on the failover node, set the SCSI controller ID to 7.

- 2 Prepare the SCSI controllers for the shared SCSI bus. Refer to your SCSI host adapter manufacturer's documentation for details.

Do not have power on to both nodes while configuring the computers, or if both nodes have power on, do not connect the shared SCSI buses to both nodes.

- 3 Connect the shared SCSI tape devices to the cable, connect the cable to both nodes, and then terminate the bus segment using one of the methods discussed in the previous section.

See [“Two-node cluster with tape devices on a shared SCSI bus”](#) on page 688.

## Multi-node clusters on a fibre channel SAN with the Central Admin Server Option

In this configuration, one or more clusters are attached to a fibre channel storage area network (SAN), with cluster-aware Backup Exec and the Central Admin Server Option (CASO) installed on the controlling node in each cluster. Shared secondary storage devices are attached to the fibre channel, although a single storage device can be shared between one or more clusters. Failover occurs (in alphabetical order of the machine name) to other designated nodes in the cluster.

---

**Note:** When using multiple clusters in a CASO environment, it is strongly recommended that the cluster nodes be connected to the storage devices using a fibre switch. If you use a hub rather than a fibre switch, the hub will receive a reset command during a failover event that causes all other components attached to the hub to be disconnected. You can designate any server on the fibre channel SAN as the central administration server.

---

You should create a failover storage pool for the cluster.

See [“Creating storage device pools for Microsoft Cluster Servers”](#) on page 680.

This configuration offers increased performance since backups are performed locally instead of over a network. Additionally, centralized media catalogs are available. Because CASO uses a shared catalog database, a tape that has already been cataloged can be physically moved from one device to another and not have to be recataloged.

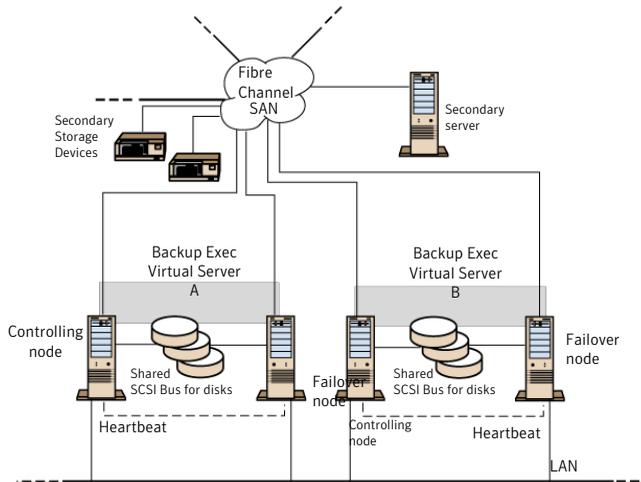
---

**Note:** The CASO option must be installed on each failover node, with the same settings that were used on the primary node. Either all nodes should be database servers or all nodes should be managed Backup Exec servers.

---

The following are examples of multi-node clusters:

**Figure 22-4** Two 2-node Clusters on a Fibre Channel SAN with the Central Admin Server Option



You can have a four-node cluster.

See [“Using the Central Admin Server Option with Microsoft clusters and a storage area network”](#) on page 692.

## Using the Central Admin Server Option with Microsoft clusters and a storage area network

Managed Backup Exec servers can be clustered. However, this configuration is not recommended because the central administration server recovers all failed jobs in a distributed job environment.

The following configurations can be used when installing Backup Exec clusters with the Central Admin Server Option (CASO).

- Backup Exec cluster with CASO
- Backup Exec cluster with the managed Backup Exec server configuration

### To install Backup Exec in a Microsoft cluster with CASO

- 1 Install Backup Exec with CASO and any additional options onto your Microsoft cluster nodes.
- 2 From the node that you want to designate as the active node, start Backup Exec.
- 3 Click the Backup Exec button, select **Configuration and Settings**, and then select **Cluster Configuration Wizard**.
- 4 Follow the instructions on the screen.
- 5 When the Cluster Configuration Wizard completes, install the managed Backup Exec server. Use the virtual Backup Exec cluster name when prompted for the central administration server.

### To install Backup Exec in a Microsoft cluster with the managed Backup Exec server configuration

- 1 Install Backup Exec with the managed Backup Exec server option and any additional options onto your Microsoft cluster nodes.  

All nodes that run Backup Exec in the Microsoft cluster configuration must access the same central administration server. If the nodes do not access the same central administration server, failovers do not occur properly.
- 2 From the node that you want to designate as the active node, start Backup Exec.
- 3 Click the Backup Exec button, select **Configuration and Settings**, and then select **Cluster Configuration Wizard**.
- 4 Follow the instructions on the screen.

See [“About backing up Microsoft Cluster Servers”](#) on page 693.

## About backing up Microsoft Cluster Servers

To protect all data in the cluster, which includes file shares, databases, and the cluster quorum, back up the following:

- Local disks, Shadow Copy Components, and System State on each node. The cluster quorum, which contains recovery information for the cluster and information about changes to the cluster configuration, is included in the System State backup.
- All shared disks, including the data in the Microsoft Cluster Server folder on the Quorum disk.

- Virtual servers, which may contain data or contain applications such as Microsoft SQL Server or Exchange Server. Use Backup Exec database agents to back up databases.

---

**Note:** For offhost backup jobs that use the hardware provider, the Backup Exec server and the remote computer must be in different cluster groups. The cluster applications cannot support devices' logical unit numbers (LUNs) that have duplicate signatures and partition layouts, therefore, the snapshots containing the LUNs must be transported to a host, or remote computer, that is outside the cluster.

---

The Command Line Applet can be used with Backup Exec when Backup Exec is installed in a cluster. The only limitation is that you cannot use the Command Line Applet to specify a device for backup. You can use the Command Line Applet to target a storage pool, but not a specific device in that pool.

See [“Backing up data”](#) on page 163.

See [“Editing backups”](#) on page 170.

See [“About stages”](#) on page 183.

## About restoring data to a Microsoft cluster

For all file restore operations, including redirecting restores, use the normal restore procedures.

When restoring files to shared drives, direct those files to the virtual server or the controlling node of the resource. When restoring individual database files, such as Microsoft SQL Server or Exchange Server, direct those files to the virtual server name of a specific installation of the SQL or Exchange database.

See [“About searching for and restoring data”](#) on page 229.

## Disaster recovery of a cluster

Prepare for recovery by creating a disaster preparation plan.

Prepare to restore SQL, Exchange, and Lotus Domino databases in a cluster after a disaster by reading the sections on preparing for disaster recovery in the appropriate chapters.

In addition to the initial preparation instructions, further action is required to completely protect the Microsoft clusters.

If a disaster occurs, the following information is required to successfully recover the cluster:

- General Cluster Information
  - Cluster name
  - Cluster IP address and subnet mask
  - Cluster node names
  - Node IP addresses
  - Local and shared drive letters and partition scheme
  - Disk signatures
- Cluster Groups
  - Group name
  - Preferred nodes
  - Failover/failback policies
- Cluster Resources
  - Resource name
  - Resource type
  - Group membership
  - Possible owners
  - Resource dependencies
  - Restart and Looks Alive/Is Alive properties
  - Resource-related parameters
  - Application-specific configuration (SQL Database Character Set)
- If you are recovering a Microsoft Cluster Server, run the Clusterrecovery.exe from the Microsoft 2003 Resource Kit to retrieve the disk signatures from the shared disk.

See [“About key elements of a disaster preparation plan \(DPP\)”](#) on page 634.

See [“How to prepare for disaster recovery of SQL”](#) on page 830.

See [“How to prepare for disaster recovery on a Lotus Domino server”](#) on page 977.

See [“Recovering from a disaster for Exchange ”](#) on page 862.

## Using Simplified Disaster Recovery to prepare for disaster recovery of a cluster

Backup Exec provides a fully-automated disaster recovery solution called Simplified Disaster Recovery, which allows you to quickly and efficiently recover the nodes that comprise the server cluster after a disaster. Oracle servers cannot be restored using Simplified Disaster Recovery. For more information about disaster recovery for these options, see the appropriate chapters.

See [“About preparing computers for use with Simplified Disaster Recovery”](#) on page 707.

---

**Note:** To change the setup, use hardware, or a hardware configuration that is different from the original configuration, you must perform a manual recovery.

---

## Recovering nodes on the cluster using Simplified Disaster Recovery

If you used Backup Exec’s Simplified Disaster Recovery to prepare for a disaster, you can use Simplified Disaster Recovery to recover the nodes to their pre-disaster state.

---

**Note:** You must create disaster recovery media for each Windows 2003 cluster node. Disaster recovery media is customized for a single computer. You will not be able to use the media interchangeably between the nodes in a cluster.

---

When recovering both nodes in a cluster, make sure that the drive letters match the original cluster configuration. The scaled-back version of Windows that runs the recovery wizard may detect the hard drives in a different order than what was originally configured under the original version of Windows.

If the original configuration does not match, then to a certain extent, you can control the hard drive numbering scheme that Windows devises.

If you cannot get the SDR **Recover This Computer Wizard** to properly detect the hard drive order, you can still manually set up hard drive partitions using the **Advanced Disk Configuration** option within the **Recover This Computer Wizard**. After this is done, you can continue with automated restore of your backup media afterward.

---

**Note:** After Windows has been installed, you cannot change the system drive’s letter. You must restore the system to the same drive letter from which it was backed up.

---

### To recover nodes on the cluster using Simplified Disaster Recovery

- 1 If you are recovering more than one node, disconnect the shared disks. If you are recovering only one node, the shared disks do not need to be disconnected.

If all nodes in the cluster are unavailable and must be recovered, the cluster cannot fail over. Disconnect the shared disks before recovery begins.

- 2 Restore the nodes.  
See [“About searching for and restoring data”](#) on page 229.
- 3 Reconnect the shared drives and bring the nodes online.
- 4 To restore a database to the shared drives, use the appropriate Backup Exec agent.

See [“About Simplified Disaster Recovery”](#) on page 704.

## Recovering Backup Exec on a Microsoft cluster using Simplified Disaster Recovery

To fully restore a cluster on which Backup Exec is installed, you can use Simplified Disaster Recovery to restore the cluster node and all shared disks or you can rebuild the cluster. To remotely restore the cluster catalog the media that contains the backup sets of the cluster nodes and the shared disk.

### To recover Backup Exec on a Microsoft Cluster with Simplified Disaster Recovery:

- 1 Replace all shared disks, if necessary.
- 2 Run the SDR **Recover This Computer Wizard** on one of the nodes. During this process, use **Advanced Disk Configuration** to repartition all shared disks to their original configuration. Restore the local disk, system state, and the data files to the shared disk.
- 3 Restart the server.  
The cluster service and all other cluster applications should come online.
- 4 Run the **Recover This Computer** wizard on all other nodes. Restore only the local disk and system state.

See [“About Simplified Disaster Recovery”](#) on page 704.

## Recovering the entire cluster using a manual disaster recovery procedure

As part of the manual recovery process, you must reinstall Windows, including the last service pack applied before the failure.

See [“How to prepare for disaster recovery of SQL”](#) on page 830.

See [“How to prepare for disaster recovery on a Lotus Domino server”](#) on page 977.

See [“About restoring Oracle resources”](#) on page 904.

#### To recover the entire cluster manually

- 1 On the first node you want to recover, reinstall Windows, including the last service pack applied before the failure.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

- 2 On the other nodes you want to recover, reinstall Windows, including the last service pack applied before the failure.

- 3 Reinstall the cluster services and bring the cluster online.

Do the following:

- If you are recovering a Microsoft Cluster Server, after booting the nodes in a cluster, make sure that the drive letters match the original cluster configuration. If the original configuration does not match, then to a certain extent, you can control the hard drive numbering scheme that Windows devises by using the Disk Administrator.

- 4 Do one of the following:

- If you are recovering a Microsoft Cluster Server, use the Cluster Wizard to reinstall Backup Exec on the cluster. You must use the same settings used during the initial installation.

See [“Installing Backup Exec on a Microsoft Cluster Server ”](#) on page 677.

- 5 Catalog the media in the cluster.

- 6 On the Backup Exec navigation bar on the active node, click **Restore**.

- 7 Restore last full backup sets made of the active node, and then restore the System State.

- 8 Do one of the following:

- If you are recovering a Microsoft Cluster Server, make sure you select **Restore cluster quorum** option (this option must be selected) in the **Restore Wizard**.

- 9 Start the restore operation.

- 10 When the restore has completed, reboot the active node.

- 11 For each node that you need to recover, repeat step 6 through step 10.

- 12 After all nodes are recovered, restore the Backup Exec data files, and all other data files, to the shared disks.
- 13 To restore a database to the shared disks, use the appropriate Backup Exec agent.

## Restoring the Microsoft Cluster Server data files

To fully recover the cluster, the cluster files in the MSCS folder may need to be restored. If the Quorum disk is still available and has not changed, then you do not have to restore the data files. If the Quorum disk is new, you need to restore the data files to the new Quorum disk. You should disable the cluster disk driver before restoring the data files.

See [“About searching for and restoring data”](#) on page 229.

## Recovering all shared disks in a Microsoft cluster

Recover shared disks using Cluster recovery from the Microsoft 2003 Resource Kit, which helps automate the recovery process or by performing a manual recovery.

### To recover all shared disks using Dumpcfg

- 1 Disable the cluster disk driver on all nodes in order to gain access to the new disk.
- 2 On the Computer Management menu, select **System Tools**. Then select **Device Manager**.
- 3 Right-click the cluster disk driver, and then select **Disable**.
- 4 Replace and then repartition the shared disk. Use Disk Manager to verify that all nodes have access to the same shared disk.
- 5 Run Dumpcfg or Clusterrecovery to replace the disk signature for the Quorum disk.
- 6 Using a remote Backup Exec server, restore the cluster files to the Quorum disk via the node that has access to the disk.
- 7 Enable the cluster disk driver on all nodes.
- 8 On the **Computer Management** menu, select **System Tools**. Then select **Device Manager**.
- 9 Right-click the cluster disk driver, and then select **Enable**.
- 10 Reboot all cluster nodes.

#### To recover all shared disks without using Dumpcfg

- 1 Uninstall all cluster applications and the cluster software from both nodes.
- 2 Replace and then use Disk Manager to repartition the shared disk to the previously saved configuration.
- 3 Reinstall the cluster software.
- 4 Reinstall the cluster-aware version of Backup Exec on the cluster.
- 5 Reinstall additional cluster-aware software applications on the shared disk.
- 6 Use Backup Exec to restore any data from the catalogs.

See [“About searching for and restoring data”](#) on page 229.

## Recovering Backup Exec in a Microsoft cluster

If you used Simplified Disaster Recovery's **Create Simplified Disaster Recovery Disk Wizard** to prepare disaster recovery media for the shared disks, you must use a manual process to recover Backup Exec on a shared disk.

#### To use a manual process to recover Backup Exec on a shared disk

- 1 Replace the shared disk if necessary, and add that disk to the cluster as a disk resource.
- 2 Reinstall the cluster-aware version of Backup Exec on the cluster using the same information used in the original installation.
- 3 Use Backup Exec to restore any data from the catalogs.

See [“About searching for and restoring data”](#) on page 229.

## Changing the Quorum disk signature

The cluster service may not start because the disk signature on the Quorum disk is different from the original signature. You can change the disk signature.

#### To change the Quorum disk signature

- 1 Start the cluster service on one node with the **-Fixquorum** option in the startup parameters.
- 2 Open the Cluster Administrator and right-click the cluster, and then select **Properties**.
- 3 Select the **Quorum** tab.
- 4 In the **Quorum resource** field, select a different disk.

- 5 Click **OK**.
- 6 Stop the cluster services and then restart them without the `-Fixquorum` option.

You may run the `-Fixquorum` option as many times as needed to redesignate a Quorum disk signature.

- 7 Bring all other nodes online.

See [“Troubleshooting clusters”](#) on page 701.

## Manually joining two cluster disk groups and resynchronizing volumes

If an Advanced Disk-based backup failed due to the application virtual server failover, you may need to re-join the cluster disk groups.

### To manually re-join the two cluster disk groups and resynchronize the volumes

- 1 Import the cluster disk group into the node, if the original cluster disk group is not already imported into the node where the production virtual server is currently online.
- 2 Rejoin the new cluster disk group with the original cluster disk group.
- 3 Snap back the snapped volumes with their original volumes. Ensure that the option to synchronize using the original volume is selected.

If you are not able to import the new cluster disk group into the node where the original cluster disk group is currently located, failover the application virtual server back to its original node before rejoining the two cluster disk groups.

See [“Troubleshooting clusters”](#) on page 701.

## Troubleshooting clusters

If you experience problems with using Backup Exec in a cluster environment, review the questions and answers in this section.

**Table 22-2** Cluster troubleshooting questions and answers

Question	Answer
<p>After I recovered my cluster and all shared disks, the cluster service will not start. Why won't it start and how can I get it started?</p>	<p>The cluster service may not start because the disk signature on the Quorum disk is different from the original signature. See <a href="#">"Changing the Quorum disk signature"</a> on page 700.</p>
<p>I used the Checkpoint Restart option for my backups. During one of my backups, a Microsoft cluster failover occurred. Multiple backup sets were created. When I try to verify or restore using these backup sets, an "Unexpected End of Data" error occurs on the set that contains the data that was backed up prior to the failover. Why does this occur? Is my data safe?</p>	<p>You received this error because failover occurred in the middle of backing up the resource, therefore the backup set was not closed on the media. However, the objects that were partially backed up in the first backup set were completely backed up again during restart, ensuring data integrity. Therefore, all of the objects on the media for the given backup set should still be restored and verified.</p>
<p>I clustered a central administration server with a managed Backup Exec server. Now the device and media service on the managed Backup Exec server fails. Why?</p>	<p>This occurs when the managed Backup Exec server becomes the active node and attempts to connect to the Backup Exec database on the central administration server, which is no longer available. To correct this, you must use the Backup Exec Utility (BEUTILITY.EXE) or reinstall the managed Backup Exec server to become a central administration server.</p>

See ["About Backup Exec and clusters"](#) on page 674.

# Simplified Disaster Recovery

This chapter includes the following topics:

- [About Simplified Disaster Recovery](#)
- [About disaster recovery information files](#)
- [About the Simplified Disaster Recovery Disk](#)
- [Requirements for using Simplified Disaster Recovery](#)
- [About installing Simplified Disaster Recovery](#)
- [About preparing computers for use with Simplified Disaster Recovery](#)
- [About setting an alternate location for a disaster recovery information file](#)
- [Requirements and recommendations for running the Create Simplified Disaster Recovery Disk Wizard](#)
- [About the Create Simplified Disaster Recovery Disk Wizard](#)
- [About copying the disaster recovery files](#)
- [Preparing a custom Simplified Disaster Recovery disk locally for remote Backup Exec servers](#)
- [About preparing to recover from a disaster by using Simplified Disaster Recovery](#)
- [About the Recover This Computer Wizard](#)
- [About using Simplified Disaster Recovery with the Central Admin Server Option](#)

- [Best practices for Simplified Disaster Recovery](#)

## About Simplified Disaster Recovery

Symantec Backup Exec Simplified Disaster Recovery (SDR) enables you to quickly and efficiently recover Windows computers after a hard drive failure. The SDR wizards guide you in preparing for disaster recovery and in recovering a local or remote computer to its pre-disaster state.

---

**Note:** If you downloaded the Backup Exec installation media, make sure that you downloaded the ISO image for the Simplified Disaster Recovery Disk as well. ISO images are available for 32-bit and 64-bit computers.

---

See [“Backing up data”](#) on page 163.

See [“Editing a stage”](#) on page 184.

## About disaster recovery information files

Simplified Disaster Recovery (SDR) works with Backup Exec when you run backup jobs that include all critical system component selections. For each computer that you protect with this type of backup job, Backup Exec creates a disaster recovery information file for that computer. A disaster recovery information file contains computer-specific information for the computer being backed up.

Computer-specific information includes details such as hard disk layout, storage drivers, network drivers, and system version details. It also includes Backup Exec catalog details such as backup set information and recovery point details. Each disaster information recovery file uses the file name <computer\_name>.DR.

Backup Exec automatically stores each disaster recovery information file it creates in a default location on the Backup Exec server. Because the files are critical, Backup Exec also lets you specify an alternate storage location where an additional copy of each file can be stored. Symantec recommends that you set a path to an alternate storage location. If the Backup Exec server crashes, you won't be able to retrieve the disaster recovery information file from the default location but you can retrieve it from the alternate location.

Each time Backup Exec runs a backup that includes all critical system components, the disaster recovery information files are automatically updated in each storage location.

SDR uses the computer-specific information that is contained in the file when you run the **Recover This Computer Wizard**. Without a disaster recovery information file, a local recovery of the computer is not possible with SDR.

See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.

See [“Disaster recovery information file storage paths”](#) on page 712.

## About the Simplified Disaster Recovery Disk

Backup Exec provides you with a generic 32-bit and a generic 64-bit system recovery DVD called the Simplified Disaster Recovery Disk. You can use either one to recover a computer. However, keep in mind that some computers contain storage controllers that can be recognized only with 32-bit drivers. Likewise, there are also some computers that contain storage controllers for which only 64-bit drivers are available. Use the appropriate Simplified Disaster Recovery Disk for your environment.

You start a computer with the Simplified Disaster Recovery Disk, and then use the **Recover This Computer** link on the **Recovery** tab to recover the computer. The recovery disk uses a minimal version of the Windows 7 operating system and contains many of the drivers that are required to recover your computer. In many cases, the generic Simplified Disaster Recovery Disk can be used to completely recover the computer. However, if you change the computer's hardware after the last SDR backup, the generic Simplified Disaster Recovery Disk might not be sufficient to recover the computer. You should run the **Create Simplified Disaster Recovery Disk Wizard** to determine if the generic Simplified Disaster Recovery Disk recognizes any new hardware drivers that are not present in its driver database. If the drivers are present, you can use the generic Simplified Disaster Recovery Disk to recover the computer. Otherwise, use the **Create Simplified Disaster Recovery Disk Wizard** to create a *custom* Simplified Disaster Recovery Disk for the computer, and then store the custom recovery disk in a safe location.

In addition to the **Recovery** tab, the Simplified Disaster Recovery Disk also provides two additional tabs that are called **Network** and **Utilities**. These tabs refer to the network tools and utility tools that you can use to facilitate the recovery of a computer.

Network tools include the following:

- Start My Networking Services
- Map a Network Drive
- Configure Network Connection Settings
- Run IP Config Utility

- Ping a Remote Computer

Utility tools include the following:

- Gather Log Files for Symantec Technical Support
- View Log File
- Start Command Prompt
- Edit the Windows boot.ini File
- Load a Driver
- Select Keyboard

Finally, SDR provides you with an advanced hard disk configuration tool called Advanced Disk Configuration.

Advanced Disk Configuration lets you run advanced hard disk operations on the computer that you are recovering.

For example, you can do tasks such as:

- Creating or deleting simple volumes.
- Resizing a volume.
- Converting a basic hard disk to a dynamic disk.
- Changing or assigning drive letters.
- Creating spanned, striped, and mirrored volumes.

See [“About Advanced Disk Configuration”](#) on page 724.

See [“Requirements for using Simplified Disaster Recovery ”](#) on page 706.

## Requirements for using Simplified Disaster Recovery

The following items are required before you use Simplified Disaster Recovery (SDR):

- Symantec Backup Exec 2012.
- The Symantec Backup Exec Agent for Windows or Backup Exec must be installed on any remote computers to be backed up with SDR.
- Encryption key files for all volumes that you encrypt with Windows BitLocker Drive Encryption (Windows Vista/Windows Server 2008/Windows Server 2008 R2/Windows 7 only).
- A third-party ISO 9660-compliant CD/DVD burning application to burn the SDR-created bootable CD/DVD image to a CD or DVD.

- A writable or rewritable CD/DVD device.

---

**Note:** Backups from previous versions of Backup Exec cannot be restored using SDR.

---

See [“Requirements and recommendations for running the Create Simplified Disaster Recovery Disk Wizard”](#) on page 714.

## About installing Simplified Disaster Recovery

Simplified Disaster Recovery (SDR) is automatically installed on the Backup Exec server during the initial installation of Backup Exec. However, the Agent for Windows is required to protect remote computers with SDR. You must purchase the Agent for Windows separately, and then install it on the remote computers that you want to protect. The Agent for Windows is a system service that runs on remote servers and enhances backup and restore performance.

See [“About push-installing the Agent for Windows to remote computers”](#) on page 83.

See [“About installing the Agent for Windows”](#) on page 83.

See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.

## About preparing computers for use with Simplified Disaster Recovery

The key to successfully recovering computers after a disaster is to carefully and properly prepare those computers before a disaster occurs.

Before you can recover computers, you must prepare the computers for disaster recovery by performing the following steps in the order listed:

- When you first use Backup Exec, you must specify an alternate location where copies of the disaster recovery information files are stored.  
See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.
- Run backup jobs that include all critical system components for the computers that you want to protect.  
See [“Backing up data”](#) on page 163.

By default, Backup Exec selects all critical system components for you when you select a computer for backup. Backup Exec makes it easy for you to determine when a computer is prepared correctly for future disaster recovery operations. When all critical system components are included in your backup job selections, the Simplified Disaster Recovery indicator on the selections pane reads **ON**. If you deselect one or more critical system component files, the indicator changes to **OFF**. Symantec does not recommend deselecting any system critical files from the backup job; if you do, the system-specific disaster recovery information file cannot be created.

---

**Warning:** If you back up a computer to a tape device, and you do not have a disaster recovery information file, the computer cannot be recovered using SDR.

---

See [“About backing up critical system components”](#) on page 539.

Backup Exec creates the disaster recovery information file after it finishes a backup job that includes all critical system components. It then stores the disaster recovery information file in the default and alternate storage locations. Catalog entries from subsequent backups are added to the disaster recovery information file as these backups are completed.

After you have performed these steps for each computer you want to protect, you can recover the computers using SDR in any of the following recovery scenarios:

- Restore a Backup Exec server using a locally attached storage device.
- Restore a Windows computer by moving the media and the storage device to the computer being restored. Then restore the computer through the locally attached storage device.
- Restore a remote Windows computer using a network connection to the Backup Exec server.
- You can create bootable CD-R (CD-Recordable) or CD-RW (CD-Rewritable) media with the **Create Simplified Disaster Recovery Disk Wizard**

During recovery operations, you have the option of recovering the computer using the most recent backup. You can also recover to a previous point-in-time backup.

## Notes about using deduplication storage devices with Simplified Disaster Recovery (SDR)

If you use deduplication storage devices, consider the following:

- Do not select a deduplication storage device on the local Backup Exec server if you are backing up the local Backup Exec server. If you use Simplified Disaster

Recovery (SDR) to recover a Backup Exec server, the **Recover This Computer Wizard** cannot restore data from a local deduplication storage device.

- SDR cannot recover a deduplication storage folder.
- Before you can use SDR to restore a remote computer that was backed up using client-side deduplication, you must first delete the direct access device. See [“About direct access sharing of storage devices”](#) on page 771.

If you use SDR to recover a Backup Exec server that contains a deduplication storage folder, consider the following:

- Any existing backup sets that were sent to the deduplication storage folder after it was backed up cannot be restored.
- The deduplication storage folder may not be in an operational state after the recovery.

## About setting an alternate location for a disaster recovery information file

Symantec recommends that you specify an alternate or additional location for the disaster recovery information files that Backup Exec automatically creates. These files contain computer-specific information for each computer that you protect with Simplified Disaster Recovery (SDR). When you recover a Backup Exec server from a disaster, you must have the Backup Exec server's disaster recovery information file available. Without it, you cannot run SDR to recover the Backup Exec server. Therefore, the alternate location should be on a different computer than the Backup Exec server whenever possible. If the Backup Exec server's hard drive is damaged, you can access a copy of the disaster recovery information from the alternate location.

A disaster recovery information file contains the following specific information for the computer being backed up:

- Hardware-specific information for each computer, such as hard disk partition information, mass storage controller information, and network interface card information.
- A list of catalog entries that identify the backup sets and storage media that are used to recover the computer.
- The Windows Automated System Recovery configuration information file (asr.xml) for Windows Vista/Windows Server 2008/Windows Server 2008 R2/Windows 7. The ASR file is necessary to recreate partitions on Windows Vista/Server 2008/Windows Server 2008 R2 computers during the recovery process.

- The Windows Automated System Recovery (ASR) configuration information files (asr.sif and asrpn.sif) for Windows XP and Windows Server 2003 computers. The ASR files are necessary to recreate partitions on Windows XP and Windows Server 2003 computers during the recovery process.

See [“About disaster recovery information files”](#) on page 704.

See [“Setting or changing the alternate location for the disaster recovery information file”](#) on page 710.

See [“About the Create Simplified Disaster Recovery Disk Wizard”](#) on page 714.

See [“About backing up data”](#) on page 155.

## Setting or changing the alternate location for the disaster recovery information file

Use the following steps to set or change the alternate location for a disaster recovery information file that is created by Simplified Disaster Recovery.

Backup Exec automatically creates a disaster recovery information file for the SDR-protected computer when it is backed up. Backup Exec then stores the disaster recovery information file in the default location on the Backup Exec server’s hard drive, which is located in the following path:

```
C:\Program Files\Symantec\Backup Exec\sdr\Data\
```

See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.

**To set or change the alternate location for the disaster recovery information file**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, select **Simplified Disaster Recovery**.

- 3 In the **Alternate path** field, enter the alternate location where you want to store a copy of the disaster recovery information file.

You can also click **Browse** to navigate to an alternate location. Symantec recommends that you enter a mapped network location.

Symantec recommends that the alternate location be on another computer or on a different physical drive than the default location.

For a clustered Backup Exec server or remote Backup Exec servers, set the alternate path to a shared drive or to a drive outside the cluster.

When using the Backup Exec Remote Administrator, do not specify a floppy drive (A:, B:) as the alternate location.

- 4 Click **OK**.

Configuring the alternate location is complete. You are ready to run SDR-type backup jobs.

## About changing the default path for the disaster recovery information files

You can change the default path for the disaster recovery information files. You can also manually set an alternate location for the disaster recovery information file.

See [“Changing the default path for the disaster recovery information files”](#) on page 712.

Copies of the disaster recovery information files are necessary to automate the recovery of a Backup Exec server.

Backup Exec automatically creates the disaster recovery information file during a backup and stores it in the following path:

```
C:\Program Files\Symantec\Backup Exec\sdr\Data\
```

Symantec recommends that you do not change the default path.

You should also specify an alternate location where a second copy of the disaster recovery information file is stored. Storing a second copy ensures that the file is available even if the Backup Exec server has been damaged. Symantec recommends that the alternate location be on another computer or on a different physical drive than the default location. The alternate location should also be a mapped network drive.

See [“Disaster recovery information file storage paths”](#) on page 712.

## Changing the default path for the disaster recovery information files

Use the following steps to edit the default path for the disaster recovery information files.

See [“About changing the default path for the disaster recovery information files”](#) on page 711.

### To change the default path for the disaster recovery information files

- 1 Click the Symantec Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, select **Simplified Disaster Recovery**.
- 3 In the **Path** field, change the path to the location where you want to store the disaster recovery information files.  
Symantec recommends that you do not change the default storage location.
- 4 Click **OK**.

See [“Disaster recovery information file storage paths”](#) on page 712.

## Disaster recovery information file storage paths

You can change the default path and the alternative path where you want to store the disaster recovery information file that is created by Simplified Disaster Recovery (SDR).

See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.

Symantec recommends that you do not change the default path.

See [“Changing the default path for the disaster recovery information files”](#) on page 712.

**Table 23-1** Path storage locations for the disaster recovery information file

Item	Description
<b>Path</b>	<p>Indicates a directory path where you want to store the disaster recovery information files for the backed up computers. Backup Exec automatically creates the files during a backup with all critical system components selected. It then stores the disaster information recovery files in the following location:</p> <p>C:\Program Files\Symantec\Backup Exec\sdr\Data\&lt;computer name&gt;.dr.</p>
<b>Alternate path</b>	<p>Indicates an alternate path where where you want to store copies of the disaster recovery information files for the backed up computers. Backup Exec automatically creates or updates the files during a backup with all critical system components selected. It then stores copies of the disaster recovery information files in this specified location after the backup jobs finish running.</p> <p>Symantec recommends that you specify an alternate path that is not on the Backup Exec server, or is on a different physical drive than the default location. During a recovery, you can copy the disaster recovery information file from the alternate path to any location to recover the failed computer if the Backup Exec server's hard drive is unavailable.</p> <p>To use a remote computer's hard drive as the alternate path, establish a valid connection to the remote computer. Specify a UNC path as the alternate path, and then check the directory to make sure the disaster recovery information files were copied.</p> <p>When using Backup Exec's Remote Administrator, do not specify a floppy drive (A:, B:) as the alternative path.</p>

## Requirements and recommendations for running the Create Simplified Disaster Recovery Disk Wizard

Before you run the **Create Simplified Disaster Recovery Disk Wizard**, run a backup of the computer with all critical system components selected.

When running backup jobs with critical system components selected for Simplified Disaster Recovery (SDR) preparation, do the following:

- Ensure that if the computer is a remote computer, a compatible version of the Agent for Windows has been installed on it. You can determine the version of the Agent for Windows by viewing the properties of the Agent for Windows computer through the Windows Explorer.
- Use the Backup Exec Agent for Microsoft SQL to periodically back up the SQL system database. This item applies only if you installed Backup Exec into an existing SQL instance.
- Avoid including files in or excluding files from the backup using the **Selection Details** tab.
- Consider creating a custom Simplified Disaster Recovery Disk if you make considerable hardware changes to the computer.

See [“About the Create Simplified Disaster Recovery Disk Wizard”](#) on page 714.

## About the Create Simplified Disaster Recovery Disk Wizard

The **Create Simplified Disaster Recovery Disk Wizard** guides you through the process of creating a custom bootable recovery disk that you use to recover backed up computers.

If the computer you recover contains a RAID setup, you may first be required to configure the RAID before starting it with the Simplified Disaster Recovery Disk. Use the computer manufacturer's RAID software to configure the RAID system before you start the computer with the Simplified Disaster Recovery Disk.

You can run the **Create Simplified Disaster Recovery Disk Wizard** locally at any Backup Exec server in your environment. When you start the wizard from a particular Backup Exec server, you can create a custom recovery disk from that Backup Exec server. During the creation of the custom recovery disk, you can include storage and network drivers from the computers that the Backup Exec server backs up.

You can also use the **Create Simplified Disaster Recovery Disk Wizard** to create a custom recovery disk that contains storage and network drivers from those computers that are backed up by a different Backup Exec server.

---

**Note:** You can add new OEM drivers to a customized Simplified Disaster Recovery Disk image. However, the drivers that you add must be Windows 7 compatible as SDR uses a minimal version of the Windows 7 operating system to do the recovery.

---

See [“Running the Create Simplified Disaster Recovery Disk Wizard”](#) on page 715.

See [“Requirements and recommendations for running the Create Simplified Disaster Recovery Disk Wizard”](#) on page 714.

See [“About copying the disaster recovery files”](#) on page 715.

## Running the Create Simplified Disaster Recovery Disk Wizard

Use the following steps to run the **Create Simplified Disaster Recovery Disk Wizard**.

**To run the Create Simplified Disaster Recovery Disk Wizard**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Create Disaster Recovery Disk**.
- 2 Follow the instructions in the wizard.

See [“About the Create Simplified Disaster Recovery Disk Wizard”](#) on page 714.

## About copying the disaster recovery files

Backup Exec stores the important disaster recovery information files in both the default path and the alternate location. However, Symantec recommends that you make additional copies of the files and store them in a safe place. Without the disaster recovery information files, you cannot recover Backup Exec servers by using Simplified Disaster Recovery (SDR). Having multiple copies of the disaster recovery information files ensures that you can successfully recover Backup Exec servers with SDR.

The disaster recovery information files reside in the \Program Files\Symantec\Backup Exec\SDR\Data directory on the Backup Exec server. They also reside in the alternate path that you configured during the initial configuration of SDR. Use the Windows Explorer or another Copy utility to copy the disaster recovery information files to another storage location of your choice.

See [“Disaster recovery information file storage paths”](#) on page 712.

# Preparing a custom Simplified Disaster Recovery disk locally for remote Backup Exec servers

You can use the **Create Simplified Disaster Recovery Disk Wizard** on a local Backup Exec server to create or update a custom disaster recovery disk for remote Backup Exec servers.

To prepare a custom Simplified Disaster Recovery disk by using other Backup Exec servers

- 1 Click the Symantec Backup Exec button, select **Configuration and Settings**, and then select **Create Disaster Recovery Disk**.
- 2 On the **Create Simplified Disaster Recovery Disk Wizard Welcome** screen, click **Choose another Backup Exec server**, and then click **Next**.
- 3 Type the name of another Backup Exec server, or click **Browse** to browse the network and select another Backup Exec server.
- 4 Enter the credentials that are required to access the Backup Exec server.  
See [“Backup Exec server logon credential options”](#) on page 716.
- 5 Click **Next** to continue preparing a disaster recover disk.  
See [“Performing a local recovery by using the Recover This Computer Wizard”](#) on page 721.

## Backup Exec server logon credential options

Enter the credentials required to access the Backup Exec server.

See [“Preparing a custom Simplified Disaster Recovery disk locally for remote Backup Exec servers”](#) on page 716.

**Table 23-2** Backup Exec server logon credential options

Item	Description
<b>Backup Exec server</b>	Indicates the name of the remote Backup Exec server that backed up your computer.
<b>Domain</b>	Indicates the domain in which the remote Backup Exec server is a member. If the Backup Exec server is in a workgroup, leave this field blank.

**Table 23-2** Backup Exec server logon credential options (*continued*)

Item	Description
User name	Indicates the user name that has administrator rights to the remote Backup Exec server.
Password	Indicates the password required for access.

## About preparing to recover from a disaster by using Simplified Disaster Recovery

When a disaster occurs, you can use Simplified Disaster Recovery (SDR) to return the computer to its pre-disaster state. To recover a computer, you must follow these steps in order:

---

**Caution:** Disconnect any storage area network (SAN) or cluster that is attached to the computer being recovered; otherwise, the hard drives on those computers may also be repartitioned and reformatted.

---

**Table 23-3** Preparing to recover from a disaster by using Simplified Disaster Recovery

Step	Description
Step 1	Plan any hardware changes to the computer to be recovered.  See <a href="#">“About changing hardware in the computer to be recovered”</a> on page 718.
Step 2	Review additional requirements for IBM computers if the computer to be recovered is an IBM computer.  See <a href="#">“About using Simplified Disaster Recovery to recover IBM computers”</a> on page 719.
Step 3	Start the computer using the generic System Recovery Disk that came with Backup Exec. Or use the custom disk that you created with the <b>Create Simplified Disaster Recovery Disk Wizard</b> to start the recovery process.

**Table 23-3** Preparing to recover from a disaster by using Simplified Disaster Recovery (*continued*)

Step	Description
Step 4	Use the <b>Recover This Computer Wizard</b> to restore the computer to its pre-disaster state.  See <a href="#">“About the Recover This Computer Wizard”</a> on page 720.

---

**Note:** Boot managers, such as System Commander or the OS/2 Boot Manager, cannot be restored with SDR. Boot managers are usually installed at a very low level that Backup Exec cannot protect. For example, the OS/2 Boot Manager resides in its own hard drive volume that Backup Exec cannot access. Because of the many different boot managers available, you may not be able to restart the computer after a SDR recovery, even though the operating system was restored. If this happens, re-installing the boot manager should fix the problem.

---

Before recovering the computer, note the following:

- There must be enough disks to restore all of the critical system disks. A disk is considered critical if it is required for the computer to start successfully.
- Storage disk geometries, which may also be called disk parameters, must be compatible.

See [“About changing hardware in the computer to be recovered”](#) on page 718.

See [“Recovering a computer by using the Recover This Computer Wizard”](#) on page 721.

## About changing hardware in the computer to be recovered

You can use Simplified Disaster Recovery (SDR) to recovery a computer that is no longer functioning. For example, if the computer’s main system board fails, you can restore the computer’s data after you replace the system board. You can also restore the data even if the new board is a different model or it contains multiple processors.

If you plan to change the hardware in the computer being recovered, consider the following information before you use SDR to recover the computer.

**Table 23-4** Hardware considerations when recovering failed computers

Item	Description
<b>Hard drives</b>	Any hard drives you replace should be the same size or larger than the original drives.
<b>System boards</b>	After you replace a faulty system board and after you use SDR to recover the computer, you must use the system board manufacturer's driver CD to re-install additional functionality such as onboard sound and video.
<b>Network interface cards</b>	If you change the network interface card in the computer you are recovering, you must install the necessary network drivers. Without the network drivers, you cannot access the network if you want to use a remote Backup Exec server or remote legacy backup-to-disk folders to recover the computer. After you complete the recovery, you must install new network interface card drivers that match the network card presently in the computer.

See [“About encrypted backup sets and the Recover This Computer Wizard”](#) on page 720.

See [“Recovering a computer by using the Recover This Computer Wizard”](#) on page 721.

## About using Simplified Disaster Recovery to recover IBM computers

To recover an IBM computer equipped with an IBM ServeRAID card, perform the following additional procedures before starting the SDR process:

- Install and configure the IBM ServeRAID controller card and ServeRAID software so that a boot volume will be visible to the Windows operating system.
- Start the server using the IBM server's ServeRAID Configuration and Management CD in the CD-ROM drive prior to using the SDR bootable media. This will start IBM ServeRAID utilities configuration and installation process to view and update the current BIOS and firmware levels.

Refer to the IBM ServeRAID documentation for complete installation instructions for installing Windows on an IBM Server with the ServeRAID controller. Create

and initialize the ServeRAID disks in order for volumes to be visible to the Windows operating system.

See [“About the Recover This Computer Wizard”](#) on page 720.

## About the Recover This Computer Wizard

When you use the **Recover This Computer Wizard** to perform a recovery, you can access the storage devices that are required to restore from the following sources.

You can do the following:

- Use locally attached storage devices at the computer that you want to recover.
- Submit restore jobs to remote Backup Exec servers.

To restore data by using the **Recover This Computer Wizard**, the following items are required:

- A disaster recovery information file if the computer to be recovered was backed up to a tape device.
- The backup set that contains all of the critical system components for the computer that is being restored.
- If you want to recover a computer locally, storage must be connected to the computer that you want to recover.

See [“Recovering a computer by using the Recover This Computer Wizard”](#) on page 721.

See [“About encrypted backup sets and the Recover This Computer Wizard”](#) on page 720.

See [“Performing a local recovery by using the Recover This Computer Wizard”](#) on page 721.

## About encrypted backup sets and the Recover This Computer Wizard

The **Recover This Computer Wizard** supports the recovery of computers with previously encrypted backup sets.

If the Simplified Disaster Recovery (SDR) backups are encrypted during backup, the wizard prompts you for the pass phrase of each encrypted backup set that is required to complete the recovery.

See [“About encryption key management”](#) on page 477.

## Recovering a computer by using the Recover This Computer Wizard

To recover a computer with the **Recover This Computer Wizard**, the following process must be followed.

---

**Warning:** If you backed up the Backup Exec server to tape, you must have the current disaster recovery information file available. If the file is unavailable or if the file is not current, you cannot recover the computer with Simplified Disaster Recovery (SDR).

See [“About the Recover This Computer Wizard”](#) on page 720.

See [“Performing a local recovery by using the Recover This Computer Wizard”](#) on page 721.

---

**Table 23-5** Process for recovering a computer by using the Recover This Computer Wizard

Step	Action
Step 1	Start the computer by using the generic Simplified Disaster Recovery Disk that came with Backup Exec, or use the custom disk that you created with the <b>Create Simplified Disaster Recovery Disk Wizard</b> .
Step 2	Use the <b>Recover This Computer Wizard</b> to recover the computer to its pre-disaster state.

## Performing a local recovery by using the Recover This Computer Wizard

Use the following steps to perform a local recovery by using the **Recover This Computer Wizard**.

See [“About the Recover This Computer Wizard”](#) on page 720.

**To perform a local recovery by using the Recover This Computer Wizard**

- 1 Place the bootable Simplified Disaster Recovery Disk in the CD or DVD drive of the computer to be recovered and then start the computer.
- 2 Select the language you want to use.
- 3 On the Simplified Disaster Recovery **Welcome** screen, click **Recover This Computer**.

- 4 Select the option **The data is located on devices locally attached to this computer.**

---

**Note:** If SCSI or RAID controller drivers are required, the drivers are automatically installed if the **Recover This Computer Wizard** finds them in its driver database. If the SCSI or RAID drivers are not found, click **Install Driver** to install the required drivers.

---

- 5 Continue the recovery by following the wizard instructions.

## Performing a remote recovery by using the Recover This Computer Wizard

Use the following steps to perform a remote recovery by using the **Recover This Computer Wizard**.

To perform a remote recovery by using the Recover This Computer Wizard

- 1 Place the bootable Simplified Disaster Recovery Disk in the CD or DVD drive of the computer to be recovered and then start the computer.
- 2 Select the language you want to use.
- 3 On the Simplified Disaster Recovery **Welcome** screen, click **Recover This Computer**.
- 4 Select the option **The data is located on devices attached to a remote Backup Exec server**.
- 5 Enter the administrator or administrator-equivalent credentials that are required to access the remote Backup Exec server where the backup data is located.
- 6 Continue the recovery by following the wizard instructions.

See [“Installing network controller drivers”](#) on page 722.

See [“Configuring network adapter settings ”](#) on page 723.

## Installing network controller drivers

You can install network controller drivers from any screen in the **Recover This Computer Wizard** where the **Configure network adapter settings** or **Load network adapter drivers** buttons appear.

See [“Performing a local recovery by using the Recover This Computer Wizard”](#) on page 721.

#### To install network drivers

- 1 Click **Load network adapter drivers**.
- 2 On the **Load drivers for network controllers** screen, click **Install Driver** for any inactive network controller that the wizard detects.
- 3 Navigate to the device that contains the network controller driver, and then click **Open**.
- 4 Select the driver, and then click **Open**.

## Configuring network adapter settings

You can configure network adapter settings in the **Recover This Computer Wizard** where the **Configure network adapter settings** button appears.

#### To configure network adapter settings

- 1 Click **Configure network adapter settings**.
- 2 To assign a static IP address for each detected network adapter, select the appropriate options.  
  
By default, each network adapter is assigned IP addresses from the default DHCP server.
- 3 To configure an IPv6 network controller, click **Configure IPv6**.
- 4 Select the appropriate options, and then click **OK**.

See [“Performing a remote recovery by using the Recover This Computer Wizard”](#) on page 722.

## About the simplified volume layout view

The **Recover This Computer Wizard** lets you restore the hard drive volumes on the computer being recovered to the same sizes they were before the disaster occurred. Using disk geometry information from the disaster recovery information file, the **Recover This Computer Wizard** presents the original disk geometry in a simplified volume layout view. Within the simplified layout view, you can accept the disk geometry as it originally existed before the disaster, or you can alter the geometry by changing the volume sizes. Depending on the size of the existing disks, you can alter volume sizes in megabytes, gigabytes, or terabytes.

The simplified layout view offers you a **Preview** tab where you can view the disk geometry as it presently exists. If you decide to alter the disk geometry and change volume sizes, you can also click the **Preview** tab to see a graphical representation of your proposed changes.

If mismatched volumes appear in the simplified volume layout view, you can use the option **Erase hard disks and recreate the volume layout shown above** to automatically create a volume layout on the available hard disks. You can also manually create a volume layout by using the **Advanced Disk Configuration** option.

If you want to make additional changes to the computer's disk configuration, Symantec recommends that you run **Advanced Disk Configuration**.

See [“About Advanced Disk Configuration”](#) on page 724.

## About Advanced Disk Configuration

When you recover a computer, the **Recover This Computer Wizard** restores the hard drive volumes to the same sizes they were before the disaster. If the hard drive in the failed computer is larger than the hard drive that was in place before the disaster, you may end up with unused and unallocated space. You can run the Advanced Disk Configuration program to alter the volume sizes to reflect the larger hard drive size.

The following is an example of why the hard drive volumes should be resized:

If the pre-disaster computer hardware contained a 40 GB hard drive with two 20 GB volumes, and you replaced it with a 90 GB model, SDR (using the disaster recovery information file) rebuilds the hard disk partition table by using the partition information that is found on the original 40 GB hard drive. As a result, only 40 GB of space is allocated on the new 90 GB hard drive, with a partition map that consists of two 20 GB partitions.

You can access Advanced Disk Configuration from within the **Recover This Computer Wizard**.

---

**Note:** You should be familiar with Microsoft Disk Management concepts before you run Advanced Disk Configuration.

---

The following table provides details about additional disk-related operations that you can do with Advanced Disk Configuration.

**Table 23-6**      Advanced Disk Configuration tasks

Task	Description
<b>Create a simple volume</b>	A simple volume is a partition on a disk that contains a file system.

**Table 23-6** Advanced Disk Configuration tasks (*continued*)

Task	Description
<b>Format a volume</b>	Disk volumes, as the primary storage devices on a computer, must be formatted before data can be stored on them. When you replace a failed hard disk in a disaster recovery situation, you may need to format the new hard disk so that Windows can store data on it.
<b>Extend the size of a volume</b>	If a disk contains some unallocated disk space that is adjacent to a functional volume, you can extend the volume to include the free space. To extend the volume, it must be either raw or formatted with the Windows NTFS file system.
<b>Shrink the size of a volume</b>	<p>You can decrease the size of a volume by shrinking the volume into the contiguous and unallocated disk space that is on the same disk.</p> <p>When you shrink a volume, there is no need to reformat the volume. Ordinary files are automatically relocated on the disk to create the new, unallocated disk space.</p>
<b>Create a spanned volume</b>	<p>A spanned volume is a volume that spans more than one physical disk. You can create a spanned volume by spanning it across multiple physical disks, or by spanning the volume into unallocated disk space.</p> <p>To create a spanned volume, you must have a startup volume and at least two dynamic volumes.</p> <p><b>Note:</b> Spanned volumes are not fault-tolerant.</p>
<b>Create a striped volume</b>	Striped volumes store data in stripes across two or more physical disks. Although striped volumes do not provide fault-tolerance protection, they do offer the best performance of all the volumes in Windows.

**Table 23-6**      Advanced Disk Configuration tasks (*continued*)

Task	Description
<b>Create a mirrored volume</b>	A mirrored volume provides an exact copy of the data that is written to a selected volume. Because all data is written to both the mirrored volume and the selected volume, mirroring reduces the capacity of both volumes by 50%.
<b>View volume properties</b>	You can view properties for each volume in the Current Disk Layout view or in the Original Disk Layout view.
<b>Change an assigned drive letter</b>	You can change assigned drive letters for all volumes if you want to organize your drive letters in a certain way.
<b>Delete a volume</b>	Deleting a volume erases all data from the volume so Symantec recommends caution when considering the use of this option.
<b>Convert a basic disk to a dynamic disk</b>	Converting basic disks to dynamic disks lets you create volumes that span multiple disks. Dynamic disks also let you create fault-tolerant volumes, such as mirrored volumes and RAID-5 volumes. All volumes on dynamic disks are referred to as dynamic volumes.
<b>Convert a Master Boot Record (MBR) disk to a Guid Partition Table (GPT) disk</b>	<p>Master boot record (MBR) disks use the standard BIOS interface. GUID partition table (GPT) disks use extensible firmware interface (EFI).</p> <p>You can convert MBR disks to GPT disks as long as the disk does not contain partitions or volumes.</p>

**Table 23-6** Advanced Disk Configuration tasks (*continued*)

Task	Description
<b>Convert a Guid Partition Table (GPT) disk to a Master Boot Record (MBR) disk</b>	<p>GUID partition table (GPT) disks use extensible firmware interface (EFI). Master boot record (MBR) disks use the standard BIOS interface.</p> <p>GPT disks can be converted to MBR disks as long as the disk does not contain partitions or volumes.</p>
<b>View the original disk layout geometry</b>	<p>The original disk layout shows the actual hard disk layout that existed during the backup job.</p> <p>See <a href="#">“About viewing the original disk layout geometry”</a> on page 727.</p> <p>See <a href="#">“About the simplified volume layout view”</a> on page 723.</p>

See [“About the simplified volume layout view”](#) on page 723.

### About viewing the original disk layout geometry

The original disk layout geometry appears in Advanced Disk Configuration beneath the current disk layout geometry view and is derived from the disaster recovery information file. The original disk layout shows the actual hard disk layout that existed during the backup job.

See [“About the simplified volume layout view”](#) on page 723.

See [“About Advanced Disk Configuration”](#) on page 724.

## Microsoft SQL Server recovery notes

The Agent for Microsoft SQL Server must be installed on the Backup Exec server to perform a complete SQL Server database recovery.

After using Simplified Disaster Recovery (SDR) to recover the Windows server, SDR automatically replaces the damaged master and model databases with copies of the master and model databases. After SQL is restarted and the latest master database backup and all other system databases are restored, you must still restore all user databases after completing the SDR recovery.

See [“About the Advanced Disk-based Backup Option”](#) on page 1047.

## Microsoft Exchange recovery notes

The Agent for Microsoft Exchange Server must be installed on the Backup Exec server to perform a complete Exchange Server database recovery.

After you use Simplified Disaster Recovery (SDR) to recover the Windows server, use Backup Exec to restore the Exchange Server databases from the most recent Exchange Server database backups.

See [“About the Backup Exec Exchange Agent”](#) on page 834.

## SharePoint Portal Server recovery notes

You can use Simplified Disaster Recovery (SDR) to recover a Windows server that has SharePoint Portal Server 2001 installed. After you restore the Windows computer, you must restart it. After the computer restarts, however, the SharePoint Portal Server software is installed but is not functional. You must remove SharePoint Portal Server 2001 and reinstall it before the SharePoint data can be restored.

See [“About the Agent for Microsoft SharePoint”](#) on page 866.

# About using Simplified Disaster Recovery with the Central Admin Server Option

In a CASO environment, Simplified Disaster Recovery (SDR) stores the disaster recovery information file on the computer that runs the backup job in the following locations:

- In the computer's disaster recovery data path.
- In the alternate path.

When you use SDR to recover a computer in CASO environment, you can submit the remote restore job to either of the following:

- The central administration server.
- The managed Backup Exec server that performed the original backup job.

See [“Disaster recovery information file storage paths”](#) on page 712.

See [“About setting an alternate location for a disaster recovery information file”](#) on page 709.

See [“About the Central Admin Server Option”](#) on page 996.

# Best practices for Simplified Disaster Recovery

The following table presents best practices when using Simplified Disaster Recovery (SDR).

**Table 23-7** Best practices for Simplified Disaster Recovery

Item	Description
Remote SDR	To perform disaster recovery of a remote computer, you must purchase the Agent for Windows separately, and it must be running on the remote computer.
Disaster Recovery	Consider the following: <ul style="list-style-type: none"><li>■ The number of installed hard disks must be the same size or larger than the original.</li><li>■ The latest RAID, SCSI, or NIC (if remote) drivers are required.</li></ul>
UEFI support	SDR supports recovering computers that use the Unified Extensible Firmware Interface standard. However, backups of UEFI-based computers cannot be restored to standard BIOS-based computers. <b>Note:</b> UEFI computers use GPT-style disks. MBR-style disk data cannot be restored to GPT-style disk, and vice versa.  For computers that support both UEFI and BIOS firmware types, you must start the computer using UEFI firmware if you backed up the computer in that mode.
OEM partitions	If you have OEM partitions such as Dell Utility partitions on the system, they are considered part of a computer's critical system components and are backed up and restored as such.

See [“About Simplified Disaster Recovery”](#) on page 704.



# Symantec Backup Exec Agent for Windows

This appendix includes the following topics:

- [About the Agent for Windows](#)
- [Requirements for the Agent for Windows](#)
- [Stopping and starting the Agent for Windows](#)
- [About establishing a trust between the Backup Exec server and a remote computer](#)
- [About the Backup Exec Agent Utility for Windows](#)
- [About the Backup Exec Agent Utility Command Line Applet](#)
- [Backup Exec Agent Utility Command Line Applet switches](#)

## About the Agent for Windows

The Symantec Backup Exec Agent for Windows (Agent for Windows) is installed as a separate add-on component. The Agent for Windows enables Windows Servers network administrators to perform backup and restore operations on Windows resources that are connected to the network.

The Agent for Windows is a system service that runs on remote Windows servers and workstations. The Agent for Windows provides faster backup processing by locally performing tasks that in typical backup technologies, require extensive network interaction. The Agent for Windows processes backup data into a continuous stream that the Backup Exec server then processes as a single task. This method provides better data transfer rates over traditional technologies,

which require multiple requests and acknowledgments between the Backup Exec server and the remote server.

The Agent for Windows enables you to do the following:

- Back up and restore in firewall environments.
- Back up and restore using a specified local network if the Backup Exec server and the remote computer are on the same subnet.
- Display the remote computer in the list of server's on the **Backup and Restore** tab.
- Attain significant performance increases when running modified backups (for example, differential and incremental). This occurs because file selection is performed locally by the Agent for Windows instead of across the network as performed by traditional network backup applications.

---

**Note:** Network hardware has a major impact on performance. Performance is directly related to the capabilities of the networking hardware in the Backup Exec server and the remote device. Higher network bandwidth ratings also contribute to faster operation processing.

---

See [“Requirements for the Agent for Windows”](#) on page 732.

See [“About installing the Agent for Windows”](#) on page 83.

See [“Changing network and security options”](#) on page 470.

See [“About using Backup Exec with firewalls”](#) on page 472.

See [“About the Backup Exec Shadow Copy Components file system”](#) on page 540.

See [“About the Backup Exec Agent Utility for Windows”](#) on page 735.

## Requirements for the Agent for Windows

Because a Agent for Windows is also a Client Access License (CAL), you must install the Agent for Windows on any remote Windows computer that you want to back up. You cannot fully protect resources on a remote server until a Agent for Windows has been installed.

At the Backup Exec server, you must enter Agent for Windows licenses for each remote Windows computer that you want to protect. To back up a remote Windows computer from more than one Backup Exec server, you must enter the same Agent for Windows licenses on each Backup Exec server.

Backup Exec database agents also include a Agent for Windows that allows you to protect one remote Windows computer. The Agent for Windows license is enabled when you install the database agents on the Backup Exec server.

To protect the Workstation versions of the supported Windows platforms, you must install the Agent for Windows on each platform.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

---

**Note:** If a previous version of the Agent for Windows is installed, it is automatically upgraded when you initiate a new Agent for Windows installation. Previous versions of the Agent for Windows are automatically detected on the remote computers and replaced with the new version during installation of the new Agent for Windows. The name of the system service may have changed when the upgrade is complete.

---

You can install the Agent for Windows using many methods, depending on your environment.

See “[About installing the Agent for Windows](#)” on page 83.

## Stopping and starting the Agent for Windows

The Agent for Windows is automatically started as a service when Windows is started on the remote computer.

### To stop or start the Agent for Windows

**1** Do one of the following:

On Windows 7/Vista/Server 2008  
R2/Server 2008 computers

Right-click **Computer**.

On a Windows Server 2003 computer

Right-click **My Computer**.

**2** Click **Manage**.

**3** Do one of the following:

On a Windows Server 2008 R2/Server 2008 computer

On the **Server Manager** dialog box, expand **Configuration**.

On Windows 7/Vista/Server 2003 computers

On the **Computer Management** dialog box, double-click **Services and Applications**.

**4** Click **Services**.

**5** In the Results pane, right-click **Backup Exec Agent for Windows**.

**6** Do one of the following:

To stop the Agent for Windows

Click **Stop** to stop the Agent for Windows.

To start the Agent for Windows

Click **Start** to start the Agent for Windows.

## About establishing a trust between the Backup Exec server and a remote computer

When you connect to a remote computer from the Backup Exec server, you must establish a trust between the Backup Exec server and the remote computer. You must also establish this trust if you want to configure a remote computer to perform client-side deduplication. You should check the IP address for the remote computer to ensure that the remote computer is a trusted source before you establish the trust. After you verify that the remote computer is a trusted source, you can establish the trust with the Backup Exec server. Backup Exec issues a security certificate for both the Backup Exec server and the remote computer. The security certificate is valid for approximately one year and is automatically renewed during normal operations. However, if the certificate expires you must re-establish the trust.

You can establish a trust between the Backup Exec server and the remote computer in the following ways:

- Push-install the Agent for Windows to one or more remote computers from the Backup Exec server. The trust between the remote computer and the Backup Exec server is automatically established during installation. See [“About push-installing the Agent for Windows to remote computers”](#) on page 83.

- Add the remote computer to the list of servers on the **Backup and Restore** tab. See [“Establishing a trust for a remote computer”](#) on page 735.

## Establishing a trust for a remote computer

You can add one or more remote computers that are in a domain or a workgroup to the list of servers on the **Backup and Restore** tab. When you add the remote computer you must establish a trust between the Backup Exec server and the remote computers to ensure secure communication.

### To establish a trust between the Backup Exec server and one or more remote computers

- 1 On the Backup and Restore tab, in the **Servers** group, click **Add**.
- 2 Click Microsoft Windows computer.
- 3 Follow the on-screen prompts.

See [“About establishing a trust between the Backup Exec server and a remote computer”](#) on page 734.

## About the Backup Exec Agent Utility for Windows

The Backup Exec Agent Utility is installed when the Agent for Windows is installed on a remote Windows computer.

You can perform the following tasks with the Backup Exec Agent Utility:

- Start the Backup Exec Agent Utility each time you log on. See [“Starting the Backup Exec Agent Utility”](#) on page 736.
- View current activity on the remote Windows computer. See [“Viewing the activity status of the remote computer from the system tray”](#) on page 737.
- Configure the Agent for Windows to send information about itself, such as its version and IP address, to a Backup Exec server. See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.
- Configure the Backup Exec Agent Utility for backup and restore operations of Oracle instances. See [“Configuring an Oracle instance on Linux servers”](#) on page 893.
- Configure the Backup Exec Agent Utility for Backup Exec server database access for Oracle operations. See [“Configuring database access”](#) on page 742.

## Starting the Backup Exec Agent Utility

You access the Backup Exec Agent Utility from the Windows taskbar.

See [“Viewing the activity status of the remote computer in the Backup Exec Agent Utility”](#) on page 736.

See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.

### To start the Backup Exec Agent Utility

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 To open the Registry Editor, the Services window, and the Event Viewer on the remote Windows computer, right-click the Backup Exec Agent Utility icon in the system tray, and then click **Tools**.

## Viewing the activity status of the remote computer in the Backup Exec Agent Utility

You can use the Backup Exec Agent Utility to view the activity status of the remote Windows computer.

### To view the activity status of the remote computer in the Backup Exec Agent Utility

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

If the Backup Exec Agent Utility is already running, you can double-click its icon in the system tray.

- 2 Click the **Status** tab.

See [“Status options for the Backup Exec Agent Utility”](#) on page 736.

- 3 Click **OK**.

## Status options for the Backup Exec Agent Utility

You can set the following status options for the Backup Exec Agent Utility.

See [“Viewing the activity status of the remote computer in the Backup Exec Agent Utility”](#) on page 736.

**Table A-1** Backup Exec Agent Utility Status options

Item	Description
<b>Start the Backup Exec Agent Utility every time you log on</b>	Indicates if the Backup Exec Agent Utility displays when you log on to this computer.
<b>Refresh interval</b>	Displays the number of seconds for the Backup Exec Agent Utility to wait before refreshing the status of the computer. The default setting is to refresh every 5 seconds.
<b>Backup Exec server</b>	Displays the name of the Backup Exec server that is processing the current operation.
<b>Source</b>	Displays the media or share that is being processed.
<b>Current folder</b>	Displays the name of the current directory, folder, or database (depending on the specific agent) that is being processed.
<b>Current file</b>	Displays the name of the current file that is being processed.

## Viewing the activity status of the remote computer from the system tray

You can view the activity status for a remote computer.

Possible statuses are as follows:

- A backup job is running
- A restore job is running
- A backup and a restore job are running
- Snapshot in progress
- The Backup Exec client service, Beremote.exe, is not running on the computer
- Idle

**To view the activity status of a remote computer**

- ◆ Position the cursor over the Agent for Windows icon in the system tray.

## Starting the Backup Exec Agent Utility automatically on the remote computer

You can start the Backup Exec Agent Utility automatically each time you log on to the remote computer.

See [“Status options for the Backup Exec Agent Utility”](#) on page 736.

#### To start the Backup Exec Agent Utility automatically on the remote computer

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

If the Backup Exec Agent Utility is already running, you can double-click its icon in the system tray.

- 2 Click the **Status** tab.
- 3 Check the **Start the Backup Exec Agent Utility every time you log on** check box.
- 4 Click **OK**.

## Setting the refresh interval on the remote computer

You can display the number of seconds for the Backup Exec Agent Utility to wait before refreshing the status of the computer.

See [“Status options for the Backup Exec Agent Utility”](#) on page 736.

#### To set the refresh interval on the remote computer

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

If the Backup Exec Agent Utility is already running, you can double-click its icon in the system tray.

- 2 Click the **Status** tab.
- 3 In the **Refresh interval** box, type the number of seconds to refresh the status.
- 4 Click **OK**.

## About publishing the Agent for Windows to Backup Exec servers

Use the Backup Exec Agent Utility to add, change, or delete the Backup Exec server names or IP addresses that this remote Windows computer publishes to. Each Backup Exec server that you add to the list on the Publishing tab displays this remote computer in the list of servers on the **Backup and Restore** tab.

This information that the Agent for Windows publishes includes the version of the Agent for Windows and the remote computer’s IP addresses. Because the remote computer’s IP address is published to the Backup Exec server, the Backup

Exec server can connect to and display the remote computer even if it is in an unknown domain.

For each Backup Exec server that is published to, you can specify a local backup network for operations between the Backup Exec server and the remote computer. Directing jobs to a specified local network rather than to a corporate network isolates the backup data traffic so that other connected networks are not affected when operations are performed between the Backup Exec server and the remote computer.

See [“About specifying backup networks”](#) on page 548.

See [“Adding Backup Exec servers that the Agent for Windows can publish to”](#) on page 739.

See [“Editing Backup Exec server information that the Agent for Windows publishes to”](#) on page 741.

See [“Removing Backup Exec servers that the Agent for Windows can publish to”](#) on page 742.

## Adding Backup Exec servers that the Agent for Windows can publish to

You can use the Backup Exec Agent Utility to add a Backup Exec server that the Agent for Windows can publish information.

See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.

See [“About the list of servers”](#) on page 157.

See [“Viewing the activity status of the remote computer from the system tray”](#) on page 737.

### To add Backup Exec servers that the Agent for Windows can publish to

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 Click the **Publishing** tab.
- 3 Complete the appropriate options.

See [“Backup Exec Agent Utility Publishing options”](#) on page 740.

- 4 Click **OK**.

## Backup Exec Agent Utility Publishing options

You can set the following publishing options for the Backup Exec Agent Utility. See [“Adding Backup Exec servers that the Agent for Windows can publish to”](#) on page 739.

**Table A-2** Backup Exec Agent Utility Publishing options

Item	Description
<b>Enable the Agent for Windows to publish information to the Backup Exec servers in the list</b>	<p>Indicates if the Agent for Windows sends information about itself, such as its version and IP address, to all of the Backup Exec servers in the list. The Backup Exec servers display the Agent for Windows in the list of servers.</p> <p>By default, the name of the Backup Exec server that push-installed this Agent for Windows is displayed in this list. If the Agent for Windows is also a Backup Exec server, the name is displayed as 127.0.0.1.</p> <p>To stop the information from being sent to all of the Backup Exec servers, uncheck <b>Enable the Agent for Windows to publish information to the Backup Exec servers in the list</b>. The list of Backup Exec servers is preserved, but the Agent for Windows does not send any information about itself to the Backup Exec servers.</p>
<b>Publishing interval</b>	<p>Displays an interval, in minutes, for the Agent for Windows to send information about its status to the Backup Exec servers in the list. The default interval is 240 minutes. This is the recommended setting to appropriately balance system responsiveness with network traffic. The maximum interval allowed is 720 minutes.</p>
<b>Change Settings</b>	<p>Enables the settings to let you add, edit, or remove Backup Exec servers in the Backup Exec servers list.</p> <p>This option appears the first time you start the Backup Exec Agent Utility.</p>
<b>Add</b>	<p>Lets you add the Backup Exec server name or IP address to the Backup Exec servers list.</p>
<b>Edit</b>	<p>Lets you edit the Backup Exec server name or IP address in the Backup Exec servers list.</p>

**Table A-2** Backup Exec Agent Utility Publishing options (*continued*)

Item	Description
<b>Remove</b>	Lets you delete a Backup Exec server name or IP address from the Backup Exec servers list. The Agent for Windows no longer publishes information to the Backup Exec server. You cannot select the remote computer for backup from the Backup Exec server's Favorite Resources node.
<b>Published names for this agent</b>	Shows the names that are used when this remote computer is published. The names appear under a Backup Exec server's Favorite Resources.  These names can include the following: <ul style="list-style-type: none"> <li>■ The fully qualified domain name.</li> <li>■ The computer name.</li> <li>■ The NetBIOS computer name.</li> <li>■ Virtual Service names, which are the names given to clustered resources that are hosted by the remote computer.</li> <li>■ Oracle RMAN Real Application Cluster (RAC) name, which is the virtual name used by computers in a RAC for the computer that hosts the Oracle application. This name is displayed in a Backup Exec server's backup selection list under the Oracle RAC node.</li> </ul>

## Editing Backup Exec server information that the Agent for Windows publishes to

You can use the Backup Exec Agent Utility to edit a Backup Exec server name or IP address to which the Agent for Windows can publish information.

See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.

### To edit Backup Exec server information

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 Click the **Publishing** tab.
- 3 Select the Backup Exec server that you want to edit from the list.
- 4 Click **Edit**.

- 5 Edit the Backup Exec server name or IP address.
- 6 Click **OK**.

## Removing Backup Exec servers that the Agent for Windows can publish to

You can use the Backup Exec Agent Utility to remove a Backup Exec server so that the Agent for Windows no longer publishes information to it.

See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.

### To remove Backup Exec servers that the Agent for Windows can publish to

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 Click the **Publishing** tab.
- 3 Select the Backup Exec server that you want to remove from the list.
- 4 Click **Remove**.
- 5 Click **OK**.

## Configuring database access

You can configure database access to enable the Backup Exec server to authenticate Oracle operations.

See [“Setting authentication credentials on the Backup Exec server for Oracle operations”](#) on page 898.

### To configure database access

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.
- 2 Click the **Database Access** tab.
- 3 To make changes, click **Change Settings**.
- 4 Complete the appropriate options.

See [“Database access options for the Backup Exec Agent Utility”](#) on page 743.

- 5 Click **OK**.
- 6 On the Backup Exec server, add the name of the Oracle server and the user name that you entered on the Database Access tab to the Backup Exec server's list of authentication credentials.

## Database access options for the Backup Exec Agent Utility

You can set the following database access options for the Backup Exec Agent Utility.

See [“Configuring database access”](#) on page 742.

**Table A-3** Backup Exec Agent Utility database access options

Item	Description
<b>Enable the Backup Exec server to authenticate Oracle operations</b>	Specifies the credentials that the Backup Exec server will use for all operations on the Oracle server, including DBA-initiated operations. The Backup Exec server also uses these credentials for authentication of the Oracle server.  You must check this to enable Oracle operations between the Backup Exec server and this computer.

**Table A-3** Backup Exec Agent Utility database access options (*continued*)

Item	Description
<b>User name</b>	<p>Specifies a user name that has administrative rights to this computer. This logon account is what the Backup Exec server uses when it connects to this computer.</p> <p>If you specify an IP address or a fully qualified computer name as part of the user name, the Backup Exec Agent Utility may not be able to verify the user account. If the credentials entered are incorrect, the error “cannot attach to a resource” may be displayed when you run a backup or restore job.</p> <p>You must add this computer name and logon account to the Backup Exec server's list of authentication credentials for Oracle servers. If the authentication fails when the Oracle resources are backed up, the backup job fails. If the authentication fails when you are browsing the backup sets for a restore job, then the backup sets become unavailable, and you must run a DBA-initiated restore job to restore data.</p>
<b>Password</b>	<p>Specifies the password for this logon account.</p> <p><b>Note:</b> For security reasons, the logon credentials are not stored on the remote computer.</p>
<b>Confirm Password</b>	<p>Specifies the password again to confirm it.</p>
<b>Use a custom port to connect to the Backup Exec server during Oracle operations</b>	<p>Designates the port that is used for communications between this computer and the Backup Exec server during Oracle operations. By default, port 5633 is used.</p> <p>If you change the port number on this computer, you must also change it on the Backup Exec server, and then restart the Backup Exec Job Engine Service on the Backup Exec server.</p>

**Table A-3** Backup Exec Agent Utility database access options (*continued*)

Item	Description
<b>Port number</b>	Specifies the port number to use for operation requests that are sent to the Backup Exec server.

## Removing a security certificate for a Backup Exec server that has a trust with the Agent for Windows

You can remove the security certificate for a Backup Exec server that has established a trust with the Agent for Windows.

See [“Backup Exec Agent Utility Security options”](#) on page 745.

### To remove a security certificate for a Backup Exec server

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.
- 2 On the **Security** tab, click **Change Settings**.
- 3 Select the Backup Exec server that you want to remove the security certificate for, and then click **Remove**.
- 4 Click **OK**.

## Backup Exec Agent Utility Security options

You can view the following information for the Backup Exec servers that have a trust with the Agent for Windows.

See [“Removing a security certificate for a Backup Exec server that has a trust with the Agent for Windows”](#) on page 745.

**Table A-4** Backup Exec Agent Utility Security options

Item	Description
<b>Backup Exec Server</b>	Displays the name of the Backup Exec server to which the security certificate was issued.
<b>Issued To</b>	Displays the name of the Agent for Windows to which the security certificate was issued.

**Table A-4** Backup Exec Agent Utility Security options (*continued*)

Item	Description
Issued By	Displays the name of the certificate authority from which the security certificate was issued.
Expiration Date	Displays the date that the security certificate expires.
Hash	Displays the unique identifier for the client certificate.
CA Hash	Displays the unique identifier for the CA certificate.

## About the Backup Exec Agent Utility Command Line Applet

You can use the Backup Exec Agent Utility Command Line Applet from any Windows operating system command prompt to access the Backup Exec Agent Utility. The Backup Exec Agent Utility Command Line Applet is installed when you install the Agent for Windows. If you run the command line utility on a Windows 7/Vista/Server 2008 R2/Server 2008 computer, you must run it in elevated command prompt.

---

**Note:** To run the Backup Exec Agent Utility Command Line Applet on a Microsoft Windows Server 2008 R2/Server 2008 computer, you must use Server Core.

---

You can run the following Backup Exec Agent Utility functions with the Backup Exec Agent Utility Command Line Applet:

- Set the publishing interval (in minutes).
- List the published name for the agent.
- List the Backup Exec server names to which the agent is publishing.
- Add a Backup Exec server to the publishing list.
- Remove a Backup Exec server from the publishing list.
- View the following status information:
  - Activity status

- Current source
- Current folder
- Current file
- Currently attached Backup Exec server

See [“Using the Backup Exec Agent Utility Command Line Applet”](#) on page 747.

## Using the Backup Exec Agent Utility Command Line Applet

Use the following steps to use the Backup Exec Agent Utility Command Line Applet.

See [“About the Backup Exec Agent Utility Command Line Applet”](#) on page 746.

### To use the Backup Exec Agent Utility Command Line Applet:

- 1 Open a command prompt.
- 2 From the Backup Exec installation directory, type `ramcmd.exe` followed by a series of command switches.

The default installation location is `c:\Program Files\Symantec\Backup Exec\RAWS`

See [“Backup Exec Agent Utility Command Line Applet switches”](#) on page 747.

## Backup Exec Agent Utility Command Line Applet switches

The following table describes the switches that you can use with the Backup Exec Agent Utility Command Line Applet.

See [“About the Backup Exec Agent Utility Command Line Applet”](#) on page 746.

**Table A-5** Backup Exec Agent Utility Command Line Applet switches

Switch	Description
<code>status:[n]</code>	<p>Status output is repeated every &lt;n&gt; seconds, with a range of 1 - 86400. Press Q to stop the output from running.</p> <pre>ramcmd /status:[n]</pre> <p>When you use the <code>/status</code> switch without a time value, the Agent for Windows status appears in the command window and then the applet exits.</p>

**Table A-5** Backup Exec Agent Utility Command Line Applet switches  
*(continued)*

Switch	Description
<p>/publish:[on   off   add   remove   interval][/ms:&lt;Backup Exec server&gt;] [/t:&lt;x&gt;]</p>	<p>Use the following parameters with the /publish switch:</p> <ul style="list-style-type: none"> <li>■ No parameter specified- Displays the publishing status and then exits.</li> <li>■ [on] - Turns publishing on. Lets the Agent for Windows send information about itself, such as its version and IP address.</li> <li>■ [off] - Turns publishing off.</li> <li>■ [add], [remove] - Used with /ms. You can use this parameter to add or remove Backup Exec servers from the Agent for Windows publish list.</li> <li>■ [interval] - Used with /t. Specifies the time interval that the Agent for Windows sends information about itself to the Backup Exec server.                      You can set the time interval in minutes using the /t:[&lt;x&gt;] parameter.</li> </ul> <p><b>Note:</b> The [interval] switch must be used with the /t: switch. Using [interval] alone on the command line is not supported.</p> <pre>ramcmd /publish:[on off add remove interval] [/ms&lt;Backup Exec server&gt;] [/t:&lt;x&gt;]</pre>

**Table A-5** Backup Exec Agent Utility Command Line Applet switches  
*(continued)*

Switch	Description
/oracle: [new   edit   delete] /in:[<instance name>] /ms:[<Backup Exec server   address>] /jt:[<job template>] /user:[<username>] /password:[<password>   * ] /rc: [yes   no] /tns:[<TNS name>]	Use the following parameters with the /oracle switch: <ul style="list-style-type: none"> <li>■ No parameter specified- Displays the existing Oracle instances and then exits.</li> <li>■ [new], [edit], [delete] - Used with switch /in.</li> <li>■ /in:[&lt;instance name&gt;] - Used to add, edit, and delete Oracle instance names from the Oracle instance list.</li> <li>■ /ms:[&lt;Backup Exec server name   address&gt;] - Sets the Backup Exec server name or its IP address.</li> <li>■ /jt:[&lt;job template&gt;] - Sets a Backup Exec job template.</li> <li>■ /user:[&lt;username&gt;] - Sets a username.</li> <li>■ /password:[&lt;password&gt;   *] - Sets a password to be used with /user:[&lt;username&gt;]. If you omit the password, or you use an asterisk [*], you do not need to enter the password on the command line. After the command runs, a prompt appears asking you for a password.</li> <li>■ /rc:[yes   no] - Turns the Use recover catalog setting on or off. If /rc appears without a parameter, then the current status for that instance is displayed.</li> <li>■ /tns:[TNS name] - Sets the TNS name alias of an available Oracle database and the server it resides on in the Oracle TNSNAMES file.</li> </ul> <pre>ramcmd.exe /oracle:edit /in:&lt;instance name&gt; /rc: [yes no] [/tns:&lt;TNS name&gt;] [/user:&lt;username&gt;] [/password:password *]</pre>
/auth:[on   off] [/user:<username>] [/password:<password>   *]	Enables or disables Backup Exec server authentication for Oracle operations. <ul style="list-style-type: none"> <li>■ /auth:on - Turns the state on. Requires /user parameter.</li> <li>■ /auth:off - Turns the state off. Requires /user parameter.</li> <li>■ /user:&lt;username&gt; - Sets a username.</li> <li>■ /password:&lt;password&gt; - Sets a password to be used with /user:&lt;username&gt;. If you enter an asterisk for the password or omit the password, you are prompted for the password.</li> </ul>

**Table A-5** Backup Exec Agent Utility Command Line Applet switches  
*(continued)*

Switch	Description
/port:[<port>]	<p>Displays or sets a custom port that is used to connect to the Backup Exec server during Oracle operations.</p> <ul style="list-style-type: none"> <li>■ /port - Displays the current port number. If the port is the default port, displays "(default)".</li> <li>■ /port:&lt;port&gt; - Sets the port number to &lt;port&gt;. To change the port to the default port number, type [/port:0].</li> </ul>
/log_path:[<log path>]	<p>Displays or sets a custom path for debug logs.</p> <ul style="list-style-type: none"> <li>■ /log_path - Displays the log directory path and then exits.</li> <li>■ /log_path:&lt;"logs path"&gt; - Creates the directory &lt;"logs path"&gt;. If the path has a space in the name, enclose the path in quotes. For example, "C:\Program files\LogFolder".</li> </ul>

See [“Using the Backup Exec Agent Utility Command Line Applet”](#) on page 747.

# Symantec Backup Exec Deduplication Option

This appendix includes the following topics:

- [About the Deduplication Option](#)
- [Deduplication methods for Backup Exec agents](#)
- [Requirements for the Deduplication Option](#)
- [About installing the Deduplication Option](#)
- [About OpenStorage devices](#)
- [About deduplication disk storage](#)
- [About sharing a deduplication device between multiple Backup Exec servers](#)
- [About direct access sharing of storage devices](#)
- [About client-side deduplication](#)
- [About backup jobs for deduplication](#)
- [About copying deduplicated data between OpenStorage devices or deduplication disk storage devices by using optimized duplication](#)
- [About copying deduplicated data to tapes](#)
- [About using deduplication with encryption](#)
- [About restoring deduplicated data](#)
- [About disaster recovery of a deduplication disk storage device](#)
- [About disaster recovery of OpenStorage devices](#)

## About the Deduplication Option

The Backup Exec Deduplication Option supports a data-reduction strategy by optimizing storage and network bandwidth. The Deduplication Option supports integrated deduplication at the Backup Exec server and on remote computers that have the Agent for Windows or the Agent for Linux installed. It also allows data to be deduplicated and stored on intelligent disk devices from Symantec and other vendors.

**Table B-1** Types of deduplication

Type of deduplication	Where deduplication occurs	Benefits
Backup Exec server-side deduplication	On the Backup Exec server.	Reduces the size of backups, which reduces storage requirements.
Client-side deduplication	On the remote computer where the data is located. <b>Note:</b> The Agent for Windows is required on the remote Windows computer to perform client-side deduplication. The Agent for Linux is required on the Linux computer to perform Linux client-side deduplication.	Reduces network traffic because only unique data is sent across the network. It also reduces the backup window.
Appliance deduplication	On an intelligent disk device, such as Symantec PureDisk or a device from a third-party vendor.	Reduces the size of backups, which reduces storage requirements. It also reduces the backup window.

With a single Deduplication Option license key, you can use two types of deduplication devices.

**Table B-2** Types of deduplication devices that work with the Deduplication Option

Type of device	Description
OpenStorage device	<p>Backup Exec uses Symantec's OpenStorage technology, which allows intelligent disk devices to integrate with Backup Exec. You can back up data to the Symantec PureDisk device and to storage devices from other vendors.</p> <p>You can find a list of compatible types of storage at the following URL:</p> <p><a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a></p> <p>See “About OpenStorage devices” on page 757.</p>
Deduplication disk storage	<p>Deduplication disk storage provides integrated deduplication on the Backup Exec server. Deduplication disk storage is a disk-based backup folder that is located on the Backup Exec server.</p> <p>See “About deduplication disk storage” on page 760.</p>

In addition to reducing storage requirements and network traffic, the Deduplication Option lets you do the following:

- Copy deduplicated data from an OpenStorage device or deduplication disk storage to tape for long-term or off-site storage.
- Use optimized duplication, which lets you copy deduplicated data between OpenStorage devices from the same vendor and between deduplication disk storage devices.
- Use Symantec's Granular Recovery Technology (GRT) with jobs that use deduplication devices.
- Share OpenStorage devices and deduplication storage devices among multiple Backup Exec servers when you use the Central Admin Server Option.

See “About installing the Deduplication Option” on page 757.

See “Requirements for the Deduplication Option” on page 755.

See “About sharing a deduplication device between multiple Backup Exec servers” on page 770.

See [“Copying deduplicated data between deduplication disk storage devices or OpenStorage devices by using optimized duplication”](#) on page 776.

See [“About copying deduplicated data to tapes”](#) on page 778.

## Deduplication methods for Backup Exec agents

Backup Exec supports the following deduplication methods:

- Client-side deduplication, either on an intelligent disk device or to a deduplication disk storage device.
- Backup Exec server-side deduplication with a deduplication disk storage device.
- Appliance deduplication on an OpenStorage device.

The following table lists the deduplication methods that are available for the Backup Exec agents.

**Table B-3** Deduplication methods for Backup Exec agents

Agent	Client-side deduplication (file system/VSS)	Client-side deduplication (with Granular Recovery Technology enabled)	Backup Exec server-side deduplication (file system/VSS)	Backup Exec server-side deduplication (with Granular Recovery Technology enabled)	Appliance deduplication on an OpenStorage device
Agent for Windows	Yes	Not applicable	Yes	Not applicable	Yes
Agent for VMware and Hyper-V	Yes (for Hyper-V only) <b>Note:</b> The Agent for Windows must be installed on the Hyper-V host.	Yes (for Hyper-V only) <b>Note:</b> The Agent for Windows must be installed on the Guest virtual machine.	Yes	Yes	Yes
Agent for Linux	Yes	No	Yes	Not applicable	Yes

**Table B-3** Deduplication methods for Backup Exec agents (*continued*)

Agent	Client-side deduplication (file system/VSS)	Client-side deduplication (with Granular Recovery Technology enabled)	Backup Exec server-side deduplication (file system/VSS)	Backup Exec server-side deduplication (with Granular Recovery Technology enabled)	Appliance deduplication on an OpenStorage device
Agent for Enterprise Vault	Yes	No	Yes	No	No
Exchange Agent	Yes	Yes	Yes	Yes	Yes
SQL Agent	Yes	Not applicable	Yes	Not applicable	Yes
SharePoint Agent	Yes	Yes	Yes	Yes	Yes
Active Directory Agent	Yes	Yes	Yes	Yes	Yes
Agent for Oracle	Linux: Yes Windows: Yes	No	Yes	No	Yes
Agent for Lotus Domino	Yes	No	Yes	No	Yes
Agent for Mac	No	Not applicable	Yes	Not applicable	Yes

See [“About the Deduplication Option”](#) on page 752.

## Requirements for the Deduplication Option

The requirements for the Deduplication Option vary depending on the type of storage devices you want to use and the type of deduplication you want to use. Before you install the Deduplication Option, you should determine what type of storage devices you want to use with it and what type of deduplication you want

to use. Then, verify that your system meets the requirements for the storage devices you want to use.

**Table B-4** Requirements for the Deduplication Option

Item	Requirements
Deduplication disk storage devices	<p>The following items are required:</p> <ul style="list-style-type: none"> <li>■ A 64-bit Backup Exec server.</li> <li>■ A Backup Exec server with either one quad-core processor or two dual-core processors.</li> <li>■ A dedicated volume to use as the location to store the deduplication disk storage. The dedicated volume must have at least 5 GB of free space.</li> <li>■ 8 GB RAM, which supports up to 5 TB of deduplicated data. For more than 5 TB of data, use the following calculation to determine the required amount of RAM: 1.5 GB x <i>N</i>, where <i>N</i> = the number of TBs of deduplicated data to be stored. Up to 32 TB of data is supported.</li> </ul> <p>Example: Use the following equation to calculate the required amount of RAM for 10 TB of data:</p> $1.5 \times 10 = 15 \text{ GB RAM}$
OpenStorage devices	<p>To use a Symantec PureDisk device or a storage device from another vendor as an OpenStorage device, you must purchase the device and the appropriate OpenStorage connector from the device's vendor.</p> <p>You can use the Deduplication Option with OpenStorage devices on either a 32-bit Backup Exec server or a 64-bit Backup Exec server. The standard system requirements for Backup Exec apply to the Deduplication Option when you use OpenStorage devices.</p>
Client-side deduplication for Windows	<p>On the server where the Agent for Windows is installed, 1.5 GB of memory is required.</p>

**Table B-4** Requirements for the Deduplication Option (*continued*)

Item	Requirements
Client-side deduplication for Linux	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"><li>■ Linux kernel Version 2.6 and later</li><li>■ SUSE Version 11 and SP1</li><li>■ Red Hat Version 5.5</li><li>■ Asianux Server 3</li></ul> <p>The following deduplication devices can be used:</p> <ul style="list-style-type: none"><li>■ Deduplication disk storage device</li><li>■ Symantec PureDisk Open Storage device. This is the only supported type of OpenStorage device for Linux.</li></ul> <p>The following Backup Exec options are required:</p> <ul style="list-style-type: none"><li>■ Agent for Linux</li><li>■ Deduplication Option</li></ul>

See “[About installing the Deduplication Option](#)” on page 757.

## About installing the Deduplication Option

The Deduplication Option is installed using the Backup Exec installation media. You install it locally as a separate, add-on component of Backup Exec. Before you attempt to install the Deduplication Option, verify that your system meets the requirements.

See “[Requirements for the Deduplication Option](#)” on page 755.

See “[Installing a custom installation of Backup Exec](#)” on page 70.

## About OpenStorage devices

OpenStorage is a Symantec technology that allows intelligent disk devices to integrate with Backup Exec.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

Some intelligent disk devices can include multiple logical storage units. However, each logical storage unit is added as a single OpenStorage device. When you add an OpenStorage device, Backup Exec can automatically locate the logical storage units on that device.

---

**Note:** When you delete or erase the media from an OpenStorage device, it may take up to 48 hours for more space to become available. Backup Exec cannot always calculate the amount of space that will be made available.

---

OpenStorage devices are added from the **Configure Storage** wizard. After you add an OpenStorage device, it appears on the **Storage** tab. An OpenStorage device cannot belong to any storage pools to prevent a deduplication job from being sent to a non-deduplication device in a storage pool if the OpenStorage device is busy.

If you use Backup Exec Central Admin Server Option, an OpenStorage device can be shared between multiple Backup Exec servers. Sharing can be enabled when you add an OpenStorage device. You can select new Backup Exec servers to share an OpenStorage device or remove the sharing ability for Backup Exec servers at any time.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About sharing a deduplication device between multiple Backup Exec servers”](#) on page 770.

## Editing the properties of an OpenStorage device

You can view all of the properties of an OpenStorage device and you can change some of the properties.

### To edit the properties for an OpenStorage device

- 1 On the **Storage** tab, double-click the name of the OpenStorage device.
- 2 In the left pane, select **Properties**.
- 3 Change the properties as needed.  
See [“OpenStorage device properties”](#) on page 758.
- 4 Click **Apply** to save the changes.

### OpenStorage device properties

You can view all of the properties of an OpenStorage device and you can change some of the properties.

See [“Editing the properties of an OpenStorage device”](#) on page 758.

**Table B-5** General OpenStorage Device Properties

Item	Description
<b>Name</b>	Indicates the user-defined name for this OpenStorage device.
<b>Description</b>	Indicates the user-defined description of this OpenStorage device.
<b>State</b>	Indicates the current state of the device. You cannot change this property.
<b>Host server</b>	Indicates the fully-qualified name of the server on which the device exists.
<b>Server name</b>	Indicates the name of the server on which the device exists.
<b>Server type</b>	Indicates the type of OpenStorage device, such as PureDisk.
<b>Storage location</b>	Indicates the name of the server where the OpenStorage device is located.
<b>Logon account</b>	Indicates the name of the logon account that is required to access the device.
<b>Concurrent operations</b>	Indicates the maximum number of jobs that you want to run at the same time on this device.
<b>Split data stream every</b>	Indicates the size at which you want Backup Exec to span to a new image. The default size is 50 GB.
<b>Data stream size</b>	Indicates the size of a single write operation that Backup Exec issues. The default size varies based on the type of device that is being used.
<b>Stream handler</b>	Indicates whether stream handler is used. Backup Exec sets this option automatically when you select a server type. For some types of devices, this option does not appear at all. If Backup Exec does not set this option, contact the device's vendor for the recommended setting.

**Table B-5** General OpenStorage Device Properties (*continued*)

Item	Description
<b>Client-side deduplication</b>	Indicates whether client-side deduplication is enabled for this OpenStorage device.  Client-side deduplication enables a remote computer to send data directly to an OpenStorage device. By using client-side deduplication, the Backup Exec server is bypassed, which leaves the Backup Exec server free to perform other operations.
<b>Disk space to reserve for non-Backup Exec operations</b>	Displays the amount of disk space to set aside for applications other than Backup Exec. The default amount is 5%.
<b>Total Capacity</b>	Shows the total amount of storage space that is available on this device.
<b>Used Capacity</b>	Shows the total amount of storage space that is being used on this device.
<b>Deduplication Ratio</b>	Indicates the ratio of the amount of data before deduplication to the amount of data after deduplication.
<b>Connection Type</b>	Indicates the type of connection between the Backup Exec server and the OpenStorage device. The connection type is Network for OpenStorage devices.
<b>Backup Exec service restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.

## About deduplication disk storage

Deduplication disk storage provides a disk-based backup folder that you can use as a destination for backup jobs. When you use deduplication disk storage, only unique data is stored.

Before you create a deduplication disk storage device, you should review the requirements. Symantec recommends a dedicated volume and a large amount of RAM for deduplication disk storage.

See [“Requirements for the Deduplication Option”](#) on page 755.

---

**Note:** You can create only one deduplication disk storage device on a Backup Exec server.

---

Deduplication disk storage devices are added from the **Configure Storage** wizard. In the wizard, you can choose to create a new deduplication disk storage device or to import an existing device from a different Backup Exec server. If you choose to import an existing device, you must enter information about the user account that was used to create the device originally on the other Backup Exec server. After you create a deduplication disk storage device, it appears on the **Storage** tab. A deduplication disk storage device cannot belong to any storage pools to prevent a deduplication job from being sent to a non-deduplication device in a storage pool if the deduplication disk storage device is busy.

You can pause, enable, disable, rename, refresh, and delete a deduplication disk storage device. When you use Backup Exec's **Delete** option on a deduplication disk storage device, the folder is removed from the Backup Exec Database. However, the folder and the files in it remain on the disk.

---

**Note:** When you delete backup sets from a deduplication disk storage device, it may take up to 48 hours for more space to become available. Backup Exec cannot always calculate the amount of space that will be made available.

---

If you use Backup Exec Central Admin Server Option, a deduplication disk storage device can be shared between multiple Backup Exec servers. Sharing can be enabled when you add a deduplication disk storage device. You can select new Backup Exec servers to share deduplication disk storage or remove the sharing ability for Backup Exec servers at any time.

Deduplication disk storage can be created on a storage array. However, if a deduplication disk storage device already exists on a Backup Exec server, then another device cannot be added to a storage array that is connected to that Backup Exec server.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About sharing a deduplication device between multiple Backup Exec servers”](#) on page 770.

## Editing the properties of a deduplication disk storage device

You can view all of the properties of a deduplication disk storage device and you can change some of the properties.

### To edit the properties of a deduplication disk storage device

- 1 On the **Storage** tab, double-click the name of the deduplication disk storage device
- 2 In the left pane, select **Properties**.
- 3 Change the properties as needed.  
See “[Deduplication disk storage properties](#)” on page 762.
- 4 Click **Apply** to save the changes

## Deduplication disk storage properties

You can view all of the general properties of a deduplication disk storage device and you can change some of the properties.

See “[Editing the properties of a deduplication disk storage device](#)” on page 761.

**Table B-6** Deduplication disk storage properties

Item	Description
<b>Name</b>	Indicates the name that was entered when the deduplication disk storage was configured. You can change the name at any time.
<b>Description</b>	Indicates the description that was entered when the deduplication disk storage was configured. You can change the description at any time.
<b>State</b>	Indicates the current state of the device. You cannot change this property.
<b>Host server</b>	Indicates the name of the computer on which the deduplication disk storage was created.
<b>Storage path</b>	Indicates the location of the folder on the computer. Symantec strongly recommends that you use a dedicated volume.
<b>Logon account</b>	Indicates the logon account that is being used to access the device.
<b>Encryption</b>	Enables or disables encryption.

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Concurrent operations</b>	Indicates the maximum number of jobs that you want to run at the same time on this device.
<b>Data stream size</b>	Indicates the size of a single write operation that Backup Exec issues. The default size varies based on the type of device being used.
<b>Client-side deduplication</b>	Indicates whether client-side deduplication is enabled for this device.  Client-side deduplication enables a remote computer that is configured to send data directly to the deduplication disk storage. After the data is deduplicated, then only unique data is sent directly to the deduplication disk storage. By using this option, the Backup Exec server is bypassed, which leaves the Backup Exec server free to perform other operations.
<b>Percentage of disk space to reserve for non-Backup Exec operations</b>	Displays the amount of disk space to set aside for applications other than Backup Exec. The default amount is 5%
<b>Log level</b>	Indicates the type of information you want to include in the diagnostic logs for this device. The choices range from critical errors only to all types of messages.
<b>Log retention period</b>	Indicates the number of days to keep the diagnostic logs for this device.

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Low disk space - Critical</b>	<p>Displays the critically low disk space threshold at which you want Backup Exec to send an alert. Backup Exec sends alerts when the amount of free disk space drops below the low disk space threshold, and again if it drops below the warning threshold. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the warning low disk space threshold.</p> <p>You may want to set the threshold slightly higher than the minimum amount that you need to run jobs. By doing so, you allow time to address the disk space issue before the jobs fail.</p> <p>The default is 5%.</p> <p>This property appears only if the deduplication disk storage is on a storage array.</p>

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Low disk space - Warning</b>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the low disk space threshold.</p> <p>You may want to set the threshold slightly higher than the minimum amount that you need to run jobs. By doing so, you allow time to address the disk space issue before the jobs fail.</p> <p>The default is 15%.</p> <p>This property appears only if the deduplication disk storage is on a storage array.</p>

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Low disk space</b>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes.</p> <p>You may want to set the threshold slightly higher than the minimum amount that you need to run jobs. By doing so, you allow time to address the disk space issue before the jobs fail.</p> <p>The default is 25%.</p> <p>This property appears only if the deduplication disk storage is on a storage array.</p>
<b>Total capacity</b>	Shows the total amount of storage space that is available on this device.
<b>Total backup storage</b>	Shows the difference between Total capacity and the amount of disk space that is reserved for non-Backup Exec operations.
<b>Used capacity</b>	Shows the total amount of storage space that is being used on this device.
<b>Amount of data written</b>	Displays the total amount of backup data that is on the storage device.
<b>Available capacity</b>	Displays the difference between Total backup storage and Used capacity.
<b>Deduplication Ratio</b>	Indicates the ratio of the amount of data before deduplication to the amount of data after deduplication.

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Connection type</b>	Indicates the type of connection between the Backup Exec server and the deduplication disk storage device. The connection type is Network for deduplication disk storage devices.
<b>Backup Exec service restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.
<b>Hardware Name</b>	Indicates the name of the virtual disk on which the deduplication folder is located. This property appears only if the deduplication disk storage was added to a storage array with the Storage Array Configuration Wizard.
<b>Hardware Status</b>	Indicates the status of the virtual disk. The values for the hardware status are as follows: <ul style="list-style-type: none"><li>■ <b>OK</b> The virtual disk is online.</li><li>■ <b>Offline</b> The virtual disk is offline. Backup Exec cannot access it.</li><li>■ <b>None</b> The status cannot be obtained.</li></ul> Refer to the vendor documentation and management software that are supplied with the storage array. This property appears only if the deduplication disk storage is on a storage array.

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Hardware Health</b>	<p>Displays one of the following values to indicate the health of the hardware:</p> <ul style="list-style-type: none"><li>■ <b>OK</b> The virtual disk is online.</li><li>■ <b>Warning</b> The virtual disk may fail or produce errors, but it is currently operational. The virtual disk is offline. Backup Exec cannot access it.</li><li>■ <b>Critical</b> The virtual disk has failed. The virtual disk is offline. Backup Exec cannot access it.</li></ul> <p>Refer to the vendor documentation and management software that are supplied with the storage array.</p> <p>This property appears only if the deduplication disk storage is on a storage array.</p>

**Table B-6** Deduplication disk storage properties (*continued*)

Item	Description
<b>Disk Classification</b>	<p>Describes the RAID level for the storage array.</p> <p>Disk classifications are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Simple (RAID 0)</b> A single physical disk, no striping, or parity. No redundancy/</li> <li>■ <b>Span</b> A set of multiple physical disks that are concatenated together. No striping or parity. No redundancy.</li> <li>■ <b>Stripe</b> A set of multiple physical disk extents with data striped across the physical disks. No redundancy.</li> <li>■ <b>Mirror (RAID 1)</b> A pair or multiple pairs of physical disks with the same data written to each physical disk of the pair. Provides for data redundancy/</li> <li>■ <b>Stripe with parity (RAID 5 or RAID 6)</b> Three or more physical disks with data striped across the physical disks, with one disk's worth of space that is used for parity. Provides for data redundancy.</li> <li>■ <b>Unknown</b></li> </ul> <p>This property appears only if the deduplication disk storage is on a storage array.</p>

## Changing the password for the logon account for deduplication disk storage

When you specify a Backup Exec logon account for a deduplication disk storage device, an additional user account is created for the deduplication components with the same user name and password. However, if you change the credentials for the Backup Exec logon account, the credentials for the additional user account are not changed automatically. You must use the `spausers.exe` utility to update the password for the additional user account. This account is known as the "User 1"

account when you use the `spausser.exe` utility to view a list of user names that are associated with the deduplication disk storage.

**To change the password for the logon account for deduplication disk storage**

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Logon Accounts**, and then select **Manage Logon Accounts**.
- 3 Select the Backup Exec logon account that you want to change, and then click **Edit**.
- 4 Type the current password for the logon account, and then click **OK**.
- 5 Click **Change Password**.
- 6 Type the new password in the **Password** field and in the **Confirm** field.
- 7 Click **OK**.
- 8 At a command prompt, switch to the Backup Exec program file directory, and then type the following command:

```
spausser.exe -c -u <UserName>
```

The default Backup Exec program file directory is `C:\Program Files\Symantec\Backup Exec`

The user name is case-sensitive. If you do not know the user name, type the following command to find the user name that is associated with "User 1":

```
spausser.exe -l
```

You will be prompted for the old password and a new password. Be sure that the new password is the same as the password that you used in step 6.

See [“About deduplication disk storage”](#) on page 760.

## About sharing a deduplication device between multiple Backup Exec servers

If you use the Backup Exec Central Admin Server Option, you can select which Backup Exec servers can share a deduplication disk storage device or an OpenStorage device. When you add a deduplication disk storage device or an OpenStorage device, the Backup Exec server that you used to add the device is automatically selected for sharing.

---

**Note:** To share a deduplication disk storage device, you must add it as an OpenStorage device on all Backup Exec servers that you want to access the device, except for the Backup Exec server that was used to create it.

---

This type of sharing is not the same as direct access sharing. With direct access sharing, a remote computer bypasses the Backup Exec server to directly access storage devices that are hosted by the Backup Exec server.

See [“Sharing a storage device”](#) on page 419.

See [“About direct access sharing of storage devices”](#) on page 771.

## About direct access sharing of storage devices

Direct access enables a remote computer to send data directly to storage devices that are hosted by a Backup Exec server. When direct access sharing is enabled, the Backup Exec server is bypassed.

If you use a deduplication disk storage device or an OpenStorage device that supports client-side deduplication, then enabling direct access sharing enables Backup Exec to perform client-side deduplication. Note that client-side deduplication is CPU-intensive.

Direct access sharing becomes available after you create a backup job in which a deduplication device is selected and the following option is selected: **Enable the remote computer to directly access the storage device and to perform client-side deduplication, if it is supported.**

After the correctly configured backup job is created, then the option **Direct access sharing** appears in the following locations.

- On the details screen for a server on the **Backup and Restore** tab.
- On the details screen for a storage device on the **Storage** tab.

In addition, the option **Direct access properties** appears on the details screen for a server on the **Backup and Restore** tab.

See [“Selecting storage devices for direct access sharing”](#) on page 771.

See [“Editing the properties for direct access”](#) on page 772.

## Selecting storage devices for direct access sharing

Direct access enables a remote computer to send data directly to storage devices that are hosted by a Backup Exec server.

### To select storage devices for direct access sharing

- 1 Do one of the following:
  - On the **Backup and Restore** tab, double-click the server that you want to set up to share devices.

- On the **Storage** tab, double-click the storage device that you want to share.
- 2 In the left pane, select **Direct access sharing**.
  - 3 Select the check box for the items that you want to share.

## Editing the properties for direct access

For servers that are enabled for direct access, you can do the following:

- Add or change a description of the server.
- Enable or disable ICMP ping operations to detect the server.
- Add or edit a logon account that is used to access the remote computer.

### To edit the properties for direct access

- 1 On the **Backup and Restore** tab, double-click the server that is enabled for direct access.
- 2 In the left pane, select **Direct access properties**.
- 3 Edit the options as needed.

See “[Direct access properties](#)” on page 772.

## Direct access properties

The following properties appear for direct access sharing.

See “[Editing the properties for direct access](#)” on page 772.

**Table B-7** Direct access properties

Item	Description
<b>Server name</b>	Indicates the name of the remote computer or managed Backup Exec server.
<b>Description</b>	Lets you enter a description of the server.
<b>State</b>	Indicates the state of the server, such as online or offline.
<b>Port</b>	Indicates that port that is used for communications between the Backup Exec server and the remote computer.
<b>Use ICMP ping operations to detect the server</b>	Lets the Backup Exec server use ICMP ping to locate the remote computer.

**Table B-7** Direct access properties (*continued*)

Item	Description
<b>Logon account</b>	Indicates the logon account that is required to access the remote computer. You can add a new logon account or edit an existing account.
<b>Host ID</b>	Indicates the unique identifier for the storage device.
<b>System version</b>	Lists the details about the operating system that is installed on the remote computer.

## About client-side deduplication

Client-side deduplication enables a remote computer to send data directly to an OpenStorage device or a deduplication disk storage device. By using client-side deduplication, the Backup Exec server is bypassed, which leaves the Backup Exec server free to perform other operations. If your deduplication device supports client-side deduplication, a remote computer deduplicates data and then sends only the unique data directly to a deduplication disk storage device or an OpenStorage device. Client-side deduplication is available for Windows computers and Linux computers.

---

**Note:** Client-side deduplication may increase the CPU utilization on the remote computer if your deduplication device supports client-side deduplication.

---

When you create a backup job with client-side deduplication, keep in mind the following items:

- The backup job can include resources from only one remote computer.
- The Agent for Windows is required on the remote Windows computer to perform Windows client-side deduplication. The Agent for Linux is required on the Linux computer to perform Linux client-side deduplication.
- The remote computer must be pingable.
- The remote computer cannot be a Backup Exec server.
- A deduplication disk storage device or an OpenStorage device must be used for the backup job.
- The option **Client-side deduplication** must be enabled on the properties for the storage device.

- The option **Enable the remote computer to directly access the storage device and to perform client-side deduplication, if it is supported** must be selected in the **Storage** options for the backup job. This option is selected by default when you select a deduplication disk storage device or an OpenStorage device as the storage for a backup job.

If you do not configure the remote computer to use client-side deduplication, then the data from the remote computer is sent to the Backup Exec server to be deduplicated. Then, the deduplicated data is backed up to the deduplication disk storage or the OpenStorage device. This process increases the CPU utilization on the Backup Exec server. However, this process is useful if you are backing up older remote computers.

See [“About the Deduplication Option”](#) on page 752.

See [“About backup jobs for deduplication”](#) on page 774.

See [“Editing the properties of an OpenStorage device”](#) on page 758.

See [“Editing the properties of a deduplication disk storage device”](#) on page 761.

## About backup jobs for deduplication

You set up a backup job for deduplication by selecting the option **Back Up to Deduplication Disk Storage**. Then, on the **Storage** settings, you must select either an OpenStorage device or a deduplication disk storage device as the destination device, and then you must select the deduplication method to use.

The following deduplication methods are available:

- If you want to enable client-side deduplication, you should select the option **Enable the remote computer to directly access the storage device and to perform client-side deduplication, if it is supported**. This is the default option. If the storage device that you select for the job does not support client-side deduplication, then either Backup Exec server-side deduplication or appliance deduplication is used.
- If you want to enable Backup Exec server-side deduplication, you should select the option **Enable the remote computer to access the storage device through the Backup Exec server and to perform Backup Exec server-side deduplication, if it is supported**. If the storage device that you select for the job does not support server-side deduplication, then appliance deduplication is used.

See [“About client-side deduplication”](#) on page 773.

## About copying deduplicated data between OpenStorage devices or deduplication disk storage devices by using optimized duplication

Backup Exec supports optimized duplication, which enables deduplicated data to be copied directly from one OpenStorage device to another OpenStorage device from the same vendor. Both devices must be attached to a single Backup Exec server. For example, you can copy data from one Symantec PureDisk device to another Symantec PureDisk device. Because the data is deduplicated, only unique data is copied between the devices.

To copy data between OpenStorage devices or deduplication disk storage devices, you must create a job to duplicate backup sets. The destination device for the duplicate job must be the same type of device from the same vendor as the device that was used in the source backup job. No additional settings are required; optimized duplication occurs automatically when you set up a duplicate backup job between appropriate devices. You can restore data from either device.

Optimized duplication can be performed on backup sets that were enabled for Granular Recovery Technology (GRT). However, only deduplication disk storage devices and PureDisk devices support optimized duplication for GRT-enabled backup sets.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

---

**Note:** The OpenStorage devices must be from the same vendor. You cannot perform optimized duplication between OpenStorage devices from different vendors. If you attempt to copy deduplicated data between OpenStorage devices from different vendors, regular duplication is performed instead of optimized duplication.

---

If you use the Central Admin Server Option (CASO), the functionality of optimized duplication is expanded to let you do the following:

- Copy data from a deduplication disk storage device on one Backup Exec server to a deduplication disk storage device on another Backup Exec server.
- Copy data from an OpenStorage device that is attached to a Backup Exec server to another OpenStorage device that is attached to a different Backup Exec server.

To use optimized duplication with CASO, the following requirements must be met:

- You must have a license for the Enterprise Server Option. CASO is installed as part of the Enterprise Server Option.
- All Backup Exec servers that you use with CASO as either a central administration server or as managed Backup Exec servers must use the 64-bit version of Windows.
- You must have a central administration server and at least one managed Backup Exec server in your CASO environment.
- For client deduplication and Backup Exec server-side deduplication, you must configure one deduplication disk storage on the Backup Exec server from which you want to copy the deduplicated data. You must also configure one deduplication disk storage on the Backup Exec server to which you want to copy the deduplicated data.
- For appliance deduplication, the Backup Exec server from which you want to copy deduplicated data must have the appropriate plug-in for the OpenStorage device and a properly configured OpenStorage device. In addition, the Backup Exec server to which you want to copy the deduplication data must have the appropriate plug-in for the OpenStorage device and a properly configured OpenStorage device.
- You must share deduplication devices between the Backup Exec servers.
- You must inventory and catalog the media on the destination server before you recover any files from the duplicated backup set. You must do this regardless of how the catalog sharing option is configured for CASO.

See [“Copying deduplicated data between deduplication disk storage devices or OpenStorage devices by using optimized duplication”](#) on page 776.

See [“About sharing a deduplication device between multiple Backup Exec servers”](#) on page 770.

## Copying deduplicated data between deduplication disk storage devices or OpenStorage devices by using optimized duplication

Optimized duplication enables deduplicated data to be copied directly from one OpenStorage device to another OpenStorage device from the same vendor. Both devices must be attached to a single Backup Exec server. If you have the Central Admin Server Option (CASO) installed, you can also copy data from one OpenStorage device on a Backup Exec server to a different OpenStorage device on a different Backup Exec server. With CASO, you can also copy deduplicated data from one deduplication disk storage device on a Backup Exec server to another deduplication disk storage device on a different Backup Exec server.

You set up a duplicate backup job to perform optimized duplication.

**Table B-8** How to set up optimized duplication

Step	For more information
<p>If you are using CASO, do the following:</p> <ul style="list-style-type: none"> <li>■ Verify that you have one central administration server and at least one managed Backup Exec server.</li> <li>■ Verify that the Backup Exec server from which you want to copy the deduplicated data has a deduplication disk storage device (for client or Backup Exec server-side deduplication) or an OpenStorage device (for appliance deduplication). Also verify that the Backup Exec server to which you want to copy the deduplicated data has a deduplication disk storage device (for client or Backup Exec server-side deduplication) or an OpenStorage device (for appliance deduplication).</li> <li>■ Verify that the Backup Exec servers are enabled for sharing.</li> </ul> <p><b>Note:</b> This information applies only to CASO. If you do not have CASO, skip this step.</p>	<p>See <a href="#">“About OpenStorage devices”</a> on page 757.</p> <p>See <a href="#">“About deduplication disk storage”</a> on page 760.</p>
<p>Create a backup job that uses an OpenStorage device or a deduplication disk storage device as the destination.</p>	<p>See <a href="#">“Backing up data”</a> on page 163.</p>
<p>Create a job to duplicate backup sets and select the appropriate OpenStorage device or deduplication disk storage as the destination.</p> <p><b>Note:</b> The destination device for the duplicate job must be the same type of device from the same vendor as the device that was used in the source backup job.</p>	<p>See <a href="#">“Duplicating backup sets”</a> on page 219.</p>

See [“About copying deduplicated data between OpenStorage devices or deduplication disk storage devices by using optimized duplication”](#) on page 775.

## About copying deduplicated data to tapes

Backup Exec lets you copy deduplicated data from an OpenStorage device to tape for long-term or off-site storage. When data is copied to tape, it is rehydrated. In other words, the files are reassembled into their original form and are not deduplicated.

To copy deduplicated data to tapes, you must create a duplicate backup job that copies the backup sets from the OpenStorage device to a tape device.

See [“Duplicating backup sets”](#) on page 219.

## About using deduplication with encryption

You should not use the Backup Exec encryption options for backup jobs that deduplicate data. Data cannot be deduplicated when the Backup Exec encryption options are used.

If you want deduplicated data to be encrypted on a deduplication disk storage device, you can enable the encryption property on the deduplication disk storage device.

See [“About encryption key management”](#) on page 477.

## About restoring deduplicated data

You set up a restore job to restore deduplicated data in the same way as you set up a regular restore job. No additional settings are required.

See [“About disaster recovery of a deduplication disk storage device”](#) on page 778.

See [“About disaster recovery of OpenStorage devices”](#) on page 780.

## About disaster recovery of a deduplication disk storage device

A deduplication disk storage device is stored on the Backup Exec server. If your Backup Exec server experiences a disaster, then the data from the deduplication disk storage device is lost. Therefore, you should take steps to prepare for recovery from a system failure. To prepare for a disaster, Backup Exec lets you take a snapshot of a deduplication disk storage device. The snapshot includes the folder and the contents of the folder. You can store the snapshot on tape, which you can then use to recover your deduplication disk storage after you recover the Backup Exec server.

When you restore data from the snapshot, the following processes occur:

- Backup Exec stops the deduplication services if they are running. The deduplication services are separate from the Backup Exec services, so the Backup Exec services are not affected.
- Backup Exec deletes any files that are present in the deduplication disk storage.
- The deduplication disk storage is restored to its original location, along with the contents of the folder.
- The deduplication services are restarted.

---

**Note:** If you use Backup Exec Simplified Disaster Recovery (SDR) to recover the Backup Exec server, SDR does not recover the deduplication disk storage during the recovery of the Backup Exec server.

---

You can recover the deduplication disk storage by running the Restore Wizard and selecting **Shadow Copy Components**. When you restore a deduplication disk storage device, the original folder is deleted and then replaced by the restored folder.

---

**Note:** You cannot redirect the restore of a deduplication disk storage device. A deduplication disk storage device must be restored to its original location.

---

See [“Preparing for disaster recovery of a deduplication disk storage device”](#) on page 779.

## Preparing for disaster recovery of a deduplication disk storage device

To prepare for a disaster, Backup Exec lets you take a snapshot of a deduplication disk storage device. The snapshot includes the folder and the contents of the folder. You can store the snapshot on tape, which you can then use to recover your deduplication disk storage after a disaster.

See [“About disaster recovery of a deduplication disk storage device”](#) on page 778.

### To prepare for disaster recovery of a deduplication disk storage device

- 1 On the **Backup and Restore** tab, right-click the server where the deduplication disk storage device is located.
- 2 Select **Backup**, and then select **Backup to Tape**.
- 3 In the **Selections** box, click **Edit**.

- 4 Expand **Shadow Copy Components**, expand **User Data**, and then select **Backup Exec Deduplication Storage**.
- 5 Click **OK**.
- 6 Complete any additional options that you want to use.  
Symantec recommends that you schedule this job to run just prior to the 12:20 a.m. and 12:20 p.m. deduplication maintenance times.
- 7 Click **OK** to create the job.

## About disaster recovery of OpenStorage devices

The following disaster recovery scenarios are possible for OpenStorage devices:

- The device fails.
- The Backup Exec server that uses the device fails.

If the device fails, you should consult the documentation from the device's vendor. If the Backup Exec server fails and you need to reinstall Backup Exec on the Backup Exec server, you must reconfigure the device, and inventory and catalog the media from it after the Backup Exec server is recovered.

See [“About disaster recovery of a deduplication disk storage device”](#) on page 778.

# Symantec Backup Exec Agent for VMware

This appendix includes the following topics:

- [About the Agent for VMware](#)
- [Requirements for using the Agent for VMware](#)
- [About installing the Agent for VMware](#)
- [About adding VMware vCenter and ESX servers](#)
- [About backing up VMware data](#)
- [About protecting databases and applications with the Symantec VSS Provider](#)
- [About restoring VMware resources](#)

## About the Agent for VMware

The Symantec Backup Exec Agent for VMware Virtual Infrastructure (Agent for VMware) lets you back up and restore virtual machines that use the following VMware products:

- ESX Server
- vCenter Server (formerly VirtualCenter)
- vSphere 4.0, 4.1, and 5.0

Backup Exec performs a single-pass backup to protect all Guest virtual machines and VSS-aware applications that are installed on the Guest virtual machines. Backup Exec's Granular Recovery Technology (GRT) is enabled by default for backup jobs. You can use a GRT-enabled backup to restore individual files and

folders from a Windows Guest virtual machine without restoring the entire virtual machine. In addition, you can restore individual items from Microsoft Exchange, SQL, SharePoint, and Active Directory applications that reside on Guest virtual machines.

Additional features of the Agent for VMware let you do the following:

- Redirect the restore of data from a Guest virtual machine to an alternate folder, datastore, host, or network.
- Back up to a disk device or to a tape device.
- Perform incremental and differential backup jobs (If your virtual machines are configured with hardware version 7 or later).

See [“Requirements for using the Agent for VMware”](#) on page 782.

See [“How Backup Exec backs up Microsoft application data on virtual machines”](#) on page 788.

See [“About backing up VMware data”](#) on page 783.

See [“About restoring VMware resources”](#) on page 791.

## Requirements for using the Agent for VMware

The Agent for VMware uses the following components, which can reside on the same computer or on separate computers:

**Table C-1** Agent for VMware components

Item	Description
Backup Exec server	This component runs the backup and restore jobs. You must enter a license for the Agent for Hyper-V and VMware on this component.
VMware vCenter Server	This component is optional. It manages the ESX servers. You do not have to install the Backup Exec Agent for Windows on this computer. If the Agent for Windows is installed, it is used only to publish the vCenter Server to the Backup Exec server.

To use Backup Exec's Granular Recovery Technology (GRT) for Microsoft application data, install the Agent for Windows on any virtual machines that run Windows.

See [“How Backup Exec backs up Microsoft application data on virtual machines”](#) on page 788.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

You can find a list of compatible devices at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

## About installing the Agent for VMware

The Agent for VMware is installed as part of the Agent for Hyper-V and VMware. You do not have to install the agent on the ESX host.

See “[Installing additional Backup Exec options to the local Backup Exec server](#)” on page 75.

## About adding VMware vCenter and ESX servers

You can add VMware vCenter and ESX servers to the list of servers on the **Backup and Restore** tab so that these servers can be selected for backup jobs. When you select the **Add VMware Server** option in the **Servers** group on the **Backup and Restore** tab, the **Add Server** wizard appears. The **Add Server** wizard guides you through the setup of the VMware server.

An option to add VMware servers is also available when you select the **Add** option in the **Servers** group on the **Backup and Restore** tab.

See “[Adding servers to the list of servers](#)” on page 158.

## About backing up VMware data

When you create a backup job, you can select an entire vCenter or ESX server, datacenters, and folders, or individual virtual machines. Additionally, Backup Exec can automatically back up new virtual machines and folders that are found when a backup job runs. If you select the vCenter or ESX server for a backup job, all virtual machines are backed up. However, a backup of a vCenter or ESX server does not include independent disks, or configuration files for the vCenter or ESX server.

---

**Warning:** Backup jobs fail for virtual machines that have Physical Raw Disk Mapping (RDM) devices.

---

Virtual compatibility mode RDM disks are automatically included in the backup of a Guest virtual machine. However, Backup Exec can only restore the virtual compatibility mode RDM disks or file data on an RDM disk through redirected restore.

---

**Note:** You cannot back up databases to devices that are attached to a computer on which the Remote Media Agent for Linux Servers is installed.

---

The following backup methods are supported for VMware resources:

**Table C-2** Supported backup methods for VMware resources

Backup method	Description
Full	<p>This method is available for both VMware vCenter Server and VMware vSphere.</p> <p>Backup Exec's Granular Recovery Technology (GRT) lets you use the full image backup to restore individual files for virtual machines that use the Windows operating system. GRT also lets you restore individual items from VSS-aware applications that are installed on the virtual machines.</p> <p>See <a href="#">“How Backup Exec backs up Microsoft application data on virtual machines”</a> on page 788.</p>
Incremental or Differential	<p>This method is available only if the virtual machine is configured with hardware version 7 or later.</p>

See [“How Backup Exec automatically backs up new virtual machines during a backup job”](#) on page 788.

## Setting default backup options for virtual machines

You can use the defaults that Backup Exec sets during installation for all VMware backup jobs, or you can choose your own defaults. You can also set backup options for individual jobs.

### To set default backup options for virtual machines

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Backup Job Defaults**, and then select a backup option.

- 3 In the left pane, select **Virtual Machines**.
- 4 Select the appropriate options.  
See “[Virtual machine backup options](#)” on page 785.
- 5 Click **OK**.

## Virtual machine backup options

The following options are available for VMware backup jobs. These options appear when the **Virtual Machines** option is selected on the **Backup Job Defaults** dialog box and on the **Options** dialog box for a backup job.

See “[Setting default backup options for virtual machines](#)” on page 784.

**Table C-3** Virtual machine backup options

Item	Description
<b>Use the full backup method for virtual machines that do not support incremental or differential backups</b>	Lets Backup Exec perform a full backup if an incremental backup or a differential backup cannot be performed. If you do not select this option and Backup Exec cannot perform an incremental backup or a differential backup, then the job fails. In addition, if Backup Exec detects a configuration change, then a full backup must be performed. If a configuration change is detected and Backup Exec cannot perform a full backup, then the job fails if this option is not selected. This scenario applies only if a full backup and some incremental or differential backups have already been performed and the next scheduled job is for an incremental or a differential backup.
<b>Back up virtual machines that are powered off</b>	Enables Backup Exec to back up virtual machines that are turned off.
<b>Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual files and folders from virtual machines</b>	<p>Enables individual files and folders to be restored from the backup. This option is for virtual machines that use a Windows operating system only.</p> <p>The vmdk file is not backed up if the virtual hard disk is configured as an Independent disk.</p> <p><b>Note:</b> GRT is not meant for system recovery but only for the restore of individual files and folders on Windows computers.</p>

**Table C-3** Virtual machine backup options (*continued*)

<b>Item</b>	<b>Description</b>
<b>Enable GRT for Microsoft Active Directory objects on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual Active Directory objects on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Microsoft Active Directory is installed.
<b>Enable GRT for Microsoft Exchange databases and mailbox items on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual Exchange databases and mailbox items on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Microsoft Exchange is installed.
<b>Enable GRT for Microsoft SQL (database-level only) on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual SQL database items on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Microsoft SQL is installed.
<b>Enable GRT for Microsoft SharePoint on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual SharePoint items on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Microsoft SharePoint is installed.
<b>Exclude virtual machines that must be put into a saved state for backup</b>	This option applies only to the Agent for Hyper-V.

**Table C-3** Virtual machine backup options (*continued*)

Item	Description
<b>Transport mode priority list</b>	<p>Lets you select the method to transport the Virtual Machine Disk Format (vmdk) file from the ESX server. You must select at least one of these options. If you select more than one option, the method is determined by the priority and the resources that are available. You can move the options up or down in the list to change the priority.</p> <p>The following methods are available:</p> <ul style="list-style-type: none"> <li>■ <b>SAN - Use the SAN to move virtual disk data</b> If you select this option, the virtual machine must reside on a SAN that the Backup Exec server can access. With this transport mode, the data is offloaded to the Backup Exec server so that the ESX server is not affected.</li> <li>■ <b>NBD - Do not encrypt the virtual disk data for over-the-network transfers</b> Use this option if you do not use SSL for security and one of the following conditions exist: <ul style="list-style-type: none"> <li>■ The virtual machine is not located on the SAN.</li> <li>■ The Backup Exec server does not have access to the SAN.</li> </ul> </li> <li>■ <b>NBDSSL - Encrypt virtual disk data for over-the-network transfers</b> Use this option if you use SSL for security and one of the following conditions exist: <ul style="list-style-type: none"> <li>■ The virtual machine is not located on the SAN.</li> <li>■ The Backup Exec server does not have access to the SAN.</li> </ul> </li> <li>■ <b>Hotadd - Use virtual disk files from the Backup Exec server on the virtual machine</b> Use this option if you want to use the hotadd feature for ESX. See your VMware documentation for more information about hotadd .</li> </ul> <p>The vmdk file is not backed up if the virtual hard disk is configured as an Independent disk.</p>
<b>vSphere Port Number</b>	Indicates the port that Backup Exec uses to connect to vCenter Server. The default port is 902.

## How Backup Exec automatically backs up new virtual machines during a backup job

Backup Exec's dynamic inclusion feature protects new virtual machines and folders that are found when a backup job runs. If new virtual machines are added between the time when the backup job is created and when the backup job runs, Backup Exec automatically backs up the new virtual machines. Because the backup job may include new virtual machines, the job may require more storage space and more time to run than you anticipated. The job history shows the number of virtual machines that were backed up.

In the backup selections, dynamic inclusion is enabled for the following VMware resources:

- ESX
- vCenter 4
- All nodes that have a folder icon

If you select ESX or vCenter 4, then dynamic inclusion is enabled automatically for all of the nodes below them that have a folder icon. If no virtual machines are located during a backup job, then the job fails.

See [“About backing up VMware data”](#) on page 783.

## How Backup Exec backs up Microsoft application data on virtual machines

Backup Exec's Granular Recovery Technology (GRT) lets you restore individual drives, files, and folders without having to restore the entire virtual machine. It also lets you restore individual items from the following VSS-aware applications that reside on virtual machines:

**Table C-4** Types of data that Backup Exec backs up for VSS-aware applications on virtual machines

Application	Types of data that Backup Exec backs up
Microsoft Exchange	Mailboxes, individual messages, calendar items, tasks, journal entries, and public folder data (disk-backups only)
Microsoft SQL	Databases
Microsoft Active Directory	Individual user accounts, printer objects, sites, and organizational units

**Table C-4** Types of data that Backup Exec backs up for VSS-aware applications on virtual machines (*continued*)

Application	Types of data that Backup Exec backs up
Microsoft SharePoint	SharePoint data

GRT works only for the virtual machines that use a Windows operating system. GRT does not work for system recovery. You should review the requirements for a GRT-enabled backup before you configure it.

See [“Requirements for backing up Microsoft application data on virtual machines”](#) on page 789.

When you create a backup job, Backup Exec automatically locates VSS-aware applications on virtual machines. During the backup job, Backup Exec backs up the data from the VSS-aware applications by using Granular Recovery Technology (GRT). By default, Backup Exec enables GRT using the same credentials that were used to connect to the virtual machine. You can disable GRT for any of the VSS-aware application types.

---

**Note:** Backup Exec supports the granular recovery of individual Exchange and SQL items only in non-clustered and non-distributed configurations.

---

See [“Virtual machine backup options”](#) on page 785.

During the backup job, Backup Exec collects metadata from the applications. If Backup Exec is unable to collect the metadata, then you cannot restore individual items for the applications. However, the backup job may otherwise complete successfully.

## Requirements for backing up Microsoft application data on virtual machines

Backup Exec can back up and restore individual items from VSS-aware applications that are installed on virtual machines.

The following items are required to back up data for Microsoft Exchange, SQL, SharePoint, and Active Directory on virtual machines:

- The virtual machine must be turned on.
- You must enter the appropriate credentials for the virtual machine. Ensure that the credentials for the virtual machine allow access to the VSS-aware applications.

- The Backup Exec server must be able to connect to the virtual machine using the network name or IP address.
- The Backup Exec Agent for Windows must be installed on the virtual machine.
- The correct number of licenses must be entered for the applications that you want to protect on the virtual machines.
- The operating system on the virtual machine must support VSS.

If you want to use Backup Exec's Granular Recovery Technology (GRT), you must purchase and install the Agent for Applications and Databases on your virtual machines.

See [“How Backup Exec backs up Microsoft application data on virtual machines”](#) on page 788.

## About protecting databases and applications with the Symantec VSS Provider

The Symantec VSS Provider helps Backup Exec protect VSS-aware applications, such as Microsoft Exchange, SQL, SharePoint, and Active Directory. The Symantec VSS Provider provides an automatic snapshot of the Windows applications and databases for each backup job.

Some of your Guest virtual machines may already have the VMware VSS Provider. However, only one VSS Provider can be used on a Guest virtual machine. Therefore, you must uninstall the VMware VSS Provider.

---

**Warning:** Having more than one VSS provider installed on a Guest virtual machine can cause quiesce and other snapshot errors. For example, the virtual machine may time out during a backup job. Verify that your Guest virtual machines have only one VSS provider.

---

When you install the Agent for Windows on a Guest virtual machine, the Symantec VSS Provider is installed automatically. You can also install it manually from the Backup Exec installation media.

---

**Warning:** Do not reinstall the VMware VSS Provider on a Guest virtual machine after you install the Agent for Windows.

---

See [“Push-installing the Agent for Windows to remote computers”](#) on page 86.

By default, the Symantec VSS Provider quiesces the operating system application writers using the full backup option. Each application responds differently to this request. In the case of Microsoft Exchange, the database logs are truncated. However, you can change the default setting by modifying the script files.

See [“Changing the log truncation setting of the Symantec VSS Provider”](#) on page 791.

## Changing the log truncation setting of the Symantec VSS Provider

By default the Symantec VSS Provider takes full backups and truncates database log files. You can change the settings to enable the Symantec VSS Provider to take copy backups without log truncation.

---

**Note:** You must add the `-copy` flag to the `Pre-freeze-script.bat` file in both the system root directory and `%Programfiles%\Symantec\Backup Exec\RAWS\VSS Provider`.

---

### To change the log truncation setting of the Symantec VSS Provider

- 1 Locate the `Pre-freeze-script.bat` file in both of the following locations:
  - Your system root directory
  - `%Programfiles%\Symantec\Backup Exec\RAWS\VSS Provider`
- 2 Add the `-copy` flag to the end of each of the three lines that include `BeVssRequestor.exe`.

For example:

```
"%Programfiles%\Symantec\Backup Exec\BE VSS  
Provider\BeVssRequestor.exe" -pre2 -log -logscreen -copy
```

## About restoring VMware resources

You can use the Restore Wizard to do the following:

- Restore VMware data to the original location or to redirect the data to a different location.
- Turn on virtual machines after the restore job completes.
- Restore over an existing virtual machine.
- Restore with a new virtual machine name in vCenter Server.

- Select the preferred network for virtual machines to use after the restore job completes.

You can restore a complete virtual machine, or its Virtual Machine Disk Format (vmdk) file, for disaster recovery purposes.

---

**Note:** To restore virtual machines that were backed up with Backup Exec 12.5, the VMware Converter (4.01 or later) must be installed on the Backup Exec server.

---

If you selected the Granular Recovery Technology (GRT) option for the backup job, you can restore individual files or folders that were backed up from inside the vmdk file.

---

**Note:** Granular Recovery Technology (GRT) allows the restore of individual data files and folders. GRT cannot restore system state files such as the active registry.

---

See [“About searching for and restoring data”](#) on page 229.

See [“VMware restore options”](#) on page 792.

See [“VMware restore redirection options”](#) on page 794.

## VMware restore options

The following options appear when you use the Restore Wizard to restore VMware data.

See [“About searching for and restoring data”](#) on page 229.

Table C-5 VMware restore job options

Item	Description
<b>Transport mode priority list</b>	<p>Lets you select the method to transport the Virtual Machine Disk Format (vmdk) file from the ESX server. You must select at least one of these options. If you select more than one option, the method is determined by the priority and the resources that are available. You can move the options up or down in the list to change the priority.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li> <p>■ <b>SAN-Use the SAN to move virtual disk data</b></p> <p>If you select this option, the virtual machine must reside on a SAN that the Backup Exec server can access. With this transport mode, the data is offloaded to the Backup Exec server so that the ESX server is not affected.</p> </li> <li> <p>■ <b>NBD-Do not encrypt the virtual disk data for over-the-network transfers</b></p> <p>Use this option if you do not use SSL for security and one of the following conditions exist:</p> <ul style="list-style-type: none"> <li>■ The virtual machine is not located on the SAN.</li> <li>■ The Backup Exec server does not have access to the SAN.</li> </ul> </li> <li> <p>■ <b>NBDSSL-Encrypt virtual disk data for over-the-network transfers</b></p> <p>Use this option if you use SSL for security and one of the following conditions exist:</p> <ul style="list-style-type: none"> <li>■ The virtual machine is not located on the SAN.</li> <li>■ The Backup Exec server does not have access to the SAN.</li> </ul> </li> <li> <p>■ <b>Hotadd-Use virtual disk files from the Backup Exec server on the virtual machine</b></p> <p>Use this option if you want to use the hotadd feature for ESX. The hotadd feature lets you use a virtual machine as your proxy server.</p> <p>See your VMware documentation for more information about hotadd .</p> </li> </ul> <p>The vmdk file is not backed up if the virtual hard disk is configured as an Independent disk.</p>

**Table C-5** VMware restore job options (*continued*)

Item	Description
<b>Delete existing virtual machines prior to restore</b>	Deletes existing virtual machines during the restore job. If you select this option, the virtual machines may be deleted even if the restore job fails.  You cannot restore a virtual machine if it already exists on the virtual server unless you select this option.
<b>Power on virtual machine after restore</b>	Turns on a virtual machine after the restore job completes.
<b>vSphere port number</b>	Indicates the port that Backup Exec uses to connect to vCenter Server. The default port is 902.

## VMware restore redirection options

The following options appear when you select the option to restore data to a different vCenter or ESX server in the Restore Wizard.

See [“About searching for and restoring data”](#) on page 229.

**Table C-6** VMware Redirection options

Item	Description
<b>vCenter and ESX Servers</b>	Indicates the name of the vCenter or ESX server to which you want to redirect data.
<b>Browse</b>	Lets you select the virtual server on which you want to redirect data. You can use this option instead of typing the name of the server.
<b>Server logon account</b>	Uses the default logon account that appears. You can select another logon account to use for the vCenter or ESX server to which you want to redirect data.
<b>Datacenter</b>	Displays the name of the datacenter, or group of ESX servers.
<b>Virtual machine datastore or datastore cluster</b>	Displays the name of the storage location on the ESX server that is used to store the data.

Table C-6 VMware Redirection options (continued)

Item	Description
<b>Host or cluster</b>	Displays the name of the ESX server that will run the virtual machine after the restore job completes.
<b>Virtual machine folder</b>	Indicates the name of the existing vSphere folder to which you want to restore.
<b>Resource pool</b>	Indicates the name of the resource pool to which you want to restore.
<b>Virtual machine name</b>	Indicates the new virtual machine name. You may want to provide a new virtual machine name if a virtual machine with the same name already exists on the server.
<b>Network</b>	Indicates the network for the virtual machine to use after the restore job completes.
<b>Use the original disk datastore selections if available on the selected host</b>	Uses the original datastore selections on the virtual server. If the original datastore selections do not exist, then the datastore selections from the backup data are used.
<b>Restore virtual machine to the most recent hardware version that the destination environment supports</b>	Restores the virtual machine with VMware hardware version 7 or later. Selecting this option causes jobs to fail when you restore to VMware ESX Server version 3.5.
<b>Restore virtual clients with thin provisioning</b>	Restores the virtual machine with thin provisioning. Thin provisioning can help you more efficiently dedicate storage capacity in your VMware ESX Server version 4.0 environment. Selecting this option causes jobs to fail when you restore to VMware ESX Server version 3.5.



# Symantec Backup Exec Agent for Microsoft Hyper-V

This appendix includes the following topics:

- [About the Agent for Microsoft Hyper-V](#)
- [Requirements for using the Agent for Microsoft Hyper-V](#)
- [About installing the Agent for Microsoft Hyper-V](#)
- [About upgrading from the Agent for Microsoft Virtual Servers](#)
- [About backing up Microsoft Hyper-V virtual machines](#)
- [About restoring Microsoft Hyper-V virtual machines](#)
- [About backing up and restoring highly available Hyper-V virtual machines](#)
- [How Backup Exec protects Microsoft application data on virtual machines](#)

## About the Agent for Microsoft Hyper-V

The Symantec Backup Exec Agent for Microsoft Hyper-V (Agent for Microsoft Hyper-V) lets you back up and restore the following resources:

- Microsoft Windows Server 2008/2008 R2 Hyper-V hosts.
- All virtual machines that reside on the Hyper-V hosts.
- Clustered Hyper-V hosts, including virtual machines that reside on cluster shared volumes (CSV).

Backup Exec performs a single-pass backup to protect the host configuration data, all virtual machines, and VSS-aware applications that are installed on the virtual machines. Backup Exec's Granular Recovery Technology (GRT) is enabled by

default for backup jobs. You can use a GRT-enabled backup to restore individual files and folders from a Windows virtual machine without restoring the entire virtual machine. In addition, you can restore individual items from Microsoft Exchange, SharePoint, and Active Directory applications that reside on virtual machines. You can also restore individual databases from Microsoft SQL when it resides on virtual machines.

---

**Note:** You must have the appropriate Backup Exec agent for Microsoft Exchange, SQL, or Active Directory on the virtual machine to perform GRT.

---

Backup Exec can back up virtual machines that are online or that are in an offline state or a saved state. Virtual machines that use Microsoft Windows 2003 (with Hyper-V Integration Services) or later can be backed up while they are online. You can include both online and offline virtual machines in the same backup job. During the backup of an online virtual machine, Backup Exec takes a snapshot backup of the Hyper-V host. The host in turn takes a snapshot of the virtual machines on the host. This process enables Backup Exec to back up virtual servers without any downtime. If an online backup cannot be performed, then an offline backup is performed. With an offline backup, the virtual machine is placed briefly in a saved state. However, the virtual machine does not remain in the saved state for the entire backup job.

The amount of downtime for a saved state backup job depends on the following:

- The amount of memory that is allocated to the virtual machine.
- The current load on the host's operating system.

See “[Requirements for using the Agent for Microsoft Hyper-V](#)” on page 798.

See “[About backing up Microsoft Hyper-V virtual machines](#)” on page 800.

See “[About restoring Microsoft Hyper-V virtual machines](#)” on page 805.

## Requirements for using the Agent for Microsoft Hyper-V

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

You can find a list of compatible devices at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

The following items are required to use the Agent for Microsoft Hyper-V:

**Table D-1** Requirements for the Agent for Microsoft Hyper-V

Software	Installed on
Microsoft Windows Server 2008 Hyper-V	Microsoft Hyper-V host
Backup Exec	Backup Exec server
Agent for Microsoft Hyper-V	Microsoft Hyper-V host
VHDMount	Backup Exec server (if the Backup Exec server is not the virtual server). <b>Note:</b> VHDmount is required only if the Backup Exec server runs Microsoft Windows 2003 or Windows 2008 without the Hyper-V role installed. You can install the VHDmount component from Microsoft Virtual Server 2005 R2 SP1.

To run an online backup, the following requirements must be met:

- Microsoft Windows Server 2008/2003 SP2/Vista SP1/XP SP3 is installed on the virtual machine.
- Hyper-V Integration Services with Backup (Volume snapshot) is installed.
- The virtual machine is in a running state.

If these conditions are not met, the virtual machine is placed in a saved state if it is running. If the virtual machine is turned off, then that virtual machine is backed up only if you select the option **Back up virtual machines that are powered off**.

To enable Backup Exec to collect catalog data for Microsoft Exchange, SharePoint, Active Directory, and SQL on the virtual machine, the following items are required on the virtual machine:

- A licensed version of the Backup Exec agent for the application.
- The Agent for Windows.  
The Agent for Microsoft Hyper-V includes a license for the Agent for Windows. The agents for Microsoft Exchange, Active Directory, and SQL also include a license for the Agent for Windows. No separate license is required for the Agent for Windows.
- The virtual machine must be capable of being backed up online.
- The credentials that you use to access the virtual machine must also have access to the application.

The Agent for Windows must be installed on the virtual machine to do the following:

- Enable individual files and folders to be restored back to the original virtual machine.
- Enable individual SQL databases, Exchange items, SharePoint items, and Active Directory objects to be restored back to the original virtual machine.

See “[About the Agent for Microsoft Hyper-V](#)” on page 797.

## About installing the Agent for Microsoft Hyper-V

The Symantec Backup Exec Agent for Microsoft Hyper-V is installed as part of the Agent for VMware and Hyper-V. The Agent for Microsoft Hyper-V is installed on the Microsoft Hyper-V host. If your Backup Exec server is also your Microsoft Hyper-V host, you can install the Agent for Microsoft Hyper-V when you install Backup Exec. Or, you can install it after Backup Exec has been installed.

If Backup Exec is not installed on your Microsoft Hyper-V host, you must push-install the Agent for Windows to your Microsoft Hyper-V host. You do not need to install the Agent for Microsoft Hyper-V on virtual machines. However, a license is required on the Backup Exec server for the Agent for Microsoft Hyper-V. The Agent for Windows is included with the Agent for Microsoft Hyper-V.

See “[Installing additional Backup Exec options to the local Backup Exec server](#)” on page 75.

See “[Push-installing the Agent for Windows to remote computers](#)” on page 86.

## About upgrading from the Agent for Microsoft Virtual Servers

If you set up recurring jobs with Backup Exec 12, you must either recreate the job or change the selection list to use Microsoft virtual servers.

Backup Exec is not intended to be a tool to migrate from Microsoft Virtual Server to Microsoft Hyper-V. For information about how to migrate, see Microsoft's virtual machine migration guide.

[http://technet.microsoft.com/en-us/library/dd296684\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd296684(WS.10).aspx)

## About backing up Microsoft Hyper-V virtual machines

When you create a backup job for Microsoft Hyper-V, options for Granular Recovery Technology (GRT) are available. GRT enables individual files and folders to be restored. GRT is enabled by default for individual files and folders on virtual machines and for individual items from VSS-aware applications that reside on

virtual machines. VSS-aware applications include Microsoft Exchange, SQL, SharePoint, and Active Directory. By default, Backup Exec uses the resource credentials of the parent virtual machine.

---

**Note:** Virtual machines that have remote .vhd files are excluded from the backup job. You can use the Agent for Windows and the appropriate Backup Exec agent to protect virtual machines that have remote .vhd files.

---

The following backup selections are available for Microsoft Hyper-V:

**Table D-2** Microsoft Hyper-V backup selections

Container name	Items in the container	What is included in the backup job
<b>Microsoft Hyper-V</b>	This item includes <b>Initial Store</b> and <b>Virtual Machines</b> .	If you select the <b>Microsoft Hyper-V</b> container for backup, the backup job includes the application configuration settings and all virtual machines.
<b>Initial Store</b>	This item includes the virtual server application configuration settings.	If you select <b>Initial Store</b> for backup, the backup job includes a single XML file that contains the Hyper-V authorization configuration.
<b>Virtual Machines</b>	This item includes each virtual machine that resides on the virtual server.  <b>Note:</b> When you select an individual virtual machine, the files that are on that virtual machine appear in the results pane. However, you cannot select individual files to include in or exclude from the backup.	If you select an individual virtual machine, the backup is a full image backup of the entire virtual machine, which includes the following items: <ul style="list-style-type: none"> <li>■ .vhd files</li> <li>■ .avhd files</li> <li>■ Differencing disks</li> <li>■ Hyper-V managed snapshots</li> </ul> <b>Note:</b> Virtual machines that have remote .vhd files are excluded from the backup job. You can use the Agent for Windows and the appropriate Backup Exec agent to protect virtual machines that have remote .vhd files.  <b>Warning:</b> Backup jobs fail for virtual machines that have pass thru disks. You can use the Agent for Windows and the appropriate Backup Exec agent to protect virtual machines that have pass thru disks.

You can set backup job default options for all Hyper-V backup jobs. Each time you create a backup job, the job uses the default options. However, you can change the default options for individual jobs.

See [“Backing up data”](#) on page 163.

See [“Microsoft Hyper-V backup options”](#) on page 802.

## Microsoft Hyper-V backup options

The following options are available for Hyper-V backup jobs. These options appear when you select the **Virtual Machines** option on the **Backup Job Defaults** dialog box and on the **Option** dialog box for a backup job.

See [“About backing up Microsoft Hyper-V virtual machines”](#) on page 800.

**Table D-3** Microsoft Hyper-V backup options

Item	Description
<b>Use the full backup method for virtual machines that do not support incremental or differential backups</b>	Enables Backup Exec to run a full backup job if an incremental backup or a differential backup of the guest virtual machine cannot be performed. Backup Exec may not be able to perform an incremental backup or a differential backup for a number of reasons, such as if the snapshot configuration is altered or the configuration of the host server changed. If this option is not selected and an incremental backup or a differential backup cannot be performed, the job fails.
<b>Back up virtual machines that are powered off</b>	Enables Backup Exec to back up virtual machines when they are not powered on.
<b>Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual files and folders from Virtual Machines</b>	Enables individual files and folders to be restored from the full backup.  You must install the Agent for Windows on the virtual machine on which you want to restore the data. The Agent for Windows does not have to be installed on the virtual machine to back up the data.

**Table D-3** Microsoft Hyper-V backup options (*continued*)

Item	Description
<b>Enable GRT for Microsoft Active Directory objects on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual Active Directory objects on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Active Directory is installed.
<b>Enable GRT for Microsoft Exchange databases and mailbox items on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual Exchange databases and mailbox items on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which Exchange is installed.
<b>Enable GRT for Microsoft SQL (database-level only) on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore individual SQL database items on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which SQL is installed.
<b>Enable GRT for Microsoft SharePoint on virtual machines</b>	Enables Backup Exec to collect the information that is required to restore SharePoint data on the virtual machine. Backup Exec uses the logon credentials that were used for the virtual machine on which SharePoint is installed.
<b>Exclude virtual machines that must be put in a saved state to back up</b>	Excludes from the backup all offline virtual machines that do not support online backups and that are in a running state when the backup begins.
<b>Transport mode priority list</b>	Applies only to virtual machines in a VMware environment. This option is not applicable to Hyper-V.
<b>vSphere Port Number</b>	Applies only to virtual machines in a VMware environment. This option is not applicable to Hyper-V.

See [“How Granular Recovery Technology works with the Agent for Microsoft Hyper-V”](#) on page 804.

## How Granular Recovery Technology works with the Agent for Microsoft Hyper-V

Backup Exec Granular Recovery Technology (GRT) lets you restore individual files and folders without having to restore the entire virtual machine. It also lets you restore individual items from VSS-aware applications that are installed on virtual machines.

GRT is not intended to be used for system recovery. However, you can perform a complete system recovery by selecting the entire virtual machine as a restore selection in a restore job.

See [“How Backup Exec protects Microsoft application data on virtual machines”](#) on page 806.

You should review the requirements for a GRT-enabled backup before you configure it.

See [“Requirements for protecting Microsoft application data on virtual machines”](#) on page 807.

To use GRT, you must select the individual files and folders that you want to restore from the list that appears when you expand the Netbios name or the computer name of the virtual machine. You cannot select individual folders and files from the virtual machines that appear when you expand the **Virtual Machines** node.

See [“About restoring Microsoft Hyper-V virtual machines”](#) on page 805.

## How Backup Exec automatically protects new virtual machines during a backup job

Backup Exec's dynamic inclusion feature protects new virtual machines and folders that are found when a backup job runs. If new virtual machines are added between the time when the backup job is created and when the backup job runs, Backup Exec automatically backs up the new virtual machines. Because the backup job may include new virtual machines, the job may require more storage space and more time to run than you anticipated. The job history shows the number of virtual machines that were backed up.

In the backup selection list, dynamic inclusion is enabled for the following Hyper-V nodes:

- Microsoft Hyper-V
- Virtual Machines under Microsoft Hyper-V
- The Hyper-V host node

If you select the host node, then dynamic inclusion is enabled automatically for the Microsoft Hyper-V node.

- Microsoft Hyper-V HA Virtual Machines
  - The cluster name node
- If you select the cluster name node, then dynamic inclusion is enabled automatically for the Microsoft Hyper-V HA Virtual Machines node.

## About restoring Microsoft Hyper-V virtual machines

You can use the Restore Wizard to restore data from virtual machines in the following ways:

- Restore a complete virtual machine for disaster recovery purposes.
- Restore individual files or folders that were backed up from the virtual machine (if you selected the Granular Recovery Technology (GRT) option for the backup job).
- Restore a virtual machine to a different Microsoft Hyper-V server.
- Redirect flat files from the virtual machine to any computer that has an Agent for Windows installed.

---

**Note:** Linux virtual machines must be restored in their entirety at the .vhd level.

---

See [“About searching for and restoring data”](#) on page 229.

## About backing up and restoring highly available Hyper-V virtual machines

When virtual machines are configured for high availability, they appear in the **Highly Available Hyper-V Machines** node in the backup selection tree. Virtual machines that are not configured for high availability remain in the **Microsoft Hyper-V** node. When you make a backup selection, Backup Exec checks for highly available virtual machines. If highly available virtual machines are discovered, Backup Exec reminds you to select those virtual machines for backup.

The restore selections are similar to the backup selections. You can restore a highly available virtual machine in the same way you restore any other virtual machine. The virtual machine maintains its high availability. However, if you redirect the restore to another Hyper-V host, then the virtual machine is no longer

highly available when the restore job completes. You must reconfigure the virtual machine to be highly available.

## How Backup Exec protects Microsoft application data on virtual machines

Backup Exec can restore individual items from the following VSS-aware applications that reside on virtual machines:

**Table D-4** Types of data that Backup Exec protects for VSS-aware applications on virtual machines

Application	Types of data that Backup Exec protects
Microsoft Exchange	Mailboxes, individual messages, calendar items, tasks, journal entries, and public folder data (disk-backups only)
Microsoft SQL	Databases
Microsoft Active Directory	Individual user accounts, printer objects, sites, and organizational units
Microsoft SharePoint	SharePoint databases

When you create a backup job, Backup Exec automatically locates VSS-aware applications on virtual machines. During the backup job, Backup Exec backs up the data from the VSS-aware applications by using Granular Recovery Technology (GRT). By default, Backup Exec enables GRT using the same credentials that were used to connect to the virtual machine. You can disable GRT for any of the VSS-aware application types.

---

**Note:** Backup Exec supports the granular recovery of individual Exchange and SQL items only in non-clustered and non-distributed configurations.

---

During the backup job, Backup Exec collects metadata for the applications. If Backup Exec is unable to collect the metadata, then you cannot restore individual items for the applications. However, the backup job may otherwise complete successfully.

Backup Exec cannot collect metadata in the following situations:

- GRT is disabled for an application.
- Backup Exec cannot connect to the virtual machine.

- Incorrect credentials were entered for the virtual machine.

---

**Note:** Backup Exec uses the Microsoft Hyper-V writer during backups of VSS-aware applications on virtual machines. The Microsoft Hyper-V writer truncates application logs before data is moved to the storage device. Therefore, the application logs for the applications on the virtual machines are truncated if you use Microsoft Hyper-V.

---

See [“Requirements for protecting Microsoft application data on virtual machines”](#) on page 807.

## Requirements for protecting Microsoft application data on virtual machines

Backup Exec can back up and restore individual items from VSS-aware applications that are installed on virtual machines.

The following items are required to protect data for Microsoft Exchange, SQL, Active Directory, and SharePoint on virtual machines:

- The virtual machine must be turned on.
- You must enter the appropriate credentials for the virtual machine. Ensure that the credentials for the virtual machine allow access to the VSS-aware applications.
- The Backup Exec server must be able to connect to the virtual machine using the network name or IP address.
- The Backup Exec Agent for Windows must be installed on the virtual machine.
- The correct number of licenses must be entered for the applications that you want to protect on the virtual machines.
- The operating system on the virtual machine must support VSS.

See [“How Backup Exec protects Microsoft application data on virtual machines”](#) on page 806.



# Symantec Backup Exec Agent for Microsoft SQL Server

This appendix includes the following topics:

- [About the Agent for Microsoft SQL Server](#)
- [Requirements for using the SQL Agent](#)
- [About installing the SQL Agent](#)
- [How to use Backup Exec logon accounts for SQL databases](#)
- [About backup strategies for SQL](#)
- [About consistency checks for SQL](#)
- [How to use snapshot technology with the SQL Agent](#)
- [About backing up SQL databases](#)
- [About SQL 2005 or later database snapshots](#)
- [About restoring SQL databases](#)
- [About disaster recovery of a SQL Server](#)

## About the Agent for Microsoft SQL Server

The Agent for Microsoft SQL Server (SQL Agent) enables network administrators to perform backup and restore operations on installations of SQL that are

connected to a network. SQL database backups can be integrated with network backups without separate administration or dedicated hardware.

The SQL Agent provides support for the following:

- Database, transaction log, and differential backups, as well as database recovery and replacement.
- An automated restore of the system databases.
- Simplified Disaster Recovery, which automates the disaster recovery process of SQL Servers.
- Restores of SQL databases to alternate locations.
- Hot backup copies of SQL databases during backup operations. This feature enables you to direct a copy of the actual data streams being sent to media by a SQL database to a local directory for later use.
- Backups of multiple instances.
- Standby database. If the primary SQL Server fails, or is shut down for maintenance, another database called a standby database can be brought online.
- Database Consistency Checks (DBCC) for each backup and restore job, including a fast database consistency check of only the physical consistency of the database.
- Full, bulk-logged, and simple recovery models. With the simple recovery model, copies of the transactions are not stored in the log file, which prevents transaction log backups from being run. Therefore, you can recover the database to the point of the last backup, but you cannot restore the database to the point of failure or to a specific point in time.
- Restores of transaction logs to a specific point in time or to a named transaction when log marks are used.

In SQL 2005 or later installations, the SQL Agent provides support for the following:

- Database snapshots.
- Copy backup jobs, which enables you to copy a SQL 2005 or later database without impacting the full-differential-log restore sequence.
- Maintaining replication settings during redirected restores.
- Verify only restore jobs, which enable you to determine both the validity of the SQL data on the media and the ability of the destination SQL database to accept this data before the database is deleted or overwritten during a restore job.

- Back up with checksum generation. Used as a redundancy check, this option works with the Verify Only Restore Job option.
- Continuation of restore jobs when errors are detected. This feature enables you to restore as much data as possible from a corrupt database backup.

In SQL Server 2008 Enterprise Edition installations, the SQL Agent provides support for the following:

- In SQL Server 2008 or later editions that support compression, you can use SQL software compression for backup jobs.

See [“About installing the SQL Agent”](#) on page 811.

## Requirements for using the SQL Agent

The following are required for the SQL Agent:

- Backup Exec must have access rights to read both of the following SQL registry keys:

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Microsoft SQL Server

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\mssqlserver

If Backup Exec does not have access to these registry keys, a restore to the default directory may not work, and the Automate system database restore option on the Restore Job Properties for SQL dialog box will not work.

To ensure that Backup Exec has access rights, verify that the logon account used has administrator rights to the Windows server that the SQL instance is installed on.

- The Backup Exec server must have access to the SQL installation.
- The credentials stored in the Backup Exec logon account used for backing up and restoring SQL must have been granted the System Administrator role on the SQL instance.
- The Agent for Windows must be installed on any remote SQL Server that you want to back up.

## About installing the SQL Agent

The SQL Agent is installed as part of the Agent for Applications and Databases and can protect local or remote SQL Server databases.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

## How to use Backup Exec logon accounts for SQL databases

To back up SQL, use a Backup Exec logon account that stores the credentials of a Windows user account. The Windows user account must have been granted the System Administrator role on the SQL instance. In the **Test/edit credentials** dialog, apply that logon account to the Windows server that SQL is installed on, not to the actual SQL instance.

If you are using SQL Server Authentication, then add a Backup Exec logon account that stores the credentials of the SQL user account. In the **Test/edit credentials** dialog, apply the Backup Exec logon account for the Windows user account to the Windows server that SQL is installed on, and then apply the logon account for the SQL user account to the SQL instance.

If you use a Backup Exec logon account that does not have the proper rights, you will receive an error message stating that the username and password are invalid.

See [“About logon accounts”](#) on page 498.

See [“Creating a new Backup Exec System Logon Account”](#) on page 505.

## About backup strategies for SQL

Backup Exec incorporates online, nondisruptive SQL database protection as part of everyday backup routines, which increases the chance of data recovery and minimizes data loss without inhibiting daily database activity. Using database, differential, and log backups provides a good balance between backup windows and minimizes the amount of time that will be spent recovering a database if the need arises.

To decide which backup methods to use for the best data protection, consider the following for typical environments:

- In small environments, consider running a daily full database backup every evening and daily transaction log backups.
- In mid-sized environments, consider running a weekly full database backup and daily transaction log backups along with daily differential backups except on the day when the full backup is run.
- In large environments, consider running daily differential database backups, weekly full database backups, and transaction log backups as necessary. Many shops run full backups on a weekly basis, preferring to run differential backups throughout the week to keep backup run time to a minimum.

The trade-off with running fewer full backups and running more differential backups occurs at recovery time when you must recover using the full database backup as well as the last differential database backup, and all log backups made after the last differential database backup.

What will work best for you will be based on the size of your environment, the number of transactions processed each day, and the expectations of your users when a recovery is required.

See “[SQL backup strategy recommendations](#)” on page 813.

## SQL backup strategy recommendations

When you develop a SQL backup strategy, consider the following:

**Table E-1** Recommendations for backing up SQL

SQL Server backup strategies	Description
Protect the entire SQL Server	<p>To ensure SQL is completely protected, back up the following on a regular basis:</p> <ul style="list-style-type: none"> <li>■ The system drive that SQL is on.</li> <li>■ The Windows registry and System State.</li> <li>■ Transaction logs.</li> </ul>
When you upgrade, run new full database backups.	If you upgrade SQL, run new full database backups. You may not be able to restore backups from one version or service pack level of SQL to other versions.
Run consistency checks before backups.	Symantec recommends that you run a consistency check before a backup. If a database or transaction log contains errors when it is backed up, the backup will still contain the errors when it is restored, if it is restorable at all.
Back up your system databases regularly.	<p>Back up the master database and services packs that are installed whenever procedures are run that change information in the database, especially after the following:</p> <ul style="list-style-type: none"> <li>■ New databases are created.</li> <li>■ Files are added to an existing database.</li> <li>■ Usernames or passwords are added or changed.</li> </ul> <p>If changes are not backed up before the master database must be restored, the changes are lost.</p>

**Table E-1** Recommendations for backing up SQL (*continued*)

SQL Server backup strategies	Description
Run one backup at a time.	Do not schedule more than one backup to occur simultaneously against a database or its transaction log.
Back up transaction logs on databases that are configured for the full recovery model.	Back up the transaction logs on databases because the transaction logs continue to grow if you do not back them up.

See [“About backup strategies for SQL”](#) on page 812.

## About consistency checks for SQL

If you back up a database or transaction log that contains errors, these errors will still exist when the backup is restored. In some cases, this can prevent a successful restore. Backup Exec enables you to check the logical and physical consistency of the data before and after a backup. SQL reports any consistency check failures in the Backup Exec job log. Symantec strongly recommends that you always run a consistency check either before the backup.

Backup Exec’s consistency check uses the following SQL consistency check utilities:

- CHECKDB
- CHECKCATALOG
- PHYSICAL\_ONLY

CHECKDB, CHECKCATALOG, and PHYSICAL\_ONLY are performed for database-related operations.

For more information concerning these utilities, see your MS SQL documentation.

See [“About backing up SQL databases”](#) on page 815.

## How to use snapshot technology with the SQL Agent

The SQL Agent supports full snapshot backups using Microsoft’s Volume Shadow Copy Service (VSS), a snapshot provider service only available on Windows 2003 or later. The use of snapshot technology can reduce both restore time and backup performance on the server.

When a backup job is submitted that uses snapshot technology, a snapshot of each volume is created, providing a point-in-time record of the data. Backup Exec uses snapshot technology to momentarily suspend write activity to a volume so that a snapshot of the volume can be created. The data is then backed up from the snapshots, and then the snapshots are deleted.

See [“About SQL 2005 or later database snapshots”](#) on page 824.

Before you use snapshot technology with the SQL Agent, review the following information:

- With snapshot technology, a point-in-time view of the SQL database is “snapped” and then backed up, leaving the actual SQL database open and available for users.
- SQL backups that use snapshot technology are considerably larger than regular SQL backups.
- Performing consistency checks before backup is strongly recommended. See [“About consistency checks for SQL”](#) on page 814.
- The SQL Agent only supports full snapshot backups; transaction log snapshots and differential snapshots are not supported.
- With the SQL Agent, snapshot and traditional backups are interoperable when you restore SQL data.
- Performing database consistency checks both before and after backups affects the time required for the backup jobs.
- Use snapshot technology with jobs that use deduplication devices.

The following SQL backup options are not supported with snapshot backups:

- **Use checksums on backup (SQL 2005 or later).**  
This option is used as a redundancy check, and works with the **Run verify only and do not restore data** restore option.
- **SQL Server 2008 Enterprise Edition software compression.**
- **Create on-disk copies of SQL backups to be placed on the SQL Server where the database is located.**

See [“SQL backup options”](#) on page 817.

## About backing up SQL databases

Backup Exec includes three methods for backing up databases: Full, Differential, and for SQL 2005 or later, Full Copy-only. The full method backs up the entire database including all system tables. The differential method backs up only the

changes made to the database since the last full backup. The copy method works in the same manner as the full method, except that it does not affect future differential or log backups.

A differential backup is smaller and faster than a full backup, so differential backups can be run more often than full backups. Because differential backups allow the restore of a system only to the point that the differential backup was created, you should also create multiple log backups between the differential backups. Using transaction log backups allows you to recover the database to the exact point of failure.

Consider using differential backups when only a relatively small amount of data changes between full backups, or if the same data changes often. Differential backups may also work well in your environment if you are using the simple recovery model and need backups more often, but cannot spare the time to do frequent full backups. If you are using the full or bulk-logged recovery models, you can use differential backups to decrease the time it takes to roll forward log backups when restoring a database.

If you want to run database backups only, instead of a mix of database and log backups, use the simple recovery model for the database so that the transaction log is automatically truncated when a checkpoint occurs in the database. This helps prevent transaction logs from becoming full since with other recovery models the logs are not cleared after a database backup.

With the simple recovery model, copies of the transactions are not stored in the log file, which prevents transaction log backups from being run.

If you do not run transaction log backups, you can recover the database to the point of the last backup, but you cannot restore the database to the point of failure or to a specific point in time.

System databases can only be backed up with the full method; you cannot use the log or differential methods to back up the master database.

---

**Note:** You cannot back up databases to storage that is attached to a computer on which the Remote Media Agent for Linux Servers is installed.

---

The SQL Agent supports a mirrored SQL database configuration, although Microsoft places limitations on the mirroring of SQL databases.

These limitations include the following:

- You cannot back up or restore a mirrored SQL database. If you attempt to back up or restore a mirrored database, the backup job or restore job fails.

- You cannot restore the primary SQL database while it is configured in a mirrored configuration. To restore the primary SQL database, you must stop database mirroring of the primary database.
- You can back up a primary SQL database and its transaction logs only if the backup job does not leave the database in a non-recovered state.

To back up a SQL database, add the database to the list of servers on the **Backup and Restore** tab. You can set backup job default options for all SQL backup jobs. Each time you create a backup job, the job uses the default options unless you change the options for that particular job.

See [“About the list of servers”](#) on page 157.

See [“Backing up data”](#) on page 163.

See [“SQL backup options”](#) on page 817.

See [“About stages”](#) on page 183.

See [“Editing backups”](#) on page 170.

See [“Editing backups”](#) on page 170.

See [“Setting default backup job settings”](#) on page 456.

## SQL backup options

The following options are available for SQL backup jobs.

These options appear when you select the SQL option for the following:

- The **Backup Job Defaults** dialog box.
- The **Backup Options** dialog box for a backup job.
- The **One-Time Backup Options** dialog box for a one time backup job.

See [“About backing up SQL databases”](#) on page 815.

See [“Setting default backup job settings”](#) on page 456.

See [“Backing up data”](#) on page 163.

See [“Creating a one-time backup”](#) on page 164.

**Table E-2** SQL backup options

Item	Description
<b>Consistency check before backup</b>	<p>Specifies one of the following consistency checks to run before a backup:</p> <ul style="list-style-type: none"> <li>■ None. This option does not run a consistency check before a backup. Symantec recommends that you always run a consistency check either before the backup.</li> <li>■ Full check, excluding indexes. This option excludes indexes from the consistency check. If indexes are not checked, the consistency check runs significantly faster but is not as thorough.</li> <li>■ Full check, including indexes. This option includes indexes in the consistency check. Any errors are logged.</li> <li>■ Physical check only. This option performs a low overhead check of the physical consistency of the database. This option only checks the integrity of the physical structure of the page. This option is selected by default.</li> </ul> <p>See <a href="#">“About consistency checks for SQL”</a> on page 814.</p>
<b>Continue with backup if consistency check fails</b>	<p>Continues with the backup operation even if the consistency check fails. You may want to continue with the backup when the consistency check fails if you think that a backup of the database in its current state is better than no backup at all, or if you are backing up a very large database with only a small problem in a table.</p>

Table E-2 SQL backup options (*continued*)

Item	Description
<b>Consistency check after backup</b>	<p>Specifies the consistency check to run after a backup. Because database transactions can occur during or after the consistency check, but before the backup runs, consider running a consistency check after the backup to ensure that the data was consistent at the time of the backup.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>■ None. This option does not run a consistency check after a backup. Symantec recommends that you always run a consistency check after the backup. This option is selected by default.</li> <li>■ Full check, excluding indexes. This option excludes indexes from the consistency check. If indexes are not checked, the consistency check runs significantly faster but is not as thorough.</li> <li>■ Full check, including indexes. This option includes indexes in the consistency check. Any errors are logged.</li> <li>■ Physical check only. This option performs a low overhead check of the physical consistency of the database. This option only checks the integrity of the physical structure of the page. This option is selected by default.</li> </ul>
<b>Use checksums on backup (SQL 2005 or later)</b>	<p>Adds the checksums to the SQL database data being backed up by Backup Exec. Adding checksums to the data being backed up is required if you want to use the restore option <b>Run verify only and do not restore data</b>. Using this option, and the <b>Run verify only and do not restore data</b> option, ensures that during a restore of the SQL database, you restore from a verified SQL backup.</p>
<b>Create on-disk copies of SQL backups to be placed on the SQL Server where the database is located</b>	<p>Creates an on-disk copy of the SQL database being backed up. This option lets you simultaneously back up a SQL database to storage media while also writing a copy of the database to a disk path you specify in the Save to path box.</p> <p>This option gives IT administrators the ability to back up SQL databases while also providing database administrators with copies of the database on disk, which can be used for such things as tests and restores.</p> <p><b>Note:</b> This option does not support snapshot technology.</p>
<b>Save to path</b>	<p>Displays a path in which to save on-disk copies of SQL backups.</p>

**Table E-2** SQL backup options (*continued*)

Item	Description
<p><b>SQL Server 2008 Enterprise Edition software compression</b></p>	<p>Specifies the following compression setting you want to use for this backup job:</p> <ul style="list-style-type: none"> <li>■ None. Do not use compression.</li> <li>■ Compress. Use SQL Server 2008 or later compression if it is supported by the SQL Server instance that is installed.</li> </ul> <p>SQL compresses the data on the computer on which SQL Server 2008 Enterprise Edition or later is installed. Therefore, faster SQL 2008 or later backups should occur if you use SQL compression.</p> <p>If you back up remote SQL 2008 or later computers and you use SQL 2008 or later software compression, you must use the latest version of the Agent for Windows.</p> <p>You can find a list of compatible operating systems, platforms, and applications at the following URL:</p> <p><a href="http://entsupport.symantec.com/umi/V-269-1">http://entsupport.symantec.com/umi/V-269-1</a></p> <p>Symantec recommends that you do not use SQL 2008 or later software compression in a backup job that uses Backup Exec-initiated software compression. Minimal additional SQL 2008 or later compression benefits are gained when you enable Backup Exec compression. In fact, in jobs where both compression schemes are used, backup times may increase.</p> <p>SQL 2008 or later software compression is not used if a backup job that includes SQL 2008 or later data uses Advanced Open File options.</p> <p><b>Note:</b> You cannot use this option for backup jobs that deduplicate data.</p>

Table E-2 SQL backup options (*continued*)

Item	Description
<b>Incremental backup method</b>	<p>Specifies one of the following methods for incremental backups:</p> <ul style="list-style-type: none"><li data-bbox="581 369 1245 487">■ Log This option backs up only the data contained in the transaction log; it does not back up database data. After the transaction log is backed up, committed transactions are removed (truncated).</li><li data-bbox="581 491 1245 668">■ Differential This option backs up only the changes that are made to the database since the last full backup. Because differential backups allows the restore of a system only to the point in time that the differential backup was created, you should also create multiple log backups between the differential backups.</li></ul> <p><b>Note:</b> To back up SQL databases using a combination of log and differential backup methods, you must create two incremental backup jobs. For the first incremental backup job, select the Log option. For the second incremental backup job, select the Differential option.</p>

**Table E-2** SQL backup options (*continued*)

Item	Description
<p><b>One-time backup method</b></p>	<p>Specifies one of the following methods for one-time backups:</p> <ul style="list-style-type: none"> <li> <p>■ <b>Full - Back up entire database</b>            This option backs up the entire database. This option is selected by default.            See <a href="#">“About backing up SQL databases”</a> on page 815.</p> </li> <li> <p>■ <b>Full Copy-only (SQL 2005 or later) - Back up entire database</b>            This option backs up the entire database without affecting future differential or log backups.            Unlike the Full backup method, the Full Copy-only backup method does not reset the SQL differential baseline that is used to indicate the database blocks that have changed since the last full backup. After making a full backup, you can use the Full Copy-only backup method to make a copy of a SQL database without affecting the baseline backup set required to run future differential backups.</p> </li> <li> <p>■ <b>Database Snapshot (SQL 2005 Enterprise Edition or later) - Read-only, point-in-time copy of another database</b>            This option creates a read only, point-in-time copy of another database.            See <a href="#">“About SQL 2005 or later database snapshots”</a> on page 824.</p> </li> <li> <p>■ <b>Log No Truncate - Back up transaction log - no truncate</b>            This option backs up the database when it is corrupt or database files are missing. Since the Log No Truncate method does not access the database, you can still back up transactions that you may not be able to access otherwise when the database is in this state. You can then use this transaction log backup along with the database backup and any previous transaction log backups to restore the database to the point at which it failed; however, any uncommitted transactions are rolled back. The Log No Truncate method does not remove committed transactions after the log is backed up.</p> </li> <li> <p>■ <b>Log</b>            This option backs up only the data contained in the transaction log; it does not back up database data. After the transaction log is backed up, committed transactions are removed (truncated).            If the databases are configured for the SQL Server simple recovery model, log backups are not supported. To change the recovery model, use the SQL administration tools to set the recovery model to Full. You should run a new full backup if you change the recovery mode before a log backup is run.            Alternatively, you can run full backups only, or run full and differential backups of the SQL databases.            See <a href="#">“About consistency checks for SQL”</a> on page 814.</p> </li> </ul>

## About automatic exclusion of SQL data during volume level backup

If you select a volume that contains SQL data for backup, the SQL Agent determines which SQL data should not be included in a volume level backup. For example, .MDF and .LDF files should not be part of the backup because they are opened for exclusive use by the SQL system. These files will be automatically excluded for backup by a feature called Active File Exclusion. If this exclusion did not happen during a non-snapshot backup, these files would appear as in use - skipped. If this exclusion did not happen during a snapshot backup, the files would be backed up in a possible inconsistent state, which could create restore issues.

While it is not recommended, if you want to include SQL data in a volume level backup, you must first dismount the database you want backed up. Then, run the backup job.

See [“About backing up SQL databases”](#) on page 815.

## How to back up SQL transaction logs

Backup Exec includes two methods for backing up transaction logs: Log and Log No Truncate.

When running log backups, it is recommended that you use Backup Exec exclusively to perform log transaction backups.

Use the Log No Truncate method only when the database is corrupted or database files are missing. This method backs up transactions that you may not be able to access otherwise when the database is in this state. You can then use this transaction log backup along with the last database backup and any previous transaction log backups to restore the database to the point at which it failed; however, any uncommitted transactions are rolled back. The Log No Truncate method does not remove committed transactions after the log is backed up.

To use the Log No Truncate backup to restore a database, you should also have a database backup that was created before the Log No Truncate backup. The transaction log contains only the log files used in the restore process, which alone are not sufficient to restore a complete database. You must have at least one database backup and a log backup of the database to restore a database.

---

**Caution:** Do not run a log backup using either method if the SQL database is using the simple recovery model. With the simple recovery model, you can recover data only up to the most recent full or differential backup. If you run a log backup on a database using the simple recovery completion state, the backup complete with exceptions.

---

To check the database properties, from the Database management tools on the SQL Server, right-click the database, click Properties, click the Options tab, and then view the configuration settings.

See [“About backing up SQL databases”](#) on page 815.

## About SQL 2005 or later database snapshots

SQL database snapshots enable you to quickly revert a database back to the state it was in when the database snapshot was created. When you use a database snapshot, a full restore of the host database is not required to revert the database. However, that changes made to the host between the time a database snapshot is created and the point at which it is reverted, are lost.

The Backup Exec SQL Agent works with the SQL database to create database snapshots, which are read-only, point-in-time copies of an existing host database. When Backup Exec runs a SQL backup job using the Database Snapshot (SQL 2005 or later) backup method, a request is sent to the host database instructing it to create a database snapshot.

---

**Note:** The snapshot backup method for SQL databases is only supported by SQL Server Enterprise Edition (versions 2005 or later).

---

Database snapshots cannot be backed up to storage media. Rather, they are written to a SQL snapshot file on disk. After running the database snapshot job, Backup Exec creates history and job log information to indicate the job's status.

Because database snapshots cannot be backed up, all database snapshots will be lost if the disk where the host database is installed fails. Therefore database snapshots should not be used as your sole database protection strategy. They should be used in conjunction with an overall Backup Exec database protection strategy that includes full, differential, and transaction log backups of the SQL database.

For more information, see your Microsoft SQL documentation.

---

**Note:** SQL database snapshots are not the same as Microsoft Virtual Shadow Copy Service (VSS) snapshots. Whereas VSS snapshots enable you to create point-in-time snapshots of disk volumes and shares, database snapshots enable you to create point-in-time copies of SQL databases. You cannot use the VSS option in Backup Exec's Advanced Open File Option to create SQL database snapshots.

---

---

**Note:** SQL database snapshot catalog information that refers to deleted database snapshots is periodically removed from the catalogs. If backup media is re-cataloged, the database snapshot catalog information will be periodically removed again.

---

## About reverting SQL 2005 or later databases using database snapshots

SQL 2005 or later database snapshots created with Backup Exec can be used to revert a SQL 2005 or later database back to the state it was in at a previous point in time, without having to run a full database restore job.

When viewed by resource in the Restore Wizard, SQL database snapshots appear as backup sets, in chronological order with the most recent snapshot appearing first.

The following caveats apply when reverting a database:

- You cannot undo a SQL 2005 or later database that has been reverted.
- Before reverting a database, Backup Exec deletes all existing database snapshots, including those created with SQL 2005 or later, with the exception of the snapshot used for the revert. After being deleted, the database snapshots cannot be recovered.
- You cannot redirect a database snapshot restore job.

## About restoring SQL databases

The SQL Agent lets you restore SQL Sever databases. You can restore the databases to their original location or you can redirect the restore to a new location. The number of jobs you decide on depends on the types of backup jobs that protect the database. If you use one job to restore a database, select all the backup sets that you want to apply. Include the full backup, any differential backups, and any log backups.

With very large databases this process can take several hours to complete. During this time Backup Exec reports that no data is being transferred, and the Byte count field in the Job Monitor view is not updated. When SQL has completed filling the files with zeros, the restore job continues. This occurs for all database restores but is noticeable only on very large databases.

See [“About restoring encrypted SQL databases”](#) on page 826.

See [“How to restore from SQL transaction logs up to a point in time”](#) on page 826.

See [“How to restore from SQL transaction logs up to a named transaction”](#) on page 826.

See [“About restoring the SQL master database”](#) on page 827.

See [“About redirecting restores for SQL”](#) on page 830.

## About restoring encrypted SQL databases

SQL 2008 supports Transparent Database Encryption (TDE), which lets you encrypt SQL 2008 databases at the backup set level.

When you back up a database that uses TDE, Microsoft recommends that you back up the certificate keys and encryption keys with the database. If you do not include the certificate keys and encryption keys, you must perform all backup and restore operations within the selected SQL instance.

---

**Note:** Backup Exec can redirect the restore of the database data that used TDE only if the certificate keys and encryption keys are applied to the destination instance. If the certificate keys and encryption keys are not applied to the destination instance, an error appears stating that the certificate thumbprint cannot be found.

See your Microsoft SQL 2008 documentation.

---

## How to restore from SQL transaction logs up to a point in time

You can restore transactions from a transaction log up to and including a point in time in the transaction log. After the point in time is reached, recovery from the transaction log is stopped. To find dates and times of transactions, check your client application event log.

If the specified point in time is later than the time contained in the most recent transaction log being restored, then the restore operation succeeds, but a warning is generated and the database remains in an intermediate state. If the specified point in time is before the time contained in the transaction log or logs being restored, no transactions are restored.

## How to restore from SQL transaction logs up to a named transaction

You can restore transactions from a transaction log up to and including a named transaction (or mark). After the named transaction is reached, recovery from the transaction log is stopped.

Since named transactions do not necessarily have unique names, you can also specify a date and time after which the restore operation is to search for the named transaction. For example, if you specify a restore from a log up to the named transaction `AfternoonBreak`, found after `6/02/2000, 12:01 p.m.`, then the restore

operation will not search for AfternoonBreak until after that time. To find dates and times of named transactions, check your client application event log.

If the named transaction is not found, then the restore operation succeeds, but a warning is generated and the database remains in an intermediate state.

---

**Note:** The names of transactions are case-sensitive. Ensure you enter the correct upper- and lower-case characters when specifying a named transaction.

---

## About restoring the SQL master database

If the master database is damaged, symptoms may include the following:

- An inability to start SQL.
- Segmentation faults or input/output errors.
- A report generated by SQL Database Consistency Checker utility (DBCC).

If the master database is critically damaged and SQL cannot be started, rather than running the Rebuild Master utility, or reinstalling SQL to be able to restart SQL, you can replace the corrupted or missing databases with the copies of the master and model databases that Backup Exec automatically creates and updates whenever backups of those databases are run. After SQL is running again, you can restore any other databases, if needed.

If copies of the master and model databases were not made, then you must use Microsoft's rebuildm.exe utility to rebuild the master database and start SQL.

Because all changes made to the master database after the last backup was created are lost when the backup is restored, the changes must be reapplied. If any user databases were created after the master database was backed up, those databases cannot be accessed until the databases are restored from backups or reattached to SQL.

See ["Restarting SQL using database copies"](#) on page 827.

See ["Restoring the master database"](#) on page 829.

## Restarting SQL using database copies

You can restart SQL manually using copies of the database from previous backups and then restore the master database.

See ["Restoring the master database"](#) on page 829.

**Table E-3** Restarting SQL using database copies

Step	Action
Step 1	<p>Ensure that the SQL services are not running.</p> <p>Refer to the SQL Server documentation for details.</p>
Step 2	<p>Verify that the database copies are present.</p> <p>See <a href="#">“SQL database copy locations”</a> on page 829.</p> <p>If necessary, restore the master and model database copies from a backup set to the same directory that the original master and model databases are in.</p>
Step 3	<p>Using the Windows Explorer, browse to the default data directory and delete the following files:</p> <ul style="list-style-type: none"> <li>■ master.mdf</li> <li>■ mastlog.ldf</li> <li>■ model.mdf</li> <li>■ modellog.ldf.</li> </ul>
Step 4	<p>Rename the copies of the databases back to their original names.</p> <p>See <a href="#">“SQL database names”</a> on page 829.</p> <p>Do not use read-only files. The SQL services will not start with read-only files.</p>
Step 5	<p>Use the SQL Service Control Manager to start SQL Server.</p>
Step 6	<p>Restore the latest changes to the master database.</p> <p>See <a href="#">“Restoring the master database”</a> on page 829.</p>

## SQL database copy locations

The database copies are named master\$4idr, mastlog\$4idr, model\$4idr, and modellog\$4idr.

See [“Restarting SQL using database copies”](#) on page 827.

**Table E-4** SQL database copy locations

SQL database copy	Location
A default installation of SQL 2000	C:\Program Files\Microsoft SQL Server\MSSQL\Data\*.*
A named instance of SQL 2000	C:\Program Files\Microsoft SQL Server\MSSQL\$Instance_Name\Data\*.*
An initial installation of SQL 2005 or later	C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\*.*
A second installed instance of SQL 2005 or later	C:\Program Files\Microsoft SQL Server\MSSQL.2\MSSQL\Data\*.*
A default installation of SQL 2008	C:\Program Files\Microsoft SQL Server\MSSQL10.<instance name>\MSSQL\Data

## SQL database names

The following table lists the copied database name and the original database name.

See [“Restarting SQL using database copies”](#) on page 827.

**Table E-5** SQL database names

Copied database name	Original database name
master\$4idr	master.mdf
master\$4idr	mastlog.ldf
model\$4idr	model.mdf
modellog\$4idr	modellog.ldf

## Restoring the master database

You can restore the master database after you restart SQL using database copies.

See [“About restoring the SQL master database”](#) on page 827.

#### To restore the master database

- 1 Run the Restore Wizard.
- 2 Ensure that you select the following:
  - The backup set that contains the last master database backup.
  - A consistency check that runs after the restore.After the restore, SQL restarts in multi-user mode.
- 3 Restore the remaining SQL databases.

## About redirecting restores for SQL

You can redirect the following:

- A database backup to a different server, database, or instance.
- Differential and log backups to wherever the associated database is restored.
- A database from a 32-bit or 64-bit platform to any other platform.

Single-job restores and multiple-job restores can both be used in redirected restore operations.

## About disaster recovery of a SQL Server

Backup Exec provides a quicker method for restoring SQL rather than running the Rebuild Master utility or reinstalling SQL to restart SQL. Using Backup Exec, you can replace the corrupted or missing databases with copies of the master and model databases that Backup Exec automatically creates and updates whenever backups of those databases are run.

If you use Simplified Disaster Recovery (SDR), then during an SDR recovery of drive C, it will automatically replace the damaged databases with the copies of the master and model databases. You can then restart SQL, and restore the latest master database backup and any other databases that are necessary.

## How to prepare for disaster recovery of SQL

To prepare for disaster recovery if you are using SQL do the following:

- Back up both system and user databases and transaction logs regularly.  
Copies of the master and model databases are automatically created by Backup Exec whenever you back up the master and model databases. Backup Exec places these copies in the same directory that the databases are in, where they must remain in order to be updated.

The following table includes information about MS SQL database locations:

The copies of the master and model databases are named:

- Master\$4idr
  
- Mastlog\$4idr
  
- Model\$4idr
  
- Modellog\$4idr
  
- Back up the system drives that contain SQL instances.  
Whenever you back up the system drive that contains a SQL instance, copies of the master and model databases are backed up. Backing up the system drive that SQL is on also backs up all the executables and registry settings needed for SQL to run.
- Back up the master database whenever any changes are made to SQL.
- Keep records of any service packs that have been installed.
- Ensure you are prepared to recover the entire server, not just SQL.

## Requirements for SQL disaster recovery

To perform a recovery, you will need the following items:

- The latest backup of the SQL directory (\Program Files\Microsoft SQL Server\MSSQL), and the Windows registry/System State.
- The SQL database backups, and differential and log backups.
- An Administrator logon account (or an Administrator equivalent) during the recovery.

## Disaster recovery of SQL

You can restore either the entire server, including the SQL databases, from full system backups, or restore only the SQL databases to a newly installed or other available SQL Server.

Restoring the entire server, including the SQL databases has the added benefit of recovering other applications and data that may have resided on the server at the time of failure, and can be accomplished using one of the following methods:

- Manual recovery of the Windows server, and then manual recovery of the SQL databases. This method involves manually restoring the Windows server from full system backups, and then recovering the SQL databases.
- Simplified Disaster Recovery. This option provides an automated method of restoring the Windows server as well as the SQL databases from full system backups.  
See [“Microsoft SQL Server recovery notes”](#) on page 727.

To restore only the SQL databases, review the following:

- To restore only the SQL databases to a newly-installed or other available server, the server must be running on the same hardware platform (cross-platform restores are not supported), and the same version of SQL with the same service pack level as the original server.
- To restore SQL databases to an existing installation of SQL with other active databases, you should redirect the restore.  
See [“About redirecting restores for SQL”](#) on page 830.  
See [“About recovering SQL manually”](#) on page 832.

## About recovering SQL manually

When you recover SQL manually, you must first restore the Windows server from full system backups. After recovery of the Windows computer is complete, or after the new server installation is available, you can recover the SQL databases.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

In order to restore SQL databases, SQL must be running; however, SQL cannot be started unless the master and model databases are present.

You can restore the master and model databases and start SQL using one of the following methods:

- Rename the files created by Backup Exec that replace the master and model databases. After the master and model databases are present on SQL, you must start SQL, and then restore all other databases.  
See [“Restarting SQL using database copies”](#) on page 827.
- Reinstall SQL.

This topic only details how to restart SQL by using the copies of the master and model databases made by Backup Exec. For more information on the Rebuild Master utility, or on reinstalling SQL, refer to your MS SQL documentation.

If you are restoring to a new SQL installation, start with the restore of the master database.

See [“Restoring the master database”](#) on page 829.

# Symantec Backup Exec Agent for Microsoft Exchange Server

This appendix includes the following topics:

- [About the Backup Exec Exchange Agent](#)
- [Requirements for using the Exchange Agent](#)
- [About installing the Exchange Agent](#)
- [About adding Exchange Servers and database availability groups](#)
- [About preferred server configurations](#)
- [Recommended configurations for Exchange](#)
- [Requirements for accessing Exchange mailboxes](#)
- [Backup strategies for Exchange](#)
- [How Granular Recovery Technology works with the Exchange Information Store](#)
- [Snapshot and offhost backups with the Exchange Agent](#)
- [About backing up Exchange data](#)
- [About restoring Exchange data](#)
- [How to prepare for disaster recovery of Exchange Server](#)

## About the Backup Exec Exchange Agent

The Symantec Backup Exec Agent for Microsoft Exchange Server (Exchange Agent) lets you integrate backups of Microsoft Exchange Server databases with network backups without separate administration or dedicated hardware.

The Exchange Agent provides the following features:

- The ability to restore individual items from backups for which you enable Granular Recovery Technology.
- The ability to restore to a PST file.
- The ability to select storage groups for backup and restore jobs, or to select one or more databases within the storage group for backup and restore jobs.
- The ability to restore individual databases or storage groups from non-snapshot backups by using the Recovery Storage Group feature in Exchange Server 2003 and Recovery Database feature in Exchange Server 2010. For Exchange Server 2007/2010, you can restore snapshot backups to a recovery storage group or database.
- Seeding of an Exchange Server 2010 database copy. Seeding adds a database copy to a location on another mailbox server in a database availability group (DAG).
- Snapshot backup and offhost backup on Exchange Server 2003 or Exchange Server 2007 instances that run on Windows Server 2003.
- Offhost backup with Granular Recovery Technology (GRT) for Exchange Server 2003/2007/2010.

See [“About installing the Exchange Agent”](#) on page 838.

See [“Backup strategies for Exchange”](#) on page 846.

See [“Recommended configurations for Exchange ”](#) on page 844.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“About off-host backup ”](#) on page 1052.

## Requirements for using the Exchange Agent

The Backup Exec server must meet the following requirements:

**Table F-1** Backup Exec server requirements for the Backup Exec Exchange Agent

Backup Exec server requirements	Description
To support the Exchange Agent	<ul style="list-style-type: none"><li>■ A license for Symantec Backup Exec Microsoft Exchange Server Agent (Exchange Agent) must be entered on the Backup Exec server.</li><li>■ The Backup Exec Agent for Windows must be installed on any remote Exchange Server that you want to back up.</li><li>■ The Backup Exec server must have access to the Exchange Server.</li></ul> <p><b>Note:</b> To back up Exchange Server 2010, you must install Backup Exec on a Microsoft Windows 2008 SP2 64-bit server or a Microsoft Windows 2008 R2 64-bit server.</p> <ul style="list-style-type: none"><li>■ Symantec recommends that you use a Backup Exec services account that has domain and local administrator rights on the Exchange Server.</li></ul>
To back up Exchange Server 2007/2010	<p>To back up Microsoft Exchange Server 2007/2010, you must install the Exchange Management Tools for Microsoft Exchange Server 2007/2010 on the Backup Exec server. The management tools on the Backup Exec server must be the same version or later as the management tools that are on the Exchange Server 2007/2010.</p> <p>You can install the management tools when you do a custom install of Microsoft Exchange Server 2007/2010. If you install the management tools and Backup Exec together on a Backup Exec server, install the tools first. If you install Backup Exec before you install the management tools, you must restart the Backup Exec server when the tools installation is complete.</p>

**Table F-1** Backup Exec server requirements for the Backup Exec Exchange Agent (*continued*)

Backup Exec server requirements	Description
To support the Backup Exec Data Discovery feature, which allows detection of new backup content within your domain	<p>For Exchange 2003, Microsoft Exchange System Manager utility must be installed.</p> <p>For Exchange 2007/2010, Exchange Management Tools must be installed. You can install both versions of the Exchange Management Tools on the Backup Exec server.</p>
To support Granular Recovery Technology (GRT) for the restore of individual items from Information Store backups	<p>One of the following versions of a Microsoft Windows operating system that supports minifilter drivers must be installed for Microsoft Exchange:</p> <ul style="list-style-type: none"> <li>■ Microsoft Windows Server 2003 (with at least Service Pack 1)</li> <li>■ Microsoft Windows Server 2003 R2 Editions</li> <li>■ Microsoft Windows Server 2008 SP2</li> <li>■ Microsoft Windows Server 2008 R2 Editions</li> </ul> <p><b>Note:</b> For Exchange Server 2010, you must use either Microsoft Windows 2008 SP2 or a Microsoft Windows Server 2008 R2.</p> <p>Storage that you use for GRT-enabled backups may have additional requirements.</p> <p>See <a href="#">“Recommended devices for backups that use Granular Recovery Technology”</a> on page 545.</p> <p>See <a href="#">“About requirements for jobs that use Granular Recovery Technology”</a> on page 547.</p>

The following are requirements for the Exchange Server with the Backup Exec Exchange Agent:

**Table F-2** Exchange Server requirements

Exchange Server requirements	Description
To support Exchange Server 2007	<p>Download the Microsoft Exchange Server MAPI Client and Collaboration Data Objects package and install it on Exchange Server 2007.</p> <p>This package provides support for the following:</p> <ul style="list-style-type: none"><li>■ The restore of individual mailboxes, mail messages, and public folders from an Information Store backup.</li><li>■ The collection of catalog information for a backup for which the Granular Recovery Technology option is enabled and the destination device is tape.</li></ul> <p>You can find this package on the Microsoft Web site.</p>
For operations on all Exchange Servers	<p>The user account must be a member of the following groups:</p> <ul style="list-style-type: none"><li>■ The Administrators group</li><li>■ The Domain Admins</li></ul> <p>To support the Granular Recovery Technology option, you must use the appropriate Exchange Server management utility to assign the user account the Exchange Organization Administrators role (2007) or the Exchange Organization Management role (2010).</p>
To support snapshot backups	<p>Use Microsoft Exchange Server that runs on Windows Server 2003 or later.</p> <p><b>Note:</b> To select incremental or differential backup methods, Exchange Server 2003 Service Pack 1 or later must be installed.</p>

**Table F-2** Exchange Server requirements (*continued*)

Exchange Server requirements	Description
To back up and restore Exchange Server 2010	To back up the databases on a database availability group (DAG) you must install the Agent for Windows on all the servers in the DAG.  To use the Granular Recovery Technology option to restore individual items, you must install Agent for Windows on all Client Access Servers in the site.  See <a href="#">“About the Agent for Windows”</a> on page 731.

Backup Exec does not support the Granular Recovery Technology option when Outlook is installed on the same computer with Exchange Server 2003.

See the Microsoft Knowledge Base for information about installing Outlook and Exchange Server on the same computer.

See [“About discovering data to back up”](#) on page 537.

## About installing the Exchange Agent

The Exchange Agent is installed as part of the Agent for Applications and Databases and can protect local or remote Exchange Server databases.

To protect Exchange Server 2010, you must install Backup Exec on a Microsoft Windows 2008 SP2 64-bit server or a Microsoft Windows 2008 R2 64-bit server.

---

**Note:** When you install Microsoft Exchange Tools 2007/2010 and Backup Exec together on a server, Exchange Tools 2007/2010 must be installed first. If you install Backup Exec before Exchange Tools, you must restart the Backup Exec server after you finish the Exchange Tools installation.

---

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

## About adding Exchange Servers and database availability groups

You can add an Exchange Server and a database availability group (DAG) to the list of servers on the **Backup and Restore** tab so that these servers can be selected for backup jobs. When you select the **Add** option in the **Servers** group on the **Backup and Restore** tab, an option to add a Microsoft Windows computer or a Microsoft Exchange database availability group appears. Complete the steps to add the Exchange Server or the DAG.

---

**Note:** When you add a Microsoft Exchange database availability group, Symantec recommends that you manually reboot each Exchange Server after installing the Agent for Windows. If you select to automatically reboot after install, all of your Exchange Servers in the DAG may reboot at the same time.

---

See [“About backing up Exchange data”](#) on page 852.

## About preferred server configurations

Preferred server configurations are collections of one or more servers and sites that you select as preferred backup sources. Preferred server configurations take priority as backup sources in instances where database copies are replicated between multiple servers. You can create preferred server configurations for Microsoft Exchange Database Availability Groups (DAG).

You do not have to create a preferred server configuration to back up replicated database copies. You can let Backup Exec choose the best server from which to back up the replicated database copies. Designating a preferred server configuration gives you more control over your backup jobs. For example, you can select a local preferred server configuration to avoid having to back up replicated data over your WAN.

Backup Exec automatically includes the children of any site or DAG that you select as part of the preferred server configuration. So if you want to ensure that a backup is performed locally, you can select the local site as the preferred server configuration. Backup Exec selects from any of the local servers that belong to that site during the backup job. If you want to ensure that a specific server is used for the backup, select only that server as the preferred server configuration.

See [“Creating preferred server configurations”](#) on page 840.

See [“Deleting preferred server configurations”](#) on page 840.

See [“Editing settings for preferred server configurations”](#) on page 840.

See [“Designating a default preferred server configuration”](#) on page 841.

## Creating preferred server configurations

You can create preferred server configurations for Microsoft Exchange Database Availability Groups. Preferred server configurations give you more control over your backup jobs by letting you specify a preferred server from which Backup Exec backs up replicated data.

See [“About preferred server configurations”](#) on page 839.

### To create preferred server configurations

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Preferred Servers**.
- 2 Click **New**.
- 3 Complete the appropriate options.  
See [“Preferred Servers options”](#) on page 843.
- 4 On the **Preferred Servers** dialog box, click **OK**.
- 5 On the **Manage Preferred Servers** dialog box, click **OK**.

## Deleting preferred server configurations

You can delete a preferred server configuration if you no longer need it.

See [“About preferred server configurations”](#) on page 839.

### To delete preferred server configurations

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Preferred Servers**.
- 2 Select the preferred server configuration you want to delete.
- 3 Click **Delete**.
- 4 Click **OK**.

## Editing settings for preferred server configurations

You can edit the settings for an existing preferred server configuration.

See [“About preferred server configurations”](#) on page 839.

### To edit settings for preferred server configurations

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Preferred Servers**.
- 2 Select the preferred server configuration you want to edit.
- 3 Click **Edit**.
- 4 Complete the appropriate options.  
See [“Preferred Servers options”](#) on page 843.
- 5 On the **Preferred Servers** dialog box, click **OK**.
- 6 On the **Manage Preferred Servers** dialog box, click **OK**.

## Designating a default preferred server configuration

You can designate a default preferred server configuration for all of your backup jobs that contain the appropriate replication data. When you back up data from a Microsoft Exchange Database Availability Group, you can set up Backup Exec to use your default preferred server configuration. You can override the default preferred server configuration for specific jobs in the backup job settings.

---

**Note:** When you designate a default preferred server configuration, it is not applied to existing backup jobs. It is considered the default preferred server configuration for any subsequent backup jobs that you create.

---

See [“About preferred server configurations”](#) on page 839.

If you no longer want the preferred server configuration to be the default, you can remove its default status.

See [“Removing the default status for a preferred server configuration”](#) on page 841.

### To designate a default preferred server configuration

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Preferred Servers**.
- 2 Select the preferred server configuration you want to set as the default.
- 3 Click **Set as Default**.
- 4 Click **OK**.

## Removing the default status for a preferred server configuration

You can designate a default preferred server configuration for all of your backup jobs that contain the appropriate replication data.

See [“Designating a default preferred server configuration”](#) on page 841.

If you no longer want the preferred server configuration to be the default, you can remove its default status.

**To remove the default status for a preferred server configuration**

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Preferred Servers**.
- 2 Select the preferred server configuration from which you want to remove the default status.
- 3 Click **Remove as Default**.
- 4 Click **OK**.

## Manage Preferred Servers options

You can manage the settings for preferred servers.

See [“About preferred server configurations”](#) on page 839.

**Table F-3** Manage Preferred Servers options

Item	Description
<b>Name</b>	Indicates the name of the preferred server configuration.
<b>Default</b>	Indicates if the server is the default.
<b>New</b>	Lets you create a new preferred server configuration.  See <a href="#">“Creating preferred server configurations”</a> on page 840.
<b>Delete</b>	Deletes the selected preferred server configuration.  See <a href="#">“Deleting preferred server configurations”</a> on page 840.
<b>Edit</b>	Lets you change settings for the selected preferred server configuration.  See <a href="#">“Editing settings for preferred server configurations”</a> on page 840.

Table F-3 Manage Preferred Servers options (continued)

Item	Description
<b>Set as Default</b>	Lets you establish the selected preferred server configuration as the default.  See <a href="#">“Designating a default preferred server configuration”</a> on page 841.
<b>Remove as Default</b>	Removes the default status for the selected preferred server configuration.  See <a href="#">“Removing the default status for a preferred server configuration”</a> on page 841.

## Preferred Servers options

You can configure settings for preferred servers for backup jobs.

See [“About preferred server configurations”](#) on page 839.

Table F-4 Preferred Servers options

Item	Description
<b>Choose a forest</b>	Lets you select a forest.
<b>Preferred servers configuration</b>	Indicates the name of the preferred server configuration. You must enter a name before the preferred server configuration can be created.
<b>New</b>	Lets you create a new preferred server configuration. This option enables the lists of available and selected servers from which you designate the preferred server.  <b>Note:</b> The <b>New</b> option appears only if you create a preferred server configuration while you create a new backup job.
<b>Available Servers and Sites</b>	Lists any available servers and sites that can be used in the preferred server configuration.
<b>Selected Servers and Sites</b>	Lists the servers and sites that you have selected to use as part of the preferred server configuration.

## Recommended configurations for Exchange

Before starting backups for Exchange, read the following recommendations for configuring Exchange to make it easier to restore from backups:

**Table F-5** Recommended configurations for Exchange

Recommendation	Description
Put transaction log files on a separate physical disk from the database.	This is the single most important configuration affecting the performance of Exchange. This configuration also has recovery implications, since transaction logs provide an additional recovery resource.
Make Write Cache unavailable on the SCSI controller.	The Windows operating system does not use buffers, so when Exchange receives a write complete notice from Windows, the write-to-disk has been completed. If Write Cache is enabled, Windows responds as though a write-to-disk has been completed, and will provide this information to Exchange (or other applications) incorrectly. The result could be data corruption if there is a system crash before the operation is actually written to disk.
Make circular logging unavailable if possible.	Circular logging minimizes the risk that the hard disk will be filled with transaction log files. But, if a solid backup strategy is in place, transaction log files are purged during the backup, thus freeing disk space. If circular logging is enabled, transaction log histories are overwritten, incremental and differential backups of storage groups and databases are disabled, and recovery is only possible up to the point of the last full or copy backup.
Avoid making the Exchange Server a domain controller.	For disaster recovery purposes, it is much easier to restore Exchange if you don't have to restore the Active Directory first.
Install Exchange into a domain that has at least two domain controllers.	Active Directory replication is not possible with only one domain controller in a domain. If the domain controller fails and corrupts the Active Directory, some transactions may not be recoverable if they were not included with the last backup. With at least two domain controllers in a domain, databases on the failed domain controller can be updated using replication to fill in missing transactions after the database backups have been restored.

See [“Requirements for accessing Exchange mailboxes”](#) on page 845.

# Requirements for accessing Exchange mailboxes

Backup Exec must have access to a uniquely named mailbox within the Exchange organization for Information Store operations, depending on how the backup and restore jobs are configured.

Access to a uniquely named mailbox is required when you do the following:

- Configure a backup job that has all of the following settings:
  - A disk storage device other than a legacy backup-to-disk folder is the destination device.
  - The Granular Recovery Technology option is enabled.
  - A backup method other than a snapshot method.
- You restore mailboxes and public folders.

You must use a Backup Exec logon account to connect to the Exchange Server when you select mailboxes or public folders for backup. Backup Exec attempts to find a mailbox with the same name as the user name that is stored in the Backup Exec logon account.

If you use a Backup Exec logon account that stores a unique user name and has a corresponding mailbox with the same name, then you are not prompted for an additional logon account. Otherwise, you must choose or create a Backup Exec logon account that stores the name of a unique mailbox within the Exchange organization.

A unique name does not share the first five characters in another mailbox name. For example, if EXCH1 is entered as the mailbox name, and there is another mailbox name such as EXCH1BACKUP, then Backup Exec cannot accept the name. You are prompted to choose another mailbox name.

You can choose or create a logon account that meets any of the following requirements:

- A logon account for which the user name matches a unique mailbox name.
- A logon account that uses a unique alias to a mailbox. The user account that connects to the Exchange Server must also have access to this mailbox.
- A logon account that uses the full computer name for a mailbox. The user account that connects to the Exchange Server must also have access to this mailbox.

An example of a full computer name is:

```
/O=Exchange_Organization/OU=Administrative_Group/CN=Recipients/CN=mailbox_name
```

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“Creating a Backup Exec logon account”](#) on page 500.

## Backup strategies for Exchange

Backup Exec incorporates online, nondisruptive Exchange database protection as part of everyday backup routines, which increases the chance of data recovery and minimizes data loss without inhibiting daily activity. Backup Exec protects Exchange data, including the individual storage group, database, mailbox, and public folder with full, copy, incremental, and differential backups.

To decide which backup methods to use, consider the following:

- In small office environments with relatively small numbers of messages passing through the system, a daily full backup will provide good data protection and the quickest recovery. If log file growth becomes an issue, consider using incremental online backups at midday to provide an added recovery point and manage the log file growth for you automatically.
- In large environments, incremental backups should be used to provide more frequent recovery point options throughout the day and to manage log file growth. Many shops run full backups on a weekly basis, preferring to run incremental backups throughout the week to keep backup run time to a minimum. The trade-off with this technique occurs at recovery time when you must recover from the full backup and from each incremental backup as well.

What works best for you is based on the size of your environment, the number of transactions processed each day, and the expectations of your users when a recovery is required.

Consider the following backup strategies:

- Run full backups with the option to enable the restore of individual items selected so that you can restore individual mail messages and folders without restoring the entire database.

Depending on your environment, run full backups as follows:

- As frequently as possible, no less than once a day.
- Daily with differential backups used at regular periods throughout the day.
- Every few days (no less than weekly) with frequent incremental backups in between each full backup.
- Run Exchange backup jobs separately from other backup jobs.

In addition to backing up Exchange storage groups or databases, you should also back up the following on a regular basis:

**Table F-6** Backup selections for Exchange configuration data

Recommended backup selections for configuration data	Description
File system	<p>Back up folders and drives containing files for Windows and Exchange. Usually, this is the root drive C:\ but may be different in each environment.</p> <p><b>Note:</b> Back up the C:\ drive, but do not back up the virtual drive that is created by Exchange, if this virtual drive exists in your environment. It is intended only to provide Explorer access to the Exchange data, but all file system functions may not be replicated. Backup and restore operations are not recommended or supported.</p>
Windows registry	<p>Back up the registry by running a full backup.</p>
System State and/or Shadow Copy Components	<p>Select System State and run a full backup to back up the following:</p> <ul style="list-style-type: none"> <li>■ The Internet Information Service (IIS) metabase</li> <li>■ The Windows registry</li> </ul> <p>See <a href="#">“About selecting data to back up”</a> on page 177.</p> <p>If the entire server must be restored, you must restore both System State and Shadow Copy Components.</p>
Active Directory	<p>To back up Active Directory, select System State on the domain controllers and run a full backup.</p> <p>When there are configuration changes on the Exchange Server database, such as when objects are added, modified, or deleted, back up the Active Directory on the domain controllers.</p> <p><b>Note:</b> Spread multiple domain controllers throughout each domain for efficient Active Directory replication, and so that if one domain controller fails, redundancy is still provided.</p>

---

**Note:** Configure an Information Store backup for which the Granular Recovery Technology (GRT) option is enabled to restore individual mailboxes, mail messages, and public folders.

---

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“How to prepare for disaster recovery of Exchange Server”](#) on page 862.

## Automatic exclusion of Exchange data during volume-level backups

If you select a volume that contains Exchange data for backup, the Exchange Agent uses Active File Exclusion to automatically exclude Exchange data that should not be included in a volume-level backup. For example, .EDB and .STM files, as well as transaction log files, should not be part of a volume-level backup because they are opened for exclusive use by Exchange.

Without this exclusion, during a non-snapshot backup, these files appear as in use - skipped. During a snapshot backup, these files may be backed up in an inconsistent state, which could create restore issues.

While it is not recommended, if you want to include Exchange data in a volume-level backup, you must first dismount the storage groups or databases that you want backed up, and then run the backup job.

See [“About backing up Exchange data”](#) on page 852.

## About the circular logging setting for Exchange

When circular logging is enabled, you cannot run incremental and differential backups of Exchange databases and storage groups. These types of backups rely on a complete history of logs.

When circular logging is enabled, transaction log files that have already been committed to the database are overwritten, preventing the accumulation of logs. The log files are overwritten whether or not a full or incremental backup has been run, and a history of previous logs since the last full or incremental backup is not maintained.

When circular logging is disabled, transaction log files accumulate on the disk until a full or incremental backup is performed.

After these operations, the log files that have all transactions committed to the database are deleted.

See [“Backup strategies for Exchange”](#) on page 846.

# How Granular Recovery Technology works with the Exchange Information Store

Backup Exec Granular Recovery Technology (GRT) lets you restore individual items from an Information Store backup without having to restore the whole backup. You should review the requirements for a GRT-enabled backup before you configure it.

When you select items to restore from GRT-enabled backups, you cannot select the top level of the Information Store. To restore these items, you must restore the entire mailbox.

You can also enable GRT when you create an offhost backup for the Information Store. Offhost backup lets Backup Exec move the backup process from the host computer to the Backup Exec server. The host computer is the remote computer that contains the volumes that you selected for backup. To run a GRT-enabled offhost backup, you must install the Backup Exec Advanced Disk-based Option on the Backup Exec server.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“Recommended devices for backups that use Granular Recovery Technology”](#) on page 545.

See [“About requirements for jobs that use Granular Recovery Technology”](#) on page 547.

See [“About Backup Exec and Microsoft Exchange Web Services”](#) on page 849.

See [“About installing the Advanced Disk-based Backup Option”](#) on page 1048.

## About Backup Exec and Microsoft Exchange Web Services

Backup Exec uses Microsoft Exchange Web Services (EWS) to support the Granular Recovery Technology option. EWS provides support for the restore of individual mailboxes, mail messages, and public folders from an Exchange Server 2010 database backup.

---

**Note:** You do not need to install the MAPI Client and Collaboration Data Objects package if you use EWS.

---

To use EWS to restore individual items, Backup Exec disables the client throttling policy for the resource credentials you specify for the restore job. The client throttling policy is located on the Client Access Server and enforces connection bandwidth limits on the Exchange Server.

Backup Exec also creates an impersonation role and a role assignment for Exchange Impersonation. Exchange Impersonation role assignment associates the impersonation role with the Backup Exec resource credentials you specify for the restore job.

Backup Exec creates and assigns the following roles:

- SymantecEWSImpersonationRole
- SymantecEWSImpersonationRoleAssignment

See “[How Granular Recovery Technology works with the Exchange Information Store](#)” on page 849.

## Snapshot and offhost backups with the Exchange Agent

The Exchange Agent supports the Microsoft Volume Shadow Copy Service (VSS), a snapshot provider service only available on Windows Server 2003 or later. Using VSS, a point in time view of the Exchange database is snapped and then backed up, leaving the actual Exchange database open and available for users.

Offhost backup enables the backup operation to be processed on a Backup Exec server instead of on the Exchange Server. Moving the backup from the Exchange Server to a Backup Exec server enables better backup performance and frees the remote computer as well.

If the Advanced Disk-based Backup Option (ADBO) is installed on the Backup Exec server, you can use the Backup Exec Granular Recovery Technology (GRT) option when you create an offhost backup for the Information Store.

See “[Setting default Granular Recovery Technology \(GRT\) options](#)” on page 482.

The Exchange Agent snapshot does not support the following:

- NAS configurations
- The Exchange 2003 Recovery Storage Group feature
- Mixing snapshot backups and non-snapshot backups

Due to a Microsoft Exchange limitation, if non-snapshot backups are run as part of a backup strategy, then snapshot backups should not be run. If snapshot backups are run, non-snapshot backups should not be done.

You can find a list of compatible storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

The type of backup method that is available when using VSS with the Exchange Agent depends on the version of Exchange Server, and are listed in the following table:

**Table F-7** Available backup methods for Exchange snapshot versions

Exchange version	Available backup methods
Exchange Server 2003	The following backup methods are available: <ul style="list-style-type: none"> <li>■ Full</li> <li>■ Copy</li> </ul>
Exchange Server 2003 with Service Pack 1 or later Exchange Server 2007/2010	The following backup methods are available: <ul style="list-style-type: none"> <li>■ Full</li> <li>■ Copy</li> <li>■ Differential</li> <li>■ Incremental storage group level snapshot backup</li> <li>■ Individual database restore</li> </ul>
Exchange Server 2007	LCR/CCR - Back up from the passive copy or the active copy. <b>Note:</b> You cannot back up the passive copy of the Standby Continuous Replication (SCR) database with Exchange Server 2007. The SCR is not available for backup selection.

## Configuring a snapshot backup for Exchange data

Symantec recommends that you perform consistency checks before running a snapshot backup.

See [“Snapshot and offhost backups with the Exchange Agent”](#) on page 850.

**Table F-8** Configuring a snapshot backup for Exchange data

Step	Action
Step 1	Create an Exchange backup job. See <a href="#">“About backing up Exchange data”</a> on page 852.
Step 2	If data that is not supported for snapshot backup is included in the backup selections, check <b>Process logical volumes for backup one at a time</b> to allow the job to complete with errors.

**Table F-8** Configuring a snapshot backup for Exchange data (*continued*)

Step	Action
Step 3	Schedule or start the backup job. See <a href="#">“Backing up data”</a> on page 163. See <a href="#">“Troubleshooting Exchange Agent snapshot and offhost jobs”</a> on page 852. See <a href="#">“About restoring Exchange data from snapshot backups”</a> on page 860.

## Troubleshooting Exchange Agent snapshot and offhost jobs

An Exchange Agent snapshot job fails on the following conditions:

- The Exchange Agent snapshot fails.
- If incremental or differential backup methods are selected, and Exchange Server 2003 Service Pack 1 or later is not installed.
- If circular logging is enabled, and incremental or differential backup methods are selected.
- You run a snapshot job on Windows Small Business Server 2003. The Microsoft Exchange Server 2003 VSS Writer is disabled on Windows Small Business Server 2003, which causes snapshot backups for Exchange 2003 to fail. To successfully perform an Exchange 2003 snapshot backup, review the following Microsoft Knowledge Base article:  
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q838183>  
You must resolve this issue to perform a successful restore job by using the Intelligent Disaster Recovery option.

See [“Snapshot and offhost backups with the Exchange Agent”](#) on page 850.

## About backing up Exchange data

To back up Exchange data, you can select the following:

- Multiple storage groups
- Individual storage groups
- Individual databases (Exchange 2010 only)
- Database availability groups (DAG)

You must enter an Exchange Agent license on the Backup Exec server for each Exchange Server in the DAG that you want to back up. You must then install the Agent for Windows on all the servers in the DAG.

Each database in the DAG must be backed up through the DAG container that displays in the list of servers on the **Backup and Restore** tab. The DAG container displays an Exchange logo on the server.

---

**Note:** If you add Exchange databases or storage groups after you create a backup job, you must edit the backup job to include the new selections.

---

Symantec recommends that you select individual storage groups for backup rather than selecting individual databases in storage groups. Although you can select individual databases in a storage group for backup, the transaction logs for the entire storage group are backed up.

For example, if back up a single database in a storage group that contains four databases, the entire collection of transaction logs for the storage group is also backed up. The transaction logs are not deleted until a full backup is run on every database in the storage group. You can still restore an individual database from a storage group backup.

---

**Note:** To perform incremental and differential backups of storage groups, ensure that circular logging is not enabled on the storage group.

---

You can set backup job default options for all Exchange backup jobs. Each time you create a backup job, the job uses the default options unless you change the options for that particular job.

See [“Backing up data”](#) on page 163.

See [“About adding Exchange Servers and database availability groups”](#) on page 839.

See [“Automatic exclusion of Exchange data during volume-level backups”](#) on page 848.

See [“Setting default backup job settings”](#) on page 456.

See [“Microsoft Exchange backup options”](#) on page 854.

See [“Editing backups”](#) on page 170.

See [“Editing a stage”](#) on page 184.

## Microsoft Exchange backup options

The following options are available for Microsoft Exchange backup jobs. These options appear when you select the Microsoft Exchange option on the **Backup Job Defaults** dialog box and on the **Backup Options** dialog box for a backup job.

See [“About backing up Exchange data”](#) on page 852.

See [“Backing up data”](#) on page 163.

See [“Setting default backup job settings”](#) on page 456.

**Table F-9** Microsoft Exchange backup options

Item	Description
<b>Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual mailboxes, mail messages, and public folders from Information Store backups</b>	Enables the restore of individual items from Information Store backups. Ensure that you meet the requirements for Granular Recovery Technology. See <a href="#">“Recommended devices for backups that use Granular Recovery Technology”</a> on page 545. See <a href="#">“About requirements for jobs that use Granular Recovery Technology”</a> on page 547.

**Table F-9** Microsoft Exchange backup options (*continued*)

Item	Description
<p><b>Perform consistency check before backup when using Microsoft Volume Shadow Copy Service (VSS) snapshot provider</b></p>	<p>Performs a consistency check when the Microsoft Volume Shadow Copy Service option is selected. The option Microsoft Volume Shadow Copy Service is automatically used whenever a software backup is selected on the Advanced Disk-based Backup properties. You can also select the Microsoft Volume Shadow Copy Service on the Advanced Open File backup properties.</p> <p>The consistency check, which is run on the snapshot, determines if possible data corruption exists.</p> <p>If this option is selected, and the dependent option Continue with backup if consistency check fails is not selected, then data for specific Exchange objects that are determined to be corrupt are not backed up. All other non-corrupt Exchange objects are backed up.</p> <p>For example, if any transaction log file for a Storage Group is corrupt, then none of the transaction log files are backed up for that Storage Group when the Continue with backup if consistency check fails option is not selected. However, the Exchange database files are backed up if Backup Exec determines they are not corrupt. Similarly, if a specific Exchange database file is corrupt, then backup is skipped only for that corrupt database file. All other non-corrupt database files and transaction log files are backed up.</p> <p>When the option Continue with backup if consistency check fails is enabled, then all Exchange data is backed up regardless if corrupt files exist.</p> <p>See <a href="#">“Snapshot and offhost backups with the Exchange Agent”</a> on page 850.</p>
<p><b>Continue with backup if consistency check fails</b></p>	<p>Continues the backup job even if the consistency check fails. You may want the job to continue if you think a backup of the database in its current state is better than no backup at all, or if you are backing up a very large database that may have only a small problem.</p>

**Table F-9** Microsoft Exchange backup options (*continued*)

Item	Description
<p><b>High Availability Server (Exchange 2007 or later)</b></p>	<p>Specifies one of the following backup sources for Exchange 2007/2010:</p> <ul style="list-style-type: none"> <li> <p>■ Back up from the passive copy and if not available, try the active copy (recommended)</p> <p>Lets you back up a passive copy of the database by default. Backup Exec selects the passive copy based on your selections in the Preferred Server settings. However, if the passive copy is not available, Backup Exec backs up the active copy of the database. During the backup, database performance degradation can occur if you have to back up the database over a WAN.</p> </li> <li> <p>■ Back up from the passive copy only (job fails if not available)</p> <p>Lets you back up a passive copy of the database. If Backup Exec cannot access the passive copy, the job fails. In this case, neither the active nor the passive database is backed up. Select this option when you do not want to affect the performance of the active copy of the database. For Exchange Server 2010, Backup Exec selects the passive copy based on your selections in the Preferred Server settings.</p> <p><b>Note:</b> You must have the preferred server settings configured to use this option.</p> <p>See “<a href="#">About preferred server configurations</a>” on page 839.</p> </li> <li> <p>■ Back up from the active copy only (job fails if not available)</p> <p>Lets you back up the active copy of the database. If Backup Exec cannot access the active copy, the job fails. Therefore, neither the active copy nor the passive copy is backed up.</p> <p>The active copy contains newer information than the passive copy. When you back up the active copy, you have a backup of the most recent database data.</p> <p><b>Note:</b> You cannot back up the passive copy of the Standby Continuous Replication (SCR) database with Exchange Server 2007. The SCR is not available for backup selection.</p> </li> </ul>

## About restoring Exchange data

The Exchange Agent lets you restore Exchange databases and storage groups as well as individual mailbox items. You can restore items to their original location or you can redirect the restore to a new location.

See [“About searching for and restoring data”](#) on page 229.

The requirements and procedures for restoring Exchange data vary depending on the backup strategy you used. Before you restore Exchange data, you should review the required configuration and tasks.

You can restore Exchange data in the following ways:

- Use the recovery storage group or recovery database to recover data from an older backup copy of the store without disturbing client access to current data. See [“About restoring data using the Exchange 2003/2007 recovery storage group or Exchange Server 2010 recovery database”](#) on page 858.
- Restore Exchange data from snapshot backups. See [“About restoring Exchange data from snapshot backups”](#) on page 860.
- Restore individual Exchange items from a backup that uses Granular Recovery Technology (GRT). See [“How Granular Recovery Technology works with the Exchange Information Store ”](#) on page 849.
- Restore Exchange data to a server other than the one from which it was backed up. See [“About redirecting Exchange restore data”](#) on page 860.

See [“Requirements for restoring Exchange”](#) on page 857.

See [“About redirecting Exchange restore data”](#) on page 860.

## Requirements for restoring Exchange

Review the following before restoring Exchange:

- The storage groups and databases must already exist on the destination server, and must have the same names as the original storage groups or databases.
- The destination server must have the same Organization and Administrative Group name as the source server.
- Before you start the restore, configure the destination databases so that they can be overwritten by a restore. See [“Configuring a database in Exchange”](#) on page 858.

## Configuring a database in Exchange

Before you restore Exchange, you should configure the destination database.

See [“Requirements for restoring Exchange”](#) on page 857.

### To configure a database

**1** Do one of the following:

For Exchange 2003

Open the Exchange System Manager utility.

For Exchange 2007/2010

Open the Exchange Management Console utility.

**2** Right-click the database that you want to overwrite.

**3** Click **Properties**.

**4** Do one of the following:

For Exchange 2003/2007

On the **Database** tab, select **This database can be overwritten by a restore**.

For Exchange Server 2010

On the **Maintenance** tab, select **This database can be overwritten by a restore**.

## About restoring data using the Exchange 2003/2007 recovery storage group or Exchange Server 2010 recovery database

The Recovery Storage Group (RSG) feature in Exchange 2003/2007 lets you to mount a second copy of an Exchange mailbox store on any Exchange Server in the same Exchange Administrative Group as the original while the original store is still running and serving clients. This allows you to recover data from an older backup copy of the store without disturbing client access to current data.

Exchange Server 2010 uses recovery databases instead of RSGs. Each server has a recovery database and there cannot be more than one mounted recovery database.

See your Microsoft Exchange documentation for more information about RSGs and recovery databases.

After the RSG or recovery database is created, you can restore online backup sets to it. Then you can use the version of the EXMerge utility in Exchange 2003 or Exchange Management Shell in Exchange 2007/2010 to extract mailbox data from

the stores into .PST files, and optionally merge the extracted data back into the online stores.

If the RSG or recovery database resides on a different Exchange Server than the databases you are restoring, you should review the requirements for redirecting the restore of Exchange storage groups or recovery databases.

Following are requirements for restoring data using the Exchange 2003/2007 data Recovery Storage Group (RSG) or Exchange Server 2010 recovery database:

- For Exchange 2003, data cannot be restored from a snapshot backup.
- If multiple stores are selected for restore, mailbox stores in the RSG must come from the same storage group. You cannot add mailbox stores from different storage groups to the RSG at the same time.
- Public folder stores are not supported for restore using the RSG.
- Do not mount mailbox stores in the RSG before the restore. If you do mount the stores before the restore, then you must dismount them. Select the following option on the database property page in Exchange System Manager: This database can be overwritten by a restore  
Then, delete any files created in the data path for the RSG and added stores prior to restoring them.  
Any files created in the data path for the RSG and added store or stores, should be deleted as well, if stores were mounted prior to the restore.
- On the server that hosts the RSG, there must be a storage group with the same name as the original storage group for the data you are restoring. If no such storage group exists on the server, then you can use that name for the RSG when you create it.
- The Active Directory topology of the Exchange system must be intact and in the same state it was in when the backup was made. You cannot restore mailbox stores that were deleted and recreated. In addition, you cannot recover mailboxes from stores if the mailboxes were deleted and purged from the system or moved to other servers or mailbox stores.
- When the RSG exists on a server, the mailbox stores that it contains are the only stores that can be restored on that server by default. Symantec recommends that you create the RSG only when you intend to recover data using it, and remove the RSG from the server after the data recovery is complete.
- You can have more than one recovery database, however, you can only mount one recovery database to recover data.
- Do not mount the recovery database before the restore. If you do mount the recovery database before the restore, you must dismount it. Select the **This**

**database can be overwritten by a restore** option on the database property page in Exchange Management Console utility.

Refer to your Microsoft Exchange Server documentation for more information on the requirements and restrictions of recovering Exchange data.

See [“About restoring Exchange data”](#) on page 857.

See [“About redirecting Exchange restore data”](#) on page 860.

## About restoring Exchange data from snapshot backups

Note the following when restoring Exchange data from snapshot backups:

- If circular logging is enabled, only point-in-time, loss restores are possible. Roll-forward, no-loss restores cannot be performed.
- For Exchange 2003/2007, individual database restores cannot be performed. The job will fail.
- The following options are not applicable to restores of Exchange 2003 snapshot backups. Exchange will use the soft-recovery process when restored databases are mounted.
  - Restore all the transaction logs and do not delete existing transaction log
  - Purge the existing data and restore only the databases and transaction logs
  - Enter a location on the Exchange Server for temporary storage of log and patch files used during the restore
- For Exchange 2003, data cannot be restored from a snapshot backup to a Recovery Storage Group (RSG).

See [“About restoring data using the Exchange 2003/2007 recovery storage group or Exchange Server 2010 recovery database”](#) on page 858.

See [“Snapshot and offhost backups with the Exchange Agent”](#) on page 850.

See [“About restoring Exchange data”](#) on page 857.

## About redirecting Exchange restore data

With Backup Exec, you can restore Exchange data to the server from which it was backed up or redirect the Exchange data to a different location. When redirecting Exchange data, the service pack on the Exchange Server where data is being redirected should be the same as the service pack on the original Exchange Server.

Following are requirements for redirecting Exchange storage group and database restores:

- The storage groups and databases must already exist on the destination server, and must have the same names as the original storage groups or databases.
- The destination server must have the same Organization and Administrative Group name as the source server.
- The destination databases must be configured so that they can be overwritten. See [“Configuring a database in Exchange”](#) on page 858.

You cannot redirect the restore of the following:

- A version of Exchange Server database to a different version of the database. Service packs for both Exchange Servers should also be the same.
- Site Replication Service (SRS) and Key Management Service (KMS). These services are dependent on the computer they reside on; redirection to another computer is not supported and could result in the loss of functionality of these services.

---

**Note:** KMS is not available in Exchange 2003/2007/2010.

---

Before starting the redirected restore job, review information on finding and viewing specific data to restore, as well as for details on restore options and submitting restore jobs.

After completing the restore, it is recommended that a full backup of the restored databases be performed.

See [“About backing up Exchange data”](#) on page 852.

See [“About redirecting Exchange mailbox items”](#) on page 861.

## About redirecting Exchange mailbox items

With Backup Exec, you can restore mailbox items such as mailboxes and public folders to a different mailbox on the same server or to a different location.

You can also restore mailboxes or mailbox items to a .PST, a Microsoft Outlook data file, that is compatible with Microsoft Outlook 2003, 2007, or 2010. The maximum size of the .PST file is 20 GB. If the restore exceeds the size limit, the .PST files are numbered consecutively.

Following are requirements for redirecting Exchange mailbox items:

- The specified mailbox or public folder store must exist.
- Microsoft Outlook 2003, 2007, or 2010 (32-bit only) must be installed on the destination server when you restore to a .PST.
- The logon account must have rights to the destination mailbox.

See [“About restoring Exchange data”](#) on page 857.

## How to prepare for disaster recovery of Exchange Server

A disaster preparation plan is an absolute necessity for restoring Exchange efficiently and effectively in the event of a catastrophic failure. Because Exchange uses Windows security for authentication, disaster recovery of Exchange cannot be separated from the disaster recovery of Windows.

Planning ahead reduces the time needed to recover.

It is critical to build a kit that includes the following items:

- An operating system configuration sheet
- A hard drive partition configuration sheet
- Any RAID configuration
- A hardware configuration sheet
- EISA/MCA configuration disks
- An Exchange configuration sheet
- A Windows emergency repair diskette

To perform the actual recovery, you will need the following items:

- An installed copy of Backup Exec
- The latest full, incremental, and differential backups of the Exchange databases you want to recover.
- The Microsoft Exchange Server Installation CD
- Any service packs that were applied to the original installation

See [“Recovering from a disaster for Exchange ”](#) on page 862.

## Recovering from a disaster for Exchange

This procedure guides you through a complete restoration of Exchange using Backup Exec. You should have already performed all the appropriate preparation.

See [“How to prepare for disaster recovery of Exchange Server”](#) on page 862.

Always log on to Windows using the Administrator account (or an Administrator equivalent) during this procedure. Other requirements include:

- The storage groups and databases must already exist on the destination server, and have the same names as the original storage groups or databases.
- The destination server must have the same Organization and Administrative Group name as the source server.
- The destination databases must be configured so that they can be overwritten. See [“Configuring a database in Exchange”](#) on page 858.

You can use Simplified Disaster Recovery to recover the Exchange Server.

See [“Microsoft Exchange recovery notes”](#) on page 728.

#### **To perform disaster recovery for Exchange**

- 1** Recover the Windows server first.  
Ensure you restore the Exchange Server files that existed on all disk partitions.
- 2** From the Services applet, verify the Microsoft Exchange Information Store service is started.
- 3** Start Backup Exec.
- 4** Catalog the backup sets of the Exchange Server storage groups you want to recover.  
See [“Cataloging backup sets”](#) on page 217.
- 5** Run the Restore Wizard and select the latest full backup set of each storage group or database for restore.  
See [“About searching for and restoring data”](#) on page 229.
- 6** If necessary, select all subsequent incremental storage group backup sets.  
If differential backup sets are to be restored, only the most recent differential storage group backup set need to be selected.
- 7** After completing the restore, it is recommended that a full backup of the restored databases be performed.



# Symantec Backup Exec Agent for Microsoft SharePoint

This appendix includes the following topics:

- [About the Agent for Microsoft SharePoint](#)
- [About installing the Agent for Microsoft SharePoint](#)
- [Requirements for the Agent for Microsoft SharePoint](#)
- [About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010](#)
- [About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0](#)
- [About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0](#)
- [About adding a Microsoft SharePoint server farm to the list of servers](#)
- [About deleting a Microsoft SharePoint server farm from the list of servers](#)
- [About backing up Microsoft SharePoint data](#)
- [About restoring Microsoft SharePoint data](#)
- [Disabling or enabling communication between a Microsoft SharePoint Web server and Backup Exec](#)
- [Viewing SharePoint farm properties](#)

- [Recovering Microsoft SharePoint 2010 data after a disaster](#)
- [Recovering Microsoft SharePoint 2007 data after a disaster](#)

## About the Agent for Microsoft SharePoint

The Agent for Microsoft SharePoint (SharePoint Agent) is an optional, add-on component to Backup Exec. The SharePoint Agent enables network administrators to perform backup and restore operations on any supported Microsoft SharePoint installations that are connected to a network. SharePoint backups can be integrated with network backups without separate administration or dedicated hardware.

The SharePoint Agent supports installations of the following SharePoint products:

- SharePoint Server 2010
- SharePoint Foundation 2010
- SharePoint Server 2007
- Sharepoint Services 3.0
- SharePoint Portal Server 2003
- Windows SharePoint Services 2.0

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010”](#) on page 868.

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0”](#) on page 869.

See [“About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0”](#) on page 869.

## About installing the Agent for Microsoft SharePoint

Before you can back up Microsoft SharePoint server farms, you must install the Agent for Microsoft SharePoint (SharePoint Agent) on the Backup Exec server. The SharePoint Agent is installed as part of the Agent for Applications and Databases.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

See [“Push-installing Backup Exec to remote computers”](#) on page 77.

See [“Requirements for the Agent for Microsoft SharePoint”](#) on page 867.

# Requirements for the Agent for Microsoft SharePoint

The Agent for Microsoft SharePoint (SharePoint Agent) has the following requirements:

- The SharePoint Agent must be installed on the Backup Exec server.
- The Agent for Windows must be installed on each remote SharePoint Server that you want to protect. In addition, the Agent for Windows must be installed on all servers in the server farm.
- You must use a logon account that has local administrative rights to back up and restore SharePoint data. The account should have local administrative rights on the servers where the SharePoint components are installed. For more information on granting permissions on folders in the workspace or backward-compatible document libraries, see your SharePoint Server documentation.
- To back up and restore the Single Sign-on database, you must use a logon account with the appropriate credentials. The credentials must be either the account name or a member of the group that is specified in the Single Sign-on Settings in SharePoint. For more information on Single Sign-on Settings, see your SharePoint Server documentation.
- The logon account that you use to restore content into an existing site collection must have appropriate rights to create objects in that site collection. If you restore into a site collection that does not exist, the logon account becomes the primary site collection owner.
- Internet Information Services (IIS) rights can affect database backups and restores. Ensure that the logon account that you use for backup and restore has rights to access the IIS sites. Integrated Windows Security should be enabled within the IIS rights.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

# About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010

The Agent for Microsoft SharePoint includes support for Microsoft Office SharePoint Server 2010 and Windows SharePoint Foundation 2010.

SharePoint Server 2010 offers new metadata features including tags, social bookmarks, and content ratings. These new types of metadata are stored in the service applications that reside outside of the content database. For example, enterprise managed tags reside in the Managed Metadata Service application. You should make sure to back up all of your service applications to ensure that all metadata is protected.

Any metadata that is stored outside of the content database cannot be restored using Granular Recovery Technology (GRT). You can, however, use GRT to restore SharePoint data with metadata attached to it. As long as the metadata resides in the same service application, SharePoint maintains the link between the data and the metadata.

You can back up and restore the following types of SharePoint Server 2010 data:

- Web applications and their associated databases
- Individual documents and any pictures that are contained in libraries
- Sites and subsites  
Individual objects and their versions can be restored from full database backups.
- Lists and list items  
Individual objects and their versions can be restored from full database backups.
- Configuration database  
A configuration database contains all of the configuration information for the entire SharePoint Server farm. Use caution when you restore this database. Any changes that you make to the farm topology before you restore from the backup are lost. The configuration database can only be restored to its original location.
- Service applications

See [“Recovering Microsoft SharePoint 2010 data after a disaster”](#) on page 877.

## About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0

The Agent for Microsoft SharePoint includes support for Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0.

You can back up and restore the following types of SharePoint Server 2007 data:

- Web applications and their associated databases  
Symantec recommends that you restore all Web application databases together to preserve the topology.
- Individual documents that are contained in libraries.
- Sites and subsites  
Individual objects and their versions can be restored from full database backups.
- Lists and list items  
Individual items and their versions can be restored from full database backups.
- Configuration database  
A configuration database contains all of the configuration information for the entire SharePoint Server farm. Use caution when you restore this database. Any changes that you make to the farm topology before you restore from the backup are lost. The configuration database can only be restored to its original location.
- Single Sign-on databases  
Single Sign-on databases can only be restored to their original locations.
- Shared Service Providers  
A Shared Service Provider is a grouping of shared services and related shared resources.

See [“Recovering Microsoft SharePoint 2007 data after a disaster”](#) on page 881.

## About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0

The Agent for Microsoft SharePoint includes support for Microsoft Office SharePoint Portal Server 2003 and Windows SharePoint Services 2.0.

You can back up and restore the following types of SharePoint Portal Server 2003 data:

- Portal sites and their associated databases  
Each portal site has a minimum of three databases, including Content databases, Services databases, and User Profile databases. Symantec recommends that you restore these databases together to preserve the topology.
- Windows SharePoint Services sites and their associated databases
- Individual documents and pictures that are contained in document or picture libraries
- Sites and subsites  
Individual objects and their versions can be restored from full database backups.
- Lists and list items  
Individual objects can be restored from full database backups.
- Configuration database  
A configuration database contains all of the configuration information for the entire SharePoint Server farm. Use caution when you restore this database. Any changes that you make to the farm topology before you restore from the backup are lost. The configuration database can be restored only to its original location.
- Single Sign-on databases  
Single Sign-on databases can be restored only to their original location.

---

**Note:** Backup Exec does not support the redirected restore of individual items from a SharePoint Portal Server 2003 or a Windows SharePoint Services 2.0 content database to another SharePoint site. Individual items can be restored only to their original locations or to a file path.

---

## About adding a Microsoft SharePoint server farm to the list of servers

Before you can back up Microsoft SharePoint data, you must add a SharePoint server farm to the list of servers on the **Backup and Restore** tab. If you select to add a single SharePoint server, Backup Exec adds the entire farm to which it belongs.

See [“About the list of servers”](#) on page 157.

See [“Adding servers to the list of servers”](#) on page 158.

## About deleting a Microsoft SharePoint server farm from the list of servers

If a Microsoft SharePoint server farm is no longer in use or is no longer valid, you can remove it from the list of servers on the **Backup and Restore** tab.

---

**Note:** If Backup Exec is installed on the same server that is used as a Web server in a farm, you cannot delete that farm.

---

See [“Removing servers from the list of servers”](#) on page 159.

## About backing up Microsoft SharePoint data

The Agent for Microsoft SharePoint enables network administrators to perform backup operations on any Microsoft SharePoint installations that are connected to a network. SharePoint backups can be integrated with network backups without separate administration or dedicated hardware.

For more information about the specific types of SharePoint content that you can back up, see the following topics:

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010”](#) on page 868.

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0”](#) on page 869.

See [“About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0”](#) on page 869.

Backup Exec's dynamic inclusion feature automatically protects any new resources that were added after a backup job was created. If Backup Exec discovers that you added a new resource as a child to a protected resource, it automatically backs up the new resource. Because the backup job may include new resources, the job may require more storage space and more time to run than you anticipated.

You can set backup job default options for all SharePoint backup jobs. Each time you create a backup job, the job uses the default options unless you change the options for that particular job.

See [“Setting default backup job settings”](#) on page 456.

See [“Backing up data”](#) on page 163.

See [“Microsoft SharePoint backup options”](#) on page 872.

See [“Editing backups”](#) on page 170.

## Microsoft SharePoint backup options

The following options are available for Microsoft SharePoint backup jobs. These options appear when you select the **Microsoft SharePoint** option on the **Backup Job Defaults** dialog box and on the **Backup Options** dialog box for a backup job.

See [“Setting default backup job settings”](#) on page 456.

See [“Backing up data”](#) on page 163.

See [“About backing up Microsoft SharePoint data”](#) on page 871.

Table G-1 SharePoint backup options

Item	Description
<b>Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual items from the database backup</b>	Enables the restore of individual documents, images, sites, subsites, lists, and list items from database backups. You must have a current version of the Agent for Windows on the SharePoint server when you run the GRT-enabled backup job.  See <a href="#">“How to restore individual items by using Granular Recovery Technology”</a> on page 543.
<b>Release the lock on the SharePoint farm topology if it is set (SharePoint 2003 only)</b>	Releases the lock on the SharePoint farm topology before you run the backup or restore operation. Because another application may have locked the topology, you should check with your SharePoint administrator before you select this option.
<b>Perform a consistency check before the backup of any Microsoft SQL databases used by Microsoft SharePoint</b>	Runs a full consistency check (including indexes) of the Microsoft SQL databases that Microsoft SharePoint uses before you back up the databases.
<b>Continue with the backup if consistency check fails</b>	Continues with the backup operation even if the consistency check fails.

## About restoring Microsoft SharePoint data

The Agent for Microsoft SharePoint lets you restore Microsoft SharePoint server farms and servers as well as other types of SharePoint content. You can restore items to their original location or you can redirect the restore to a new location.

See [“About searching for and restoring data”](#) on page 229.

You can redirect a restore job to an existing site on a Web server in a farm. SharePoint file-based data, such as documents and images that have been uploaded to a document library or are attached to list items, can be redirected to a new location. If you use Windows SharePoint Server 3.0 or Windows SharePoint Foundation 2010, you can redirect the restore of one site to another site. When you redirect a restore from one site to another site, the restored items inherit the security permissions of the parent item to which they are restored.

---

**Note:** Backup Exec does not support the redirected restore of individual items from a SharePoint Portal Server 2003 or a Windows SharePoint Services 2.0 content database to another SharePoint site. Individual items can be restored only to their original locations or to a file path.

---

Before you redirect the restore of SharePoint 2003 document library data, you must install the SharePoint Portal Server software on the server to which you want to redirect the restore. If any of the folders in the original document library do not exist in the destination document library, they are created during the restore.

Backup Exec also lets you restore individual documents, images, sites, subsites, lists, and list items from SharePoint database backups. To restore individual items from SharePoint database backups, you must ensure that the following Microsoft SharePoint option is selected during the backup job:

**Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual objects from the database backup**

---

**Note:** Backup Exec does not support the restore of granular items from compressed databases or encrypted databases.

---

You should keep in mind the following things when you restore SharePoint data:

- Individual SharePoint documents are always restored to SharePoint document libraries as checked out.  
The documents are checked out using the same credentials as the logon account that you use for the restore. The documents must be checked in or published by that user before other users can use them.
- You can restore SharePoint databases to an alternate SQL instance.  
You can attach a database to a new Web application, for example. To bring the databases online after you complete a redirected restore job, verify that the **Yes, restore over existing databases** option is selected. When you restore Web applications or Windows SharePoint Services sites, this option also

reestablishes the link between the restored databases and their corresponding sites.

- If you try to restore over a document that is checked out, the restore may fail. The restore fails if the document is checked out to a user that differs from the logon account credentials that are used for the restore.

---

**Caution:** When you restore SharePoint Portal document library data, any documents that exist in the selected destination and that have the same name as the documents being restored may be overwritten. You can select whether they should be overwritten in the properties for the restore job.

---

For more information about the different types of SharePoint content, see the Microsoft SharePoint documentation.

For more information about the specific types of SharePoint content that you can restore, see the following topics:

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2010 and Windows SharePoint Foundation 2010”](#) on page 868.

See [“About using the Agent for Microsoft SharePoint with SharePoint Server 2007 and Windows SharePoint Services 3.0”](#) on page 869.

See [“About using the Agent for Microsoft SharePoint with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0”](#) on page 869.

See [“Microsoft SharePoint restore options ”](#) on page 874.

## Microsoft SharePoint restore options

When you restore Microsoft SharePoint data, you should consider the following versioning and security options.

See [“About searching for and restoring data”](#) on page 229.

See [“About restoring Microsoft SharePoint data”](#) on page 872.

**Table G-2** SharePoint restore options

Item	Description
<b>Restore only the most recent version of an item</b>	Restores only the most recent version of an item.

Table G-2 SharePoint restore options (*continued*)

Item	Description
<b>If versioning is enabled at the destination</b>	<p>Lets you choose from the following options if versioning is enabled on the destination to which you want to restore an individual item:</p> <ul style="list-style-type: none"> <li>■ <b>Add the item as a new version</b> Backup Exec restores the existing item as a new version, which makes it the most recent version of the existing item.</li> <li>■ <b>Skip if the item exists</b> Backup Exec does not restore the item if an identical item exists in the restore destination. Backup Exec notes that the file was skipped in the job log.</li> <li>■ <b>Restore over existing items</b> Backup Exec replaces the existing item with the restored item.</li> </ul>
<b>If versioning is not enabled at the destination</b>	<p>Lets you choose from the following options if versioning is not enabled on the destination to which you want to restore an individual item:</p> <ul style="list-style-type: none"> <li>■ <b>Skip if the item exists</b> Backup Exec does not restore the item if an identical item exists in the restore destination. Backup Exec notes that the file was skipped in the job log.</li> <li>■ <b>Restore over existing items</b> Backup Exec replaces the existing item with the restored item.</li> </ul>
<b>Restore site list and item level permissions</b>	<p>Restores any applicable security information with the item. You can restore different levels of security based on the SharePoint item that you restore:</p> <ul style="list-style-type: none"> <li>■ Sites - User and SharePoint Group information and security ACL are restored for top-level sites</li> <li>■ Subsites - Security ACL is restored</li> <li>■ Lists - Security ACL and other security-related information is restored</li> </ul>

# Disabling or enabling communication between a Microsoft SharePoint Web server and Backup Exec

Backup Exec communicates with the Web servers that participate in Microsoft SharePoint server farms to discover the farm topology. This process may take some time if Backup Exec attempts to communicate with a Web server that is unavailable. If you know that a particular Web server in a farm is unavailable for a period of time, you can disable the communication between the Web server and Backup Exec.

**To disable or enable communication between a SharePoint Web server and Backup Exec**

- 1 On the **Backup and Restore** tab, double-click the SharePoint server farm to which the Web server belongs.
- 2 In the left pane, click **Properties**.  
See [“SharePoint farm properties”](#) on page 876.
- 3 To prevent Backup Exec from communicating with a SharePoint Web server, clear the check box next to that Web server’s name. If the SharePoint Web server is now available to communicate with Backup Exec, select the check box next to the Web server’s name.

## Viewing SharePoint farm properties

You can view properties for any SharePoint farm that you monitor with Backup Exec. Backup Exec displays general and system information about the server.

See [“SharePoint farm properties”](#) on page 876.

You can also enable or disable communication between a SharePoint web server and Backup Exec from the SharePoint farm properties dialog.

See [“Disabling or enabling communication between a Microsoft SharePoint Web server and Backup Exec”](#) on page 876.

**To view SharePoint farm properties**

- 1 On the **Backup and Restore** tab, double-click the SharePoint farm whose properties you want to view.
- 2 In the left pane, click **Properties**.

## SharePoint farm properties

You can view the properties of any SharePoint farms that you back up.

See [“Viewing SharePoint farm properties”](#) on page 876.

**Table G-3** SharePoint farm properties

Item	Description
SharePoint farm name	Displays the name of the SharePoint farm.
Description	Lets you enter a unique description to identify the farm in Backup Exec. The description is optional.
Logon account	Lists the logon account that Backup Exec uses to access the farm.
Add/Edit	Lets you add a new logon account or edit an existing logon account.  See <a href="#">“Logon Account Management options”</a> on page 506.
Web Servers	Lists the web servers that belong to the farm. You can enable or disable communication between the web servers and Backup Exec.  See <a href="#">“Disabling or enabling communication between a Microsoft SharePoint Web server and Backup Exec”</a> on page 876.

## Recovering Microsoft SharePoint 2010 data after a disaster

You can use the Agent for Microsoft SharePoint to recover a Microsoft SharePoint server after a hard drive failure. Before you recover SharePoint data, you must recover the SharePoint server's operating system.

You can use Backup Exec's Simplified Disaster Recovery Option or you can manually recover the server's operating system.

See [“About Simplified Disaster Recovery”](#) on page 704.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

After the Windows server is recovered, you can recover SharePoint 2010 data. Complete the actions in the table in successive order to recover the SharePoint data.

**Table G-4** To recover SharePoint 2010 data after a disaster

Step	Action	Notes
Step 1	Recover the master database and the model database for the SQL instances that SharePoint uses. You must perform this step if you manually recovered the server's operating system.	Skip this step if you used Backup Exec's Simplified Disaster Recovery Option to recover the server's operating system.  See <a href="#">"About recovering SQL manually"</a> on page 832.
Step 2	Inventory the media to be recovered.	See <a href="#">"Inventorying a storage device"</a> on page 423.
Step 3	Catalog the media to be recovered.	See <a href="#">"Cataloging a storage device"</a> on page 424.
Step 4	Restore the msdb databases for any SQL instances that SharePoint uses.	Select the backup sets that contain the msdb databases for the SQL instances that SharePoint uses.  Configure the following Microsoft SQL restore options:  <ul style="list-style-type: none"> <li>■ Select <b>Leave the database ready to use; additional transaction logs or differential backups cannot be restored.</b></li> <li>■ Select <b>Overwrite existing databases.</b></li> </ul> See <a href="#">"About searching for and restoring data"</a> on page 229.
Step 5	Restore all Web applications.	Select the backup sets for all SharePoint Web applications.  Select <b>Yes, restore over existing databases.</b>  See <a href="#">"About searching for and restoring data"</a> on page 229.

**Table G-4** To recover SharePoint 2010 data after a disaster (*continued*)

Step	Action	Notes
Step 6	Restore Shared Services Applications databases.	<p>Restore the following Shared Services Applications databases:</p> <ul style="list-style-type: none"><li>■ Business Data Connectivity Service</li><li>■ Managed Metadata Service</li><li>■ PerformancePoint Service Application</li><li>■ Search Service Application</li><li>■ Secure Store Service</li><li>■ User Profile Service Application</li><li>■ Web Analytics Service Application</li><li>■ Word Automation Services</li><li>■ Services\State Services\Service DB 1</li></ul> <p>Select <b>Yes, restore over existing databases</b>.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p> <p><b>Note:</b> Some of the remaining restore jobs may fail because communication with the SharePoint server has not been fully established yet. This behavior is expected. Proceed with the recovery process until all steps are complete.</p>

**Table G-4** To recover SharePoint 2010 data after a disaster (*continued*)

Step	Action	Notes
Step 7	Restore search services.	Restore the following services: <ul style="list-style-type: none"> <li>■ SharePoint Foundation Help Search\Search Instance\Index Files 1</li> <li>■ Search-DB 1</li> </ul> Select <b>Yes, restore over existing databases</b> . See <a href="#">“About searching for and restoring data”</a> on page 229. <b>Note:</b> You may get a message in the job log to restart your computer. You can ignore the message.
Step 8	Restore the SharePoint Configuration V4-DB resource.	Select the backup sets for the SharePoint Configuration V4-DB resource. Select <b>Yes, restore over existing databases</b> . See <a href="#">“About searching for and restoring data”</a> on page 229.
Step 9	Restart the SharePoint server.	After the restore job is complete, restart the SharePoint server. Then proceed to the next step.
Step 10	Restore remaining SharePoint resources.	Select the backup sets for the SharePoint Global Settings resources, if necessary. See <a href="#">“About searching for and restoring data”</a> on page 229.

**Table G-4** To recover SharePoint 2010 data after a disaster (*continued*)

Step	Action	Notes
Step 11	Back up the SharePoint server.	When the disaster recovery is complete, Symantec recommends that you perform a backup job as soon as possible.  See <a href="#">“About backing up data”</a> on page 155.

## Recovering Microsoft SharePoint 2007 data after a disaster

You can use the Agent for Microsoft SharePoint to recover a Microsoft SharePoint server after a hard drive failure. Before you recover SharePoint data, you must recover the SharePoint server's operating system.

You can use Backup Exec's Simplified Disaster Recovery Option or you can manually recover the server's operating system.

See [“About Simplified Disaster Recovery”](#) on page 704.

See [“About manual disaster recovery of Windows computers”](#) on page 637.

After the Windows server is recovered, you can recover SharePoint 2007 data. Complete the actions in the table in successive order to recover the SharePoint data.

**Table G-5** To recover SharePoint 2007 data after a disaster

Step	Action	Notes
Step 1	Recover the master database and the model database for the SQL instances that SharePoint uses. You must perform this step if you manually recovered the server's operating system.	Skip this step if you used Backup Exec's Simplified Disaster Recovery Option to recover the server's operating system.  See <a href="#">“About recovering SQL manually”</a> on page 832.
Step 2	Inventory the media to be recovered.	See <a href="#">“Inventorying a storage device”</a> on page 423.

**Table G-5** To recover SharePoint 2007 data after a disaster (*continued*)

Step	Action	Notes
Step 3	Catalog the media to be recovered.	See <a href="#">“Cataloging a storage device”</a> on page 424.
Step 4	Restore the msdb databases for any SQL instances that SharePoint uses.	<p>Select the backup sets that contain the msdb databases for the SQL instances that SharePoint uses.</p> <p>Configure the following Microsoft SQL restore options:</p> <ul style="list-style-type: none"> <li>■ Select <b>Leave the database ready to use; additional transaction logs or differential backups cannot be restored.</b></li> <li>■ Select <b>Overwrite existing databases.</b></li> </ul> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>
Step 5	Restore SharePoint farm components.	<p>Select the backup sets for the following SharePoint components:</p> <ul style="list-style-type: none"> <li>■ Help Search service</li> <li>■ WSS Administration</li> <li>■ Shared Service web application (if applicable)</li> </ul> <p>Select <b>Yes, restore over existing databases.</b></p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>
Step 6	Restore SharePoint web applications.	<p>Select the backup sets for any SharePoint web applications.</p> <p>See <a href="#">“About searching for and restoring data”</a> on page 229.</p>

**Table G-5** To recover SharePoint 2007 data after a disaster (*continued*)

Step	Action	Notes
Step 7	Restore the SharePoint Configuration V3-DB resource.	Select the backup sets for the SharePoint Configuration V3-DB resource.  Select <b>Yes, restore over existing databases</b> .  See <a href="#">“About searching for and restoring data”</a> on page 229.
Step 8	Restart the SharePoint server.	After the restore job is complete, restart the SharePoint server. Then proceed to the next step.
Step 9	Restore remaining SharePoint resources.	Select the backup sets for the SharePoint Global Settings and Single Sign-on database resources, if necessary.  See <a href="#">“About searching for and restoring data”</a> on page 229.
Step 10	Back up the SharePoint server.	When the disaster recovery is complete, Symantec recommends that you perform a backup job as soon as possible.  See <a href="#">“About backing up data”</a> on page 155.



# Symantec Backup Exec Agent for Oracle on Windows or Linux Servers

This appendix includes the following topics:

- [About the Backup Exec Oracle Agent](#)
- [About installing the Oracle Agent](#)
- [Configuring the Oracle Agent on Windows computers and Linux servers](#)
- [About authentication credentials on the Backup Exec server](#)
- [About Oracle instance information changes](#)
- [About backing up Oracle databases](#)
- [About restoring Oracle resources](#)
- [Troubleshooting the Oracle Agent](#)

## About the Backup Exec Oracle Agent

The Symantec Backup Exec Agent for Oracle on Windows or Linux Servers (Oracle Agent) uses Oracle's Recovery Manager (RMAN) to protect Oracle databases. RMAN is a tool that manages the backup and restore and recovery of Oracle databases.

The following features are available with the Oracle Agent:

- The ability to initiate backup and restore operations from Backup Exec or from the RMAN console as a Database Administrator (DBA).

Operations that the DBA performs on the RMAN console are referred to as DBA-initiated operations. You should refer to your Oracle documentation for information about RMAN.

- Multiple data stream support for increased performance during backup and restore operations.
- RMAN recovery catalog support to manage the backup, restore, and recovery of Oracle databases.
- Oracle Real Application Cluster (RAC) support.

The following are not supported:

- Tivoli Storage Manager (TSM) devices as storage for Oracle backup jobs.
- The Oracle Management Server.

See [“About installing the Oracle Agent”](#) on page 886.

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

## About installing the Oracle Agent

The Oracle Agent is installed as part of the Agent for Applications and Databases and can protect local or remote Oracle instances.

To protect local or remote Oracle instances, you must install the following Backup Exec options:

- Backup Exec Agent for Windows on remote Windows computers.

---

**Note:** If you upgrade a previous version of the Agent for Windows on an Oracle server, you must restart the Oracle server after the upgrade. Backup Exec jobs cannot complete successfully until you restart the Oracle server.

---

See [“About installing the Agent for Windows”](#) on page 83.

- Backup Exec Agent for Linux on remote Linux computers.  
See [“About installing the Agent for Linux”](#) on page 1075.
- Backup Exec Oracle Agent on the Backup Exec server.  
See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

# Configuring the Oracle Agent on Windows computers and Linux servers

Before you can back up or restore Oracle databases, you must do the following:

**Table H-1** Configuring the Oracle Agent on Windows computers and Linux servers

Step	Action
Step 1	Configure information about the Oracle instances for the Oracle Agent.  See <a href="#">“Configuring an Oracle instance on Windows computers”</a> on page 888.  See <a href="#">“Configuring an Oracle instance on Linux servers”</a> on page 893.

**Table H-1** Configuring the Oracle Agent on Windows computers and Linux servers *(continued)*

Step	Action
Step 2	<p>Enable database access for the Backup Exec server.</p> <p>Whenever Oracle instance information changes or a new configuration is added, you must update the Backup Exec Agent Utility. If credential information is not updated, is incorrect, or the server is down, the error "Unable to attach to a resource..." may appear when you run a backup job. If this message appears, you must bring the server online and configure the information.</p> <p>For Oracle RAC, run the Backup Exec Agent Utility on each node and add information about the instances. When Oracle RAC nodes are added or removed, you must enter information about any changes to instances in the Backup Exec Agent Utility.</p> <p><b>Note:</b> When you use the Backup Exec Agent Utility, the user account with which you are logged on should be a member of the Oracle DBA group.</p> <p>You must have administrator privileges to run the Backup Exec Agent Utility.</p> <p>See <a href="#">"Enabling database access for Oracle operations on Windows computers"</a> on page 892.</p> <p>See <a href="#">"Enabling database access for Oracle operations on Linux servers"</a> on page 896.</p>
Step 3	<p>Set authentication credentials for Oracle.</p> <p>See <a href="#">"About authentication credentials on the Backup Exec server"</a> on page 897.</p>

## Configuring an Oracle instance on Windows computers

You can use the Backup Exec Agent Utility to configure information about the Oracle instances for the Oracle Agent on Windows computers.

### To configure an Oracle instance on Windows computers

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 On the **Oracle** tab, click **New**.

Any instances that currently exist on the computer appear on the tab.

- 3 Complete the appropriate options.

See [“Oracle Agent Configuration options”](#) on page 889.

- 4 Click **OK**.

### Oracle Agent Configuration options

You can set the following Oracle Agent Configuration options.

See [“Configuring an Oracle instance on Windows computers”](#) on page 888.

See [“Editing an Oracle instance on Windows computers”](#) on page 891.

**Table H-2** Oracle Agent Configuration options

Item	Description
<b>Local instance name</b>	<p>Displays the name of the Oracle instance. If you edit an instance, you cannot change the instance name.</p> <p>For Oracle RAC nodes, enter the fully qualified domain name of each physical node.</p> <p>The fully qualified domain name of the node appears in the list of servers on the <b>Backup and Restore</b> tab.</p> <p>The name is in the format RAC-&lt;dbname&gt;-&lt;dbid&gt;, where dbname is the database name, and dbid is the database ID.</p>
<b>User name</b>	<p>Displays the user name for the Oracle instance.</p> <p>If the credentials for the Oracle instance change, you must enter a user with SYSDBA rights to the Oracle instance.</p> <p>For Oracle RAC nodes, enter the same set of credentials for all of the nodes.</p>
<b>Password</b>	Displays the password for the Oracle instance user name.
<b>Confirm password</b>	Displays the password again to confirm it.

**Table H-2** Oracle Agent Configuration options (*continued*)

Item	Description
<b>Use recovery catalog</b>	Indicates that you plan to use the Oracle recovery catalog.  The Oracle Agent supports the use of the RMAN recovery catalog to manage the backup, restore, and recovery of Oracle databases. If you choose not to use a recovery catalog, RMAN uses the source database control file as the sole repository of metadata.
<b>TNS name</b>	Displays the Oracle Net Service name.
<b>User name</b>	Displays the user name for the Oracle recovery catalog.
<b>Password</b>	Displays the password for the Oracle recovery catalog.
<b>Confirm password</b>	Displays the password for the recovery catalog again to confirm it.
<b>Backup Exec server name or IP address</b>	Displays the name or IP address of the Backup Exec server where you want to send the DBA-initiated backup jobs.  You must use the same form of name resolution for all operations.
<b>Job template name</b>	Displays the name of the Backup Exec job template that you want the DBA-initiated job to use for backup and restore operations. You create the job template on the DBA-initiated Job Settings dialog box on the Backup Exec server. If you do not specify a job template, the default job template is used.  See <a href="#">“Creating a template for DBA-initiated jobs”</a> on page 485.

## Viewing an Oracle instance on Windows computers

You can use the Backup Exec Agent Utility to view information about the Oracle instances for the Oracle Agent on Windows servers.

### To view an Oracle instance on Windows computers

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.
- 2 On the **Oracle** tab, view the instances that currently exist on the computer.  
See [“Oracle options for the Backup Exec Agent Utility”](#) on page 890.
- 3 Click **OK**.

### Oracle options for the Backup Exec Agent Utility

You can set the following Oracle options for the Backup Exec Agent Utility.

See “[Viewing an Oracle instance on Windows computers](#)” on page 890.

**Table H-3** Oracle options for the Backup Exec Agent Utility

Item	Description
<b>Instance</b>	Displays the name of the Oracle instance.
<b>User Name</b>	Displays the user name for the Oracle instance.
<b>Recovery Catalog</b>	Displays the name of the recovery catalog.
<b>Backup Exec Server</b>	Displays the name or IP address of the Backup Exec server where you want to send the DBA-initiated backup jobs.
<b>Job Template</b>	Displays the name of the DBA-initiated template.  See “ <a href="#">About performing a DBA-initiated backup job for Oracle</a> ” on page 902.
<b>New</b>	Lets you add an Oracle instance.
<b>Edit</b>	Lets you revise an Oracle instance.
<b>Delete</b>	Lets you remove an Oracle instance.

## Editing an Oracle instance on Windows computers

You can use the Backup Exec Agent Utility to revise information about the Oracle instances for the Oracle Agent on Windows computers.

### To edit an Oracle instance on Windows computers

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 On the **Oracle** tab, click **Edit**.

Any instances that currently exist on the computer appear on the tab.

- 3 Edit the appropriate options.

See “[Oracle Agent Configuration options](#)” on page 889.

- 4 Click **OK**.

## Deleting an Oracle instance on Windows computers

You can use the Backup Exec Agent Utility to remove an Oracle instance for the Oracle Agent on Windows computers.

### To delete an Oracle instance on Windows computers

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 On the **Oracle** tab, click **Delete**.

Any instances that currently exist on the computer appear on the tab.

- 3 Click **OK**.

## Enabling database access for Oracle operations on Windows computers

You can use the Backup Exec Agent Utility to enable database access for the Windows computer after you configure an Oracle instance.

See [“About backing up Oracle databases”](#) on page 900.

See [“About backing up Oracle RAC databases”](#) on page 901.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Setting default backup job settings”](#) on page 456.

### To enable database access for Oracle operations on Windows computers

- 1 On the computer on which the Agent for Windows is installed, on the taskbar, click **Start > All Programs > Symantec Backup Exec > Backup Exec 2012 Backup Exec Agent Utility**.

When the Backup Exec Agent Utility is running, an icon appears in the system tray. You can double-click this icon to view the utility.

- 2 On the **Database Access** tab, complete the appropriate options.

See [“Database access options for the Backup Exec Agent Utility”](#) on page 743.

- 3 Click **OK**.

- 4 For Oracle RAC installations, type the fully qualified domain name that you want to publish to.

The Backup Exec server that you publish to lists the RAC databases in the list of servers on the **Backup and Restore** tab.

If you do not enter a fully qualified domain name to publish to, the RAC databases are not in the list of servers.

See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.

- 5 On the Backup Exec server, add the name of the Oracle server and the user name that you enabled for database access to the Backup Exec server's list of authentication credentials.

See [“About authentication credentials on the Backup Exec server”](#) on page 897.

## Configuring an Oracle instance on Linux servers

You can use the Backup Exec Agent Utility to configure information about the Oracle instances for the Oracle Agent on Linux servers.

### To configure an Oracle instance on Linux servers

- 1 On the Linux server on which the Oracle instances are installed, open a Terminal window.
- 2 Change to the following directory:  
**cd /opt/VRTSralus/bin**
- 3 Start the Backup Exec Agent Utility:  
**./AgentConfig**
- 4 Type **2** to select Configure Oracle instance information, and then press **Enter**.
- 5 Type **1** to select the Add a new Oracle Instance option, and then press **Enter**.
- 6 Enter the name of the Oracle instance in upper case characters.  
For example, ORACLENAME.

**7** Enter the user name for the Oracle instance.

If the credentials for the Oracle instance are changed, you must update the credentials in this field. For Oracle RAC nodes, enter the same set of credentials for all of the nodes.

When you use the Backup Exec Agent Utility to enter the Oracle credentials for an instance, the credentials cannot be verified if the user account with which you are logged on is a member of the Oracle DBA group. If the credentials are incorrect, the error "Unable to attach to a resource..." may appear when you run a backup job.

**8** To display the Oracle database in a Backup Exec server's list of servers on the **Backup and Restore** tab, type the Backup Exec server name or IP address to which you want the remote computer to publish to.

**9** When prompted, specify if you want to use a recovery catalog.

The Oracle Agent supports the use of the RMAN recovery catalog to manage the backup, restore, and recovery of Oracle databases. If you choose not to use a recovery catalog, RMAN uses the source database control file as the sole repository of metadata.

If you specify a recovery catalog, any database that you want to back up must be registered in the recovery catalog before you can run backup jobs from the Backup Exec server.

**10** To use a recovery catalog, type the recovery catalog name and a user name and password for the recovery catalog.

**11** To use a customized DBA-initiated job settings template, type the name of the template.

See "[Creating a template for DBA-initiated jobs](#)" on page 485.

**12** Do one of the following:

To commit the new entry to the configuration file Type **Y**, and then press **Enter**.

To cancel this entry Type **N**, and then press **Enter**.

## Viewing an Oracle instance on Linux servers

You can use the Backup Exec Agent Utility to view information about the Oracle instances for the Oracle Agent on Linux servers.

The following information is listed:

- Name of the instance
- Logon name for the instance
- IP address of the default Backup Exec server name for DBA-initiated operations
- Name of the DBA-initiated job template

#### To view an Oracle instance on Linux servers

- 1 On the Linux server on which the Oracle instances are installed, open a Terminal window.
- 2 Change to the following directory:  

```
cd /opt/VRTSralus/bin
```
- 3 Start the Backup Exec Agent Utility:  

```
./AgentConfig
```
- 4 Type 4.

## Editing an Oracle instance on Linux servers

You can use the Backup Exec Agent Utility to revise information about the Oracle instances for the Oracle Agent on Linux servers.

#### To edit an Oracle instance on Linux computers

- 1 On the Linux server on which the Oracle instances are installed, open a Terminal window.
- 2 Change to the following directory:  

```
cd /opt/VRTSralus/bin
```
- 3 Start the Backup Exec Agent Utility:  

```
./AgentConfig
```
- 4 Type 2 to select Configure Oracle Instance Information, and then press **Enter**.  
Any instances that currently exist on the computer are discovered.
- 5 Type 2.
- 6 Follow the prompts.

## Deleting an Oracle instance on Linux servers

You can use the Backup Exec Agent Utility to remove an Oracle instance for the Oracle Agent on Linux servers.

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

#### To delete an Oracle instance for the Oracle Agent on Linux servers

- 1 On the Linux server on which the Oracle instances are installed, open a Terminal window.
- 2 Change to the following directory:  

```
cd /opt/VRTSralus/bin
```
- 3 Start the Backup Exec Agent Utility:  

```
./AgentConfig
```
- 4 Type **2** to select Configure Oracle Instance Information, and then press **Enter**. Any instances that currently exist on the computer are discovered.
- 5 Type **3**.
- 6 Follow the prompts.

## Enabling database access for Oracle operations on Linux servers

You can use the Backup Exec Agent Utility to enable database access for the Linux server after you configure an Oracle instance.

See [“Setting authentication credentials on the Backup Exec server for Oracle operations”](#) on page 898.

See [“About backing up Oracle databases”](#) on page 900.

See [“About backing up Oracle RAC databases”](#) on page 901.

See [“Creating a template for DBA-initiated jobs”](#) on page 485.

See [“Setting default backup job settings”](#) on page 456.

#### To enable database access for Oracle operations on Linux servers

- 1 On the Linux server on which the Oracle instances are installed, open a Terminal window.
- 2 Change to the following directory:  

```
cd /opt/VRTSralus/bin
```
- 3 Start the Backup Exec Agent Utility:  

```
./AgentConfig
```
- 4 Type **1** to select Configure database access, and then press **Enter**.

- 5 Type the user name that is in the beoper group on the Linux system.

See [“About the Backup Exec operators group for the Agent for Linux”](#) on page 1078.

If the authentication fails when the Oracle resources are backed up, the backup job fails. If the authentication fails when you browse the backup sets for a restore job, then the backup sets become unavailable, and you must run a DBA-initiated restore job to restore data.

- 6 Type the password for this logon account, and then confirm it.

The logon credentials are not stored on this computer.

- 7 When prompted, specify if you want to use a custom port to connect to the Backup Exec server communications between this computer and the Backup Exec server during Oracle operations.

Port 5633 is used by default. If you change the port number on this computer, you must also change it on the Backup Exec server, and then restart the Backup Exec Job Engine Service on the Backup Exec server. If a Windows firewall is enabled, you must add this port as an exception.

See [“Changing network and security options”](#) on page 470.

- 8 Do one of the following:

To commit the Oracle operation settings to the configuration file      Type **Y**, and then press **Enter**.

To cancel this entry      Type **N**, and then press **Enter**.

## About authentication credentials on the Backup Exec server

You must add the Oracle fully qualified domain name and the logon account name to the Backup Exec server’s list of Oracle servers and authentication credentials. The Backup Exec server has database access for operations on Oracle instances that are included in the authentication list. Before you start any backup or restore operations, on the computer on which the Oracle instances are installed, ensure that you use the Backup Exec Agent Utility to configure instance information and database access.

The logon account name must have administrative rights to the Oracle server. If the user name is incorrect or is not provided, or if it does not have the appropriate rights, then you cannot perform Oracle backup or restore operations to that computer.

---

**Note:** For Oracle RAC nodes, enter the fully qualified domain name for the logon account name. You can view the fully qualified domain name of the node in the list of servers on the **Backup and Restore** tab. It is in the form RAC-<database name>-<database ID>.

---

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

See [“Setting authentication credentials on the Backup Exec server for Oracle operations”](#) on page 898.

See [“Deleting an Oracle server from the Backup Exec server’s list of authentication credentials”](#) on page 899.

## Setting authentication credentials on the Backup Exec server for Oracle operations

You must add the Oracle server to the list so that the Backup Exec server has database access for operations.

See [“About authentication credentials on the Backup Exec server”](#) on page 897.

See [“About Oracle instance information changes ”](#) on page 900.

### To set authentication credentials on the Backup Exec server for Oracle operations

- 1 Click the Backup Exec button, and then select **Configuration and Settings** and then click **Backup Exec Settings**.
- 2 In the left pane, click **Oracle**.
- 3 Enter the name of the Oracle server on which the instance is installed.

The name of the Oracle server should match the name of the server that lists the Oracle resource. Symantec recommends that you enter the fully qualified domain name. For example, Servername.domain.com is the fully qualified domain name and Servername is the NETBIOS name. For Oracle RAC nodes, enter the RAC-<database name>-<database ID> for each node in the list.

- 4 Click **Add**.

**5** To add the logon account name, do one of the following:

Click the arrow      Select the logon account name that you want to add.

Click <new logon account>      Enter the appropriate options.

See [“Add Logon Credentials options”](#) on page 508.

Use the same logon account format that you use when you enter the logon account name on the **Database Access** tab in the Backup Exec Agent Utility. For example, if you entered Domainname\Username on the Backup Exec Agent Utility, use that same format on the list of authentication credentials.

**6** Click **OK**.

## Oracle job settings options

You can add the Oracle fully qualified domain name and the logon account name to the Backup Exec server’s list of Oracle servers and authentication credentials. See [“About authentication credentials on the Backup Exec server”](#) on page 897.

**Table H-4** Authentication credentials for Oracle servers options

Item	Description
<b>Server name</b>	Displays the name of the Oracle server.
<b>Logon account</b>	Displays the name of the logon account that has rights to the Oracle server.
<b>Add</b>	Lets you add the fully qualified domain name and logon account credentials to the list.
<b>Delete</b>	Lets you remove the fully qualified domain name and logon account credentials.

## Deleting an Oracle server from the Backup Exec server’s list of authentication credentials

You can delete an Oracle server name or logon account from a Backup Exec server’s list of authentication credentials.

See [“About authentication credentials on the Backup Exec server”](#) on page 897.

**To delete an Oracle server from the Backup Exec server's list of authentication credentials**

- 1 Click the Backup Exec button, and then select **Configuration and Settings** and then click **Backup Exec Settings**.
- 2 In the left pane, click **Oracle**.
- 3 Select the item that contains the server name or logon account that you want to delete.
- 4 Click **Delete**.
- 5 Click **OK**.

## About Oracle instance information changes

Whenever information about the Oracle instance changes, such as the instance user name and password, you must update the Backup Exec Agent Utility.

When Oracle RAC nodes are added or removed, you must enter information about any changes to instances in the Backup Exec Agent Utility. After these changes are entered, the Backup Exec server discovers them.

If the changes are not updated in the Backup Exec Agent Utility, the error "Unable to attach to a resource..." may appear when you run a backup job.

See ["Configuring the Oracle Agent on Windows computers and Linux servers"](#) on page 887.

## About backing up Oracle databases

Before you back up Oracle databases, review the following:

- You must run the Backup Exec Agent Utility on the Oracle server and add information about the instances before you can perform any backup or restore operations.

When Oracle instance information changes, you must update the Backup Exec Agent Utility. After these changes are entered, the Backup Exec server discovers them.

See ["Configuring the Oracle Agent on Windows computers and Linux servers"](#) on page 887.

- During a backup operation, the amount of data that is backed up may not equal the size of the Oracle files that are on the disk. This behavior is normal. Backup Exec backs up the selected data files as well as a copy of the control file.

- In a Central Admin Server Option environment, all backup jobs for a specific Oracle instance must be delegated to the same managed Backup Exec server. If you do not restrict the backup job to the same managed Backup Exec server, then before you can restore data, you must move the physical media that contains the backup sets to a single managed Backup Exec server. See [“Selecting a Backup Exec server pool for backups”](#) on page 1030.

- If the Oracle database resides on volumes that are configured with Oracle Automatic Storage Management (ASM), you cannot select these volumes as part of a file system backup.

The following message appears when you attempt to select the volumes:

```
An error was encountered while attempting to browse the
contents of <drive>. A device-specific error occurred.
```

- The database must be in a mounted or open state before you can make backup selections.
- The database must be in ARCHIVELOG mode before an archive log can be displayed in the list of servers on the **Backup and Restore** tab.

You can add an Oracle database to the list of servers on the **Backup and Restore** tab so that the database can be selected for backup jobs. You can set backup job default options for all Oracle backup jobs. Each time you create a backup job, the job uses the default options unless you change the options for the particular job.

See [“About the list of servers”](#) on page 157.

See [“Backing up data”](#) on page 163.

See [“Oracle backup options”](#) on page 903.

See [“About backing up Oracle RAC databases”](#) on page 901.

See [“About performing a DBA-initiated backup job for Oracle”](#) on page 902.

## About backing up Oracle RAC databases

Oracle Real Application Cluster (RAC) is an active/active cluster with shared storage, in which multiple instances share a single physical database. Since all of the participating nodes can access the database, you can initiate backup, restore, or recovery from any node. You can add an Oracle RAC database to the list of servers on the **Backup and Restore** tab so that the database can be selected for backup jobs.

Requirements for backing up Oracle RAC resources include the following items:

- You must run the Backup Exec Agent Utility on each node and add information about the instances before you can perform any backup or restore operations.

When RAC nodes are added or removed, you must update the Backup Exec Agent Utility. with information about the affected instances. After these changes are entered, the Backup Exec server discovers them.

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

- You must select the RAC fully qualified domain name when making backup selections.

Each node in the cluster uses the same fully qualified domain name. The fully qualified domain name of the node appears in the list of servers on the **Backup and Restore** tab. It is in the form RAC-<database name>-<database ID>.

Backing up Oracle RAC is similar to backing up standard Oracle databases.

You should be aware of the following differences:

- By default, each node in an Oracle RAC stores its archive logs locally. To have a meaningful backup of the archive logs, back up each archive log. Alternatively, you can move the archive logs to shared storage for backup.
- Each node that is part of the cluster is assigned a priority. For database backups, Backup Exec connects to the node that has the highest priority. Backup Exec uses the fully qualified domain name to connect to the node.

See [“About the list of servers”](#) on page 157.

See [“Backing up data”](#) on page 163.

See [“Oracle backup options ”](#) on page 903.

See [“About backing up Oracle databases”](#) on page 900.

See [“About performing a DBA-initiated backup job for Oracle”](#) on page 902.

## About performing a DBA-initiated backup job for Oracle

A Database Administrator (DBA) can initiate a backup or restore operation for Oracle from the RMAN console. Example scripts for backup and restore operations that you can run from the RMAN console are installed to the following location:

```
\Program Files\Symantec\Backup Exec\scripts\Oracle
```

Refer to your Oracle documentation for more information on using the RMAN console.

Review the following notes before initiating backup jobs for Oracle from the RMAN console:

- Ensure that you have completed all of the preparations for configuring the Oracle Agent.

See [“Configuring the Oracle Agent on Windows computers and Linux servers”](#) on page 887.

- The channel is not released if the RMAN console is not exited, or if a new manual channel is not allocated on that console.  
See [“Troubleshooting the Oracle Agent”](#) on page 910.
- The SKIP INACCESSIBLE option is available in RMAN to skip corrupt data and log files. Jobs that include this option may complete successfully, but it is likely that if this data is restored, the database will be in an inoperable state. The SKIP INACCESSIBLE option is not available for Backup Exec server operations. If a backup job encounters corrupt data or log files, the job fails. Symantec recommends that you do not use this option.
- In a CASO environment, the destination storage that you select in the DBA-initiated job template must be locally attached to the central administration server.

If the destination storage includes a storage device pool, all storage in the pool must be locally attached to the central administration server.

See [“About Oracle instance information changes”](#) on page 900.

See [“About Oracle instance information changes”](#) on page 900.

See [“About backing up Oracle databases”](#) on page 900.

See [“About configuring DBA-initiated job templates”](#) on page 483.

## Oracle backup options

The following options are available for Oracle backup jobs. These options appear when you select the Oracle option on the **Backup Job Defaults** dialog box and on the **Backup Options** dialog box for a backup job.

See [“About backing up Oracle databases”](#) on page 900.

See [“Backing up data”](#) on page 163.

See [“Setting default backup job settings”](#) on page 456.

**Table H-5** Oracle backup options

Item	Description
<b>Maximum number of devices to use for resources that support multiple data streams</b>	<p>Specifies the maximum number of devices that the backup job can use.</p> <p>If you specify more than one device, you must choose one of the following items as the destination storage for the backup job:</p> <ul style="list-style-type: none"> <li>■ A storage pool.</li> <li>■ A legacy backup-to-disk folder that has at least two concurrent operations enabled.</li> </ul> <p>If there is only one storage device for the backup job to use, then the data streams from RMAN are backed up serially to the media.</p> <p>This feature is not available for DBA-initiated jobs.</p>
<b>Minimum number of devices, terminate job if fewer devices are available</b>	<p>Specifies the minimum number of storage devices that the job can use.</p> <p>If the job cannot acquire the minimum number of devices, the job fails.</p> <p>This feature is not available for DBA-initiated jobs.</p>
<b>Delete backed up archived log files</b>	<p>Lets you delete the archived log files automatically after the backup.</p>
<b>Do not back up archived logfiles that have already been backed up</b>	<p>Enables Backup Exec to skip any archived logfiles that have been backed up previously.</p>
<b>Perform the backup offline</b>	<p>Enables Backup Exec to take the database offline before you start the backup job. Backup Exec brings the database online after the backup job is complete.</p> <p>Select this option if the Oracle database is a non-archived logged database.</p>

## About restoring Oracle resources

The Oracle Agent lets you restore Oracle databases, tablespaces, or datafiles. You can restore items to their original location or you can redirect the restore to a new location. The restore selections that you choose in Backup Exec are converted to a script. RMAN uses the script to determine what to restore from the Backup Exec backup set. After the data has been restored to the Oracle server, RMAN completes any requested recovery and restore operations. These recovery and restore operations are determined by the options that you select.

Some recovery operations may not require media from the Backup Exec server. For example, the redo logs may still be on the Oracle server. During a restore operation, the amount of data that is restored may not be equal to the amount of data that is backed up. In some cases, the amount of data that is restored is listed as 0 bytes. This behavior is normal because Oracle might skip data files that are already up-to-date on the disk.

If you perform a complete recovery on the whole database, or on a tablespace or datafile, you must restore a backup of the database or files that you want to recover. Then you must apply online or archived redo logs, or both. For jobs that are initiated both from the Backup Exec server and from a DBA, RMAN determines the specific data that it requires from Backup Exec to complete the restore and the recovery that you request.

---

**Note:** Backup Exec does not support Oracle tablespace point-in-time restore (TSPITR) through server-initiated operations.

---

You can only choose Oracle restore selections from the **Resource View** in the Restore Wizard. The **Details View** displays backup sets, but you cannot browse or select the contents.

On the **Resource View**, you can make restore selections from the online database or from control files.

**Table H-6** Restore selections for Oracle resources

View restore data in	Description
Online database	<p>Provides a view of the live database (if available). You can select an entire database or select individual tablespaces and datafiles.</p> <p><b>Note:</b> For Oracle RAC, the Oracle database is listed under its fully qualified domain name. It is in the form RAC-<i>&lt;database name&gt;</i>-<i>&lt;database ID&gt;</i>.</p>
Control files	<p>Provides a list of all backed up control files. Each control file lists the date it was backed up and the control file's piece ID.</p> <p>You cannot select individual tablespaces or datafiles for restore.</p> <p><b>Caution:</b> When you recover to a point in time by using a control file, ensure that the date of the control file backup is before the specified recovery point in time. There should not be any database structure changes between the two times. Additionally, when you restore a control file, the entire database reverts to the point in time of the restored control file.</p>

See [“About searching for and restoring data”](#) on page 229.

## About DBA-initiated restore for Oracle

DBAs can initiate restore jobs directly from the RMAN console. For example, you can specify the resources you want restored, and the number of channels to allocate for the restore job. Refer to your Oracle documentation for more information on using the RMAN console.

All DBA-initiated restore jobs are deleted after the jobs have completed.

---

**Note:** If you attempt to use a DBA-initiated restore job to restore a datafile, a tablespace, or a database that is online, a message appears on the RMAN console. The message indicates that the restore cannot be performed because Oracle does not allow the restore of these items if they are online. However, this message is not reported to Backup Exec. Therefore, the DBA-initiated restore job is reported in Backup Exec as completing successfully.

---

## About redirecting a restore of Oracle data

In Backup Exec, you can redirect an Oracle instance or its files by redirecting the following:

- An Oracle instance to another Oracle server.

---

**Note:** If you redirect the instance to a different Oracle server, ensure that an instance with the same name and database ID (DBID) is set up on that server. The database status should be Nomount. Refer to your Oracle documentation for details on creating an instance with the same name and database ID.

---

- An Oracle instance to another Oracle server and specifying alternate paths for the Oracle files.
- Tablespaces, datafiles, and archive logs to an alternate location on the original server.

Symantec recommends that you select only one instance for each redirected restore operation.

See [“About searching for and restoring data”](#) on page 229.

## Requirements for recovering the complete Oracle instance and database using the original Oracle server

If you experience a complete loss, deletion, or destruction of the Oracle instance or database, you can use the same Oracle server for the recovery. You can also use these instructions when you configure a new physical server that uses the same server name and SID name.

To successfully complete the recovery using this scenario, you must have the following items:

**Table H-7** Requirements when you recover using the original Oracle server

Item	Description
DBID	If you do not know the DBID, you can find it in the Backup Exec job log or in RMAN after you login.
ControlFile piece ID	You can identify the ControlFile piece ID in the Backup Exec restore view in the Control Files subnode under the Oracle node.
A full system Oracle backup	The full system Oracle backup must include the following: <ul style="list-style-type: none"><li>■ controlfile</li><li>■ datafiles</li><li>■ archive logs</li></ul>
The original Oracle server	To successfully recover the Oracle system using disaster recovery scenario 1, you must restore to the original Oracle server.

## Recovering the complete Oracle instance and database using the original Oracle server

You can use the same Oracle server for a recovery if you experience a complete loss, deletion, or destruction of the Oracle instance or database.

See [“Requirements for recovering the complete Oracle instance and database using the original Oracle server”](#) on page 907.

### To recover the complete Oracle instance or database using the original Oracle server

- 1 Recreate the Oracle database using the same name you used for the original database that was lost.
- 2 Find and rename the `pwd<SID>.ora` file.
- 3 Do the following in the order listed to create a new `pwd<SID>.ora` file:
  - Open a command prompt.

- Type the following command:  
`orapwd file=path\pwdsid.ora password=<password>`
- 4 Type the following commands in the order listed:
  - `RMAN`
  - `CONNECT TARGET <sys/password@sid>;`
  - `SHUTDOWN ABORT;`
  - `STARTUP NOMOUNT;`
  - `SET DBID<dbid ID>;`
- 5 At the Backup Exec server, launch the Backup Exec Restore Wizard.
- 6 Select the appropriate ControlFile to restore.  
The restore job will fail because the recovery portion encounters inconsistent archive logs. This is a normal occurrence during a disaster recovery.
- 7 After the restore job completes, exit Backup Exec.
- 8 At the Oracle server command prompt, type:  
**Alter database open resetlogs;**
- 9 Close the command prompt.

## Requirements for recovering the complete Oracle instance or database to a computer other than the original Oracle server

If you experience a complete loss, deletion, or destruction of the Oracle instance or database, you can restore the instance and database to a computer other than the original Oracle server.

See [“Recovering the complete Oracle instance and database using the original Oracle server”](#) on page 907.

To successfully complete the recovery, you must have the following items:

**Table H-8** Requirements when you recover using a new or alternate Oracle server

Item	Description
DBID	If you do not know the DBID, you can find it in the Backup Exec job log or in RMAN after you login.
ControlFile piece ID	You can identify the ControlFile piece ID in the Backup Exec restore view in the Control Files subnode under the Oracle node.

**Table H-8** Requirements when you recover using a new or alternate Oracle server *(continued)*

Item	Description
A full system Oracle backup	The full system Oracle backup must include the following: <ul style="list-style-type: none"><li>■ controlfile</li><li>■ datafiles</li><li>■ archive logs</li></ul>

## Recovering the complete Oracle instance or database to a computer other than the original Oracle server

You can restore an Oracle instance or database to a computer other than the original Oracle server.

See [“Requirements for recovering the complete Oracle instance or database to a computer other than the original Oracle server”](#) on page 908.

### To recover the complete Oracle instance and database to a computer other than the original Oracle Server

- 1 Recreate the Oracle instance using the same name you used for the original instance that was lost.
- 2 Find and rename the `pwd<SID>.ora` file.
- 3 Do the following in the order listed to create a new `pwd<SID>.ora` file:
  - Open a command prompt.
  - Type the following command:  
**orapwd file=path\pwdsid.ora password=<password>**
- 4 Type the following commands in the order listed:
  - **RMAN**
  - **CONNECT TARGET <sys/password@sid>;**
  - **SHUTDOWN ABORT;**
  - **STARTUP NOMOUNT;**
  - **SET DBID<dbid ID>;**
- 5 At the Backup Exec server, launch the Backup Exec Restore Wizard.
- 6 Select the appropriate ControlFile to restore.

**7** Select the option to restore **To a different Oracle server** and select the appropriate options.

**8** After the restore job completes, exit Backup Exec.

The restore job will fail because the recovery portion encounters inconsistent archive logs. This is a normal occurrence during a disaster recovery.

**9** Move to the Oracle server.

**10** Type **Alter database open resetlogs;**

**11** Do one of the following:

If an error is encountered while Oracle tries to open the database      Note the online redo log path and then update the path. See [“Updating the online redo log file path”](#) on page 915.

If an error does not occur      Do nothing. The disaster recovery is complete.

## Troubleshooting the Oracle Agent

If you have a problem with the Oracle Agent, the following questions and answers may help you solve the problem.

**Table H-9** Questions and answers about the Oracle Agent

Question	Answer
What should I do if I get a message that an attempt by Backup Exec to change the state of the Oracle database timed out?	<p data-bbox="821 326 1239 586">For Backup Exec server operations, the Oracle database may take some time to change states, such as from open to shut down, from shut down to mount, and so on. A SQLplus script in Backup Exec allows a default time-out of 10 minutes to handle the changing database state. For Oracle Real Application Cluster (RAC), a srvctl script is used.</p> <p data-bbox="821 604 1224 661">The time-out for database state change is named <code>SqlplusTimeout</code>.</p> <p data-bbox="821 678 1224 760">You may need to change the length of the default time-out if the following error message appears:</p> <p data-bbox="821 777 1239 951">An attempt by Backup Exec to change the state of the database timed out. For details, refer to the Database Script output section in the job log. Contact your database administrator to change the state of the database.</p> <p data-bbox="821 968 1239 1177">Try shutting down the database. If you succeed, then the SQLplus time-out is too short. Change the default time-out appropriately, based on how long it took to shut down the database. If you cannot shut down the database, contact your DBA to troubleshoot the database.</p> <p data-bbox="821 1194 1239 1333">If the time-out is too short, then restore jobs and offline backups may fail with a time-out error. If the time-out is too long, and the database does not respond to the state change request, the job takes longer to fail.</p> <p data-bbox="821 1350 1239 1432">See <a href="#">“Changing the <code>SqlplusTimeout</code> for Oracle instances on Windows computers”</a> on page 913.</p> <p data-bbox="821 1449 1239 1506">See <a href="#">“Changing the <code>SqlplusTimeout</code> for Oracle instances on Linux computers”</a> on page 914.</p>

**Table H-9** Questions and answers about the Oracle Agent (*continued*)

Question	Answer
<p>What should I do if a job continues to run on the Backup Exec server even after it ends on the Oracle RMAN console?</p>	<p>When a backup or restore operation is run on an automatically allocated channel, and if the channel is not released, the job continues to run on the Backup Exec server even after the operation ends on the RMAN console. The channel is not released if the RMAN console is not exited, or if a new manual channel is not allocated on that console. The job ends on the Backup Exec server when either the automatic channel is released, or after a time-out period elapses without any activity on that channel, whichever occurs first. If a new backup or restore operation is started within the time-out period on the same automatic channel, a new job is not created. Instead, the existing job performs the operation at the Backup Exec server.</p> <p>The channel time-out has a default value of 10 minutes, which is recommended for most purposes. If the time-out is too short, then multiple jobs are created for successive operations on a channel. If the time-out is too long, the job runs for a long time on the Backup Exec server unnecessarily, after the operation has ended.</p> <p>See <a href="#">“Changing the time-out for an automatic RMAN channel for Oracle instances on Windows computers”</a> on page 914.</p> <p>See <a href="#">“Changing the time-out for an automatic RMAN channel for Oracle instances on Linux computers”</a> on page 915.</p>

**Table H-9** Questions and answers about the Oracle Agent (*continued*)

Question	Answer
<p>The error "Unable to attach to a resource..." is displayed when Oracle instance information changes</p>	<p>Whenever Oracle instance information changes, you must update the Backup Exec Agent Utility. If credential information is not updated or is incorrect, the error "Unable to attach to a resource..." may be displayed when you run a backup job. If this message appears, you must bring the server online and configure the information.</p> <p>See <a href="#">"Configuring the Oracle Agent on Windows computers and Linux servers"</a> on page 887.</p>
<p>What should I do if the error ORA-12546: TNS: Permission denied appears on the Linux computer where Oracle is installed?</p>	<p>If a Backup Exec operation fails on the Linux computer on which the Oracle instances are installed, and the error in the RMAN output section is ORA-12546: TNS: Permission denied, then you must change the machine-level resource credentials in the job. The resource credentials must be an account that is a member of the dba and beoper groups on the Linux computer. Retry the operation.</p> <p>See <a href="#">"Setting authentication credentials on the Backup Exec server for Oracle operations"</a> on page 898.</p> <p>See <a href="#">"About the Backup Exec operators group for the Agent for Linux"</a> on page 1078.</p>

## Changing the SqlplusTimeout for Oracle instances on Windows computers

You can change the length of time Backup Exec handles a change in the state of the Oracle database. Backup Exec allows a default time-out of 10 minutes to handle the changing database state.

See ["Troubleshooting the Oracle Agent"](#) on page 910.

### To change the SqlplusTimeout for Oracle instances on Windows computers

- 1 Create a registry entry of the type DWORD in:  
`Software\Symantec\Backup Exec\Engine\Agents\XBSA\Oracle RMAN Agent`
- 2 Name the entry SqlplusTimeout.
- 3 Set the time-out value in seconds.  
For example, a time-out of 5 minutes is set as 300 seconds.

## Changing the SqlplusTimeout for Oracle instances on Linux computers

You can change the length of time Backup Exec handles a change in the state of the Oracle database. Backup Exec allows a default time-out of 10 minutes to handle the changing database state.

See [“Troubleshooting the Oracle Agent”](#) on page 910.

### To change the SqlplusTimeout for Oracle instances on Linux computers

- 1 In a command prompt, type the following:  
`vi etc/VRTSralus/ralus.cfg`
- 2 Create the following entry:  
`Software\Symantec\Backup Exec\Engine\Agents\XBSA\Oracle RMAN Agent\SqlplusTimeout`
- 3 Set the time-out value in seconds.  
For example, a time-out of 5 minutes is set as 300 seconds.

## Changing the time-out for an automatic RMAN channel for Oracle instances on Windows computers

You can change the default channel time-out of 10 minutes for an automatic RMAN channel.

See [“Troubleshooting the Oracle Agent”](#) on page 910.

### To change the time-out for an automatic RMAN channel for Oracle instances on Windows computers

- 1 Create a registry entry of the type DWORD in:

```
HKLM\Software\Symantec\Backup Exec\Engine\Agents\XBSA\Oracle RMAN Agent
```

- 2 Name the entry ChannelTime.
- 3 Set the time-out value in minutes.

## Changing the time-out for an automatic RMAN channel for Oracle instances on Linux computers

You can change the default channel time-out of 10 minutes for an automatic RMAN channel.

See [“Troubleshooting the Oracle Agent”](#) on page 910.

### To change the time-out for an automatic RMAN channel for Oracle instances on Linux computers

- 1 In a command prompt, type the following:

```
vi etc/VRTSralus/ralus.cfg
```

- 2 Create the following entry:

```
HKLM\Software\Symantec\Backup Exec\Engine\Agents\XBSA\Oracle RMAN Agent <time-out>
```

- 3 Set the time-out value in minutes.

## Updating the online redo log file path

You may have to update the online redo log file path during the recovery of a complete Oracle instance or database.

See [“Recovering the complete Oracle instance or database to a computer other than the original Oracle server”](#) on page 909.

### To update the online redo log file path

- 1 At the Oracle server, open a command prompt.
- 2 Type the following commands in the order listed:

```
■ SQLPLUS /nolog  
■ connect<sys/password@SID>;
```

- 3 Type the following SQLPlus command:

```
SQLPLUS ALTER DATABASE RENAME FILE <old path from backup to any  
redolog file name> to <path to expected restored redolog file  
name>;
```

For example,

```
ALTER DATABASE RENAME FILE  
'D:\ORACLE\ORADATA\JACOB\REDO01.LOG' to  
'C:\ORACLE\ORADATA\JACOB\REDO01.LOG';
```

- 4 In the command prompt, type **RMAN**.
- 5 Type the following command at the RMAN prompt:

```
Alter database open resetlogs;
```

- 6 Close the command prompt.

## Symantec Backup Exec Agent for Enterprise Vault

This appendix includes the following topics:

- [About the Agent for Enterprise Vault](#)
- [Requirements for the Enterprise Vault Agent](#)
- [About installing the Enterprise Vault Agent](#)
- [About backup methods for Enterprise Vault backup jobs](#)
- [About backing up Enterprise Vault components](#)
- [About consistency checks for Enterprise Vault databases and Compliance and Discovery Accelerator databases](#)
- [About restoring Enterprise Vault](#)
- [Configuring Enterprise Vault to use the name of the new SQL Server that holds the Directory database](#)
- [Best practices for the Enterprise Vault Agent](#)
- [About the Backup Exec Migrator for Enterprise Vault](#)

### About the Agent for Enterprise Vault

The Symantec Backup Exec Agent for Enterprise Vault (Enterprise Vault Agent) is installed as part of the Agent for Applications and Databases.

The Enterprise Vault Agent provides data protection for the following Enterprise Vault components:

- Sites

- Vault Store Groups
- Databases
- Indexes
- Vault partitions

The Enterprise Vault Agent can help provide a disaster recovery solution for data that is archived with Enterprise Vault. Recovery of the archived data is not dependent on the archive source, such as Exchange Server or a specific file system.

The Enterprise Vault Agent lets you do the following:

- Back up and restore Enterprise Vault archives from open or closed vault store partitions.
- Back up and restore individual Enterprise Vault vault store groups from an Enterprise Vault site.
- Back up and restore Enterprise Vault sites, databases, and index locations.

When you back up Enterprise Vault servers the following Enterprise Vault components can be backed up along with the vault partitions:

- Enterprise Vault Directory and Monitoring databases
- Enterprise Vault Audit, FSA Reporting, and Fingerprint databases
- Enterprise Vault vault store databases
- Enterprise Vault indexing files

If you install the Enterprise Vault Compliance and Discovery Accelerator products, the following components can be backed up:

- Enterprise Vault Compliance Accelerator and Discovery Accelerator Configuration databases
- Enterprise Vault Compliance and Discovery Accelerator Customer databases
- Enterprise Vault Discovery Accelerator Custodian database

The Enterprise Vault Agent uses Enterprise Vault Backup mode to back up Enterprise Vault components. By using the Backup mode, the Enterprise Vault Agent can back up Enterprise Vault components without having to suspend Enterprise Vault archiving operations.

For example, when you select a vault store group or site for backup, the individual vault store or indexes are placed in Backup mode. Backup mode lets Enterprise Vault continue archiving operations in other vault store groups or sites. After the backup job successfully completes, the Enterprise Vault Agent takes the Enterprise Vault components out of Backup mode so that those components can continue archival operations.

While Enterprise Vault versions 8.x, 9.x, and 10.x all implement Backup mode, Enterprise Vault 9.x and 10.x offer you more flexibility with your vault store backup jobs. With Enterprise Vault 9.x and 10.x, you can run multiple backup jobs of the same Enterprise Vault 9.x and 10.x vault store simultaneously. With Enterprise Vault 8.x, multiple vault store backup jobs must run one at a time.

For example, you can create multiple backup jobs to back up a vault store. Each backup job includes in its selection list one or more unique partitions of the vault store. Under Enterprise Vault 9.x and 10.x, the partitions are backed up simultaneously when the different backup jobs access them at the same time. Under Enterprise Vault 8.x, the partitions are backed up in both backup jobs; however they are backed up sequentially. The first backup job must finish before the second job starts, or else a backup job failure occurs.

---

**Note:** With all versions of Enterprise Vault, the Enterprise Vault Agent automatically backs up the vault store database whenever an open partition is backed up.

---

The Enterprise Vault Agent backs up the Compliance Accelerator and Discovery Accelerator application databases while they are online. It does not place the databases in Read-only mode or Backup mode before it backs them up.

The Enterprise Vault Agent runs a physical check on each Enterprise Vault database before it backs them up. The Enterprise Vault Agent also runs a physical check on each database before you restore them.

---

**Note:** The Enterprise Vault Agent uses physical database consistency checks because physical checks consume less system resources than other types of Database Consistency Checking options.

---

Backing up and restoring Enterprise Vault databases and related components require specific user account credentials for each Enterprise Vault component you protect.

**Table I-1** Supported user accounts that are required to back up and restore Enterprise Vault components

Enterprise Vault components	User credentials
<p>Enterprise Vault databases and components (vault store, indexes, partitions, vault store database, Directory, Monitoring, Fingerprint, FSA Reporting, and Audit databases)</p>	<p>The following credentials are required:</p> <ul style="list-style-type: none"> <li>■ Vault Service account</li> <li>■ Domain Admin account with Role Based Admin privileges</li> </ul> <p>You can also use any domain user account that meets the following requirements:</p> <ul style="list-style-type: none"> <li>■ The user account must be included in the Administrators group on all Enterprise Vault servers.</li> <li>■ The user account must be included in the Backup Operators group on all computers where Enterprise Vault databases reside. With Enterprise Vault partitions, the user account must be included in the Administrators group.</li> <li>■ The user account must have backup-related Role Based Admin privileges for the vault store and the index location.</li> </ul> <p>Backup-related Role Based Admin privileges include:</p> <ul style="list-style-type: none"> <li>■ EVT Manage Vault Store Backup Mode</li> <li>■ EVT Manage Index Location Backup Mode</li> </ul> <p>To configure Role Based Admin privileges for a Windows Domain Admin account, see your Enterprise Vault documentation.</p> <p><b>Note:</b> To back up a computer that has a partition, or a partition and a database, you must be a member of the computer's Administrator's group. To back up a computer that has only an Enterprise Vault database on it, you need only to be a member of the Backup Operators group.</p>

**Table I-1** Supported user accounts that are required to back up and restore Enterprise Vault components (*continued*)

Enterprise Vault components	User credentials
Compliance Accelerator and Discovery Accelerator	<p>The following credentials are required:</p> <ul style="list-style-type: none"> <li>■ Vault Service account</li> <li>■ Domain Admin account</li> </ul> <p>A user account that is a member of the following groups:</p> <ul style="list-style-type: none"> <li>■ Administrator's group on those computers where the Compliance and Discovery Accelerator applications reside.</li> <li>■ Administrator's group and Backup Operator's group on those computers where the Accelerator databases reside.</li> </ul>

When you back up specific Enterprise Vault components, the other Enterprise Vault components are automatically backed up at the same time. Backup Exec includes these components to hasten an Enterprise Vault recovery.

**Table I-2** Enterprise Vault databases that are automatically backed up

When you back up this	Backup Exec automatically backs up this	Description
Enterprise Vault site	Directory database	Backup Exec automatically backs up the Directory database that is associated with the Enterprise Vault site.
Open partition	Vault store database	Backup Exec automatically backs up the vault store database that is associated with the open partition.

Over time the amount of data that Enterprise Vault stores continues to grow. At some point, you may observe that as the data moves through its usage lifecycle, you no longer access it as frequently. You can use the Backup Exec Migrator for Enterprise Vault to automatically migrate the older Enterprise Vault data to the storage devices that Backup Exec manages.

See [“About the Backup Exec Migrator for Enterprise Vault”](#) on page 940.

## Requirements for the Enterprise Vault Agent

Review the following requirements before you use the Agent for Enterprise Vault (Enterprise Vault Agent).

- You must create at least one partition on an Enterprise Vault server before the Enterprise Vault server can publish itself to Backup Exec.
- You must install the Backup Exec Agent for Windows and license the Enterprise Vault Agent on any computer that hosts an Enterprise Vault component.

---

**Note:** The Enterprise Vault Agent uses the Agent for Windows to back up all NTFS shares on a remote computer that contains Enterprise Vault data. However, if the Agent for Windows is not installed, the Enterprise Vault Agent uses Microsoft's Common Internet File System (CIFS) to back up the data.

For a device or a filer that does not support the Agent for Windows, the Enterprise Vault Agent uses CIFS to back up the data. Symantec recommends that you create separate backup jobs when you want to do NDMP backups of Enterprise Vault data. You may see a significant performance improvement of NDMP backups with the Symantec Backup Exec NDMP Option.

---

## About installing the Enterprise Vault Agent

The Agent for Enterprise Vault (Enterprise Vault Agent) is installed as part of the Agent for Applications and Databases. To back up all Enterprise Vault servers, the Enterprise Vault Agent must be installed on each Enterprise Vault server in your environment. In addition, the Enterprise Vault Agent must also be installed on any remote computer where Enterprise Vault components are installed. If the Compliance and Discovery Accelerators are installed on remote computers, the Enterprise Vault Agent must be installed on those computers too.

You can install the Enterprise Vault Agent in the following ways:

- Install it automatically from the Backup Exec server as part of a Agent for Windows installation to the local Enterprise Vault server. After you finish the installation, you may need to configure the Enterprise Vault Agent to publish itself to a Backup Exec server of your choice.  
See [“About publishing the Agent for Windows to Backup Exec servers”](#) on page 738.
- Install the required Enterprise Vault Agent licenses on the Backup Exec server.

After you install the licenses, you can push-install the Backup Exec Agent for Windows to all Enterprise Vault servers and the computers where other Enterprise Vault components are installed.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

See [“Push-installing the Agent for Windows to remote computers”](#) on page 86.

## About backup methods for Enterprise Vault backup jobs

You can select a backup method that depends on the Enterprise Vault object that you want to backup.

The following table describes the type of Enterprise Vault backup jobs you can run. The table also describes the backup methods that are available for each type of backup job.

**Table I-3** Backup methods to use with Enterprise Vault backup jobs

To back up	Select	Description
Directory and Monitoring databases Audit database and FSA Reporting database	Full, differential, or incremental backup method	Directory, Monitoring, Audit, and FSA Reporting database backups can use the full and incremental backup methods. These databases cannot be backed up using the differential backup method. If you select the differential backup method, Backup Exec does a full backup instead. <b>Note:</b> Selecting an incremental backup method backs up the database transaction logs and then truncates them.
Vault database and Fingerprint database	Full, differential, or incremental backup method	Vault database and Fingerprint database backups can use all three backup methods: Full, differential, and incremental. <b>Note:</b> Selecting an incremental backup method backs up the database transaction logs and then truncates them.
Vault partitions and index locations	Full, differential, or incremental backup methods.	You can use all of the backup methods that are available for standard file system backup jobs.

When you combine Enterprise Vault components in a backup job, each component may use a backup method that differs from what you selected for the overall job. For example, you create a job that uses the differential backup method to back up both a Directory database and a partition. However, because a Directory database cannot be backed up using the differential method, Backup Exec uses the full backup method to back up the Directory database. This results in fast and easy restores. After the Directory database is backed up, Backup Exec uses the differential backup method to back up the partition.

Use the following table as a guide.

**Table I-4** Actual backup methods that are used for Enterprise Vault components

Enterprise Vault component	Full (F)	Differential (D)	Incremental (I)
Directory and Monitoring databases	F	F	I Always truncates the transaction logs
Vault store database	F	D	I Always truncates the transaction logs
Audit database	F	F	I Always truncates the transaction logs
FSAReporting database	F	F	I Always truncates the transaction logs
Fingerprint database	F	D	I Always truncates the transaction logs
Partition	F	D	I
Index root path	F	D	I

**Table I-4** Actual backup methods that are used for Enterprise Vault components (*continued*)

Enterprise Vault component	Full (F)	Differential (D)	Incremental (I)
Compliance Accelerator/Discovery Accelerator Configuration database <b>Note:</b> Also includes the Compliance Accelerator and Discovery Accelerator databases that are installed with runtime versions of Enterprise Vault.	F	F	I Always truncates the transaction logs
Compliance Accelerator/Discovery Accelerator Customer database <b>Note:</b> Also includes the Compliance Accelerator and Discovery Accelerator databases that are installed with runtime versions of Enterprise Vault.	F	D	I Always truncates the transaction logs
Discovery Accelerator Custodian database <b>Note:</b> Also includes the Discovery Accelerator Custodian databases that are installed with runtime versions of Enterprise Vault.	F	D	I Always truncates the transaction logs

See [“About backup methods”](#) on page 528.

See [“About backing up Enterprise Vault components”](#) on page 926.

## Enterprise Vault backup options

You can select a backup method that is based on the type of Enterprise Vault database that you want to back up.

See [“About backup methods for Enterprise Vault backup jobs”](#) on page 923.

See [“Backing up data”](#) on page 163.

See [“About backing up Enterprise Vault components”](#) on page 926.

## About backing up Enterprise Vault components

You can select any or all of the Enterprise Vault components for backup when you create a backup job. If you select all of the components for backup in the same job, recovery time is faster. However, if you create multiple backup jobs for the components, the backup jobs run faster.

The Enterprise Vault components that you can select are described in the following table, along with recommendations for backup:

**Table I-5** Enterprise Vault components

Enterprise Vault Component	Description
Directory database	<p>The Directory database is a Microsoft SQL Server database that contains configuration data.</p> <p>After the database is populated, the amount of data in the Directory database changes very little over time.</p> <p>You should back up the Directory database after you add or remove any Enterprise Vault component. You should also back up the Directory database if you change the location of any component. Configuration changes can include creating vault stores, creating vault store partitions, and changing vault store partition statuses.</p>

**Table I-5** Enterprise Vault components (*continued*)

Enterprise Vault Component	Description
Monitoring database	<p>Enterprise Vault includes a Monitoring agent on each Enterprise Vault server. The Monitoring agent monitors the following:</p> <ul style="list-style-type: none"> <li>■ The status of Enterprise Vault services and tasks.</li> <li>■ Performance counters for vault stores, disk space, memory, and processors.</li> <li>■ The status of Exchange Server journal mailbox target archiving targets, including item counts for Inbox, Archive Pending, and failed operations such as Failed DL Expansion.</li> <li>■ The status of Lotus Domino Server journaling location archiving targets, including item counts for Inbox, Archive Pending, and failed operations.</li> </ul> <p>The Monitoring agent collects monitoring data at scheduled intervals, typically every few minutes.</p> <p>All of the information that the Monitoring agent collects is stored in a Microsoft SQL Server database called the Monitoring database.</p>
Fingerprint databases	<p>The Fingerprint databases contains the single instance storage-related information for all of the vault stores in the vault store group.</p> <p>If you enable single instance storage of archived items, you should back up the Fingerprint databases on a regular basis.</p>
Index location	<p>The index location stores all of the archived data content that is indexed to enable fast searching and retrieval of archived items. The indexing data is stored in index files in the location that is specified when you install Enterprise Vault.</p> <p>You should back up the index location on regular basis.</p>

**Table I-5** Enterprise Vault components (*continued*)

Enterprise Vault Component	Description
Vault store group	The vault store group is a logical entity. If you select it for backup, all of the vault databases, vault store partitions, and the Fingerprint databases are backed up. Because these components are closely related, you should consider selecting the vault store group to back up all of these components together.
Vault store	The vault store is a logical entity. If you select it for backup, all of the vault databases and the vault store partitions are backed up.
All partitions	A vault store partition represents the physical location where the archived items are stored. A vault store can contain one or more vault store partitions. If you select <b>All Partitions</b> for backup, then all of the vault store partitions in the vault store are selected for backup.  <b>Note:</b> When you back up an open partition, Backup Exec automatically backs up the vault store database.
Site	An Enterprise Vault site is a logical representation of an installation of the Enterprise Vault. If you select this component for backup, the Directory database is also automatically backed up.
Compliance Accelerator database and Discovery Accelerator database	Installed as optional add-ons to Enterprise Vault, these databases are part of the Discovery Accelerator and Compliance Accelerator products.

See [“Backing up data”](#) on page 163.

See [“Editing backups”](#) on page 170.

See [“About stages”](#) on page 183.

# About consistency checks for Enterprise Vault databases and Compliance and Discovery Accelerator databases

Backup Exec automatically checks the physical consistency of an Enterprise Vault database before a backup job and after a restore job. It also checks the consistency of the Compliance and Discovery databases before a backup job and after a restore job. Backup Exec uses Microsoft SQL Server's Physical Check Only utility for consistency checks of the databases. In the event a consistency check fails, Backup Exec continues with the job and reports the consistency check failures in the Backup Exec job log.

If consistency checks fail during a restore operation, Backup Exec continues the job and reports the consistency check failures in the Backup Exec job log.

For more information about the Physical Check Only utility, see the Microsoft SQL Server documentation.

## About restoring Enterprise Vault

Review the following before you begin an Enterprise Vault restore operation.

- When you restore an Enterprise Vault installation, you should restore the Directory database in a separate restore job. After you successfully restore the Directory database, you can restore other Enterprise Vault components and partitions.
- When you restore Enterprise Vault databases, you can select the options that either leave databases in a ready-to-use state or in a non-operational state. The non-operational state options that you select apply to all Enterprise Vault databases except the vault store database. When you restore an Enterprise Vault vault store database, the Agent for Enterprise Vault (Enterprise Vault Agent) places the vault store database in Enterprise Vault Backup mode. If the vault store database remains in a non-operational state after the restore job completes, the Enterprise Vault Agent cannot remove it from Backup mode.

If you select the option that leaves the databases ready to use, the following applies:

- The Enterprise Vault Agent restores the vault store database in a ready-to-use, operational state. The vault store database's operational status is maintained even when you select additional backup sets for restore in the same vault store database restore job. Additional backup sets can include Full, Differential, and Incremental backup methods.

When you choose the option that leaves the databases in a nonoperational state, the following applies:

- The Enterprise Vault Agent prompts you to stop the **Enterprise Vault Storage Service** before you start the vault store database restore operation. You can restart the vault store restore operation again after the Enterprise Vault Storage Service stops.

As a best practice, Symantec recommends that you restore the vault store database in a ready-to-use state. When you restore the vault store database in a nonoperational state, Enterprise Vault cannot remove it from Backup mode after the restore operation finishes.

See [“Enterprise Vault restore options”](#) on page 931.

- You can individually restore Enterprise Vault components. Before you begin the restore, the databases and other components may or may not exist on the destination Enterprise Vault server. If the databases do not exist, you can restore them using the Enterprise Vault Agent. After the restore job completes, you must configure Enterprise Vault to use the restored databases. To configure Enterprise Vault to use the restored databases, see your Enterprise Vault documentation.

These items include the:

- Enterprise Vault 8.x/9.x/10.x Directory, Monitoring, Audit, FSAReporting, and Fingerprint databases
- Vault store databases, indexes, and partitions.
- Compliance and Discovery Accelerator Configuration and Customer databases.
- Discovery Accelerator Custodian database
- Symantec recommends that you use the Enterprise Vault service account or an account with rights to access the restore selections as the default logon account. Otherwise, you may have to enter proper credentials for each Enterprise Vault resource that you select for restore.
- After you restore Enterprise Vault, a message appears that says you need to run Enterprise Vault recovery tools. The recovery tools are used to re-synchronize Enterprise Vault with the newly restored databases after you complete the restore.  
For information on running the Enterprise Vault recovery tools, see your Enterprise Vault documentation.

Before you restore Enterprise Vault sites, servers or other components, you should have the following items installed on the destination computer:

- Enterprise Vault

- The Backup Exec Agent for Windows

---

**Note:** You must install the Agent for Windows on remote Enterprise Vault computers where you want to restore Enterprise Vault components.

---

See “[About searching for and restoring data](#)” on page 229.

## Enterprise Vault restore options

Use the following table to select the restore option you want to use when you restore the Enterprise Vault databases.

**Table I-6** Enterprise Vault restore options

Item	Description
<b>Automatically take the Enterprise Vault databases offline when restoring selected databases</b>	

**Table I-6** Enterprise Vault restore options (*continued*)

Item	Description
	<p>Takes the shared Enterprise Vault Directory, Monitoring, Audit, FSA Reporting, and Fingerprint databases offline so Backup Exec can replace them during a restore job.</p> <p><b>Note:</b> If you don't use this option, you must stop the Directory and Admin services on all Enterprise Vault servers before you restore the previously mentioned databases. In addition, you must also stop the Accelerator Manager server on all of the Compliance Accelerator servers and the Discovery servers. Only after you stop the Accelerator Manager can you restore the Customer, Configuration, and Custodian databases.</p> <p>This option causes the Enterprise Vault Admin and Directory services on all related Enterprise Vault servers to terminate the connection to the Directory database that you restore.</p> <p>It also terminates connections to the following:</p> <ul style="list-style-type: none"><li>■ Monitoring database</li><li>■ Audit, Fingerprint, and FSA Reporting databases (Enterprise Vault 8.x, 9.x, 10.x only)</li><li>■ Configuration, Customer, and Custodian databases</li></ul> <p>When the restore job completes, you must manually restart the Enterprise Vault Admin and Directory services on your Enterprise Vault server. After you restart the services, the services reconnect to the restored databases and Enterprise Vault begins archival operations again.</p> <p><b>Note:</b> This option causes the Enterprise Vault Admin and Directory services on all Enterprise Vault servers to terminate their connections to the Directory database that you restore. It also terminates the connections to the Enterprise Vault</p>

**Table I-6** Enterprise Vault restore options (*continued*)

Item	Description
	Accelerator Manager database.
<b>Do not take the Enterprise Vault databases offline</b>	<p>Leaves all Enterprise Vault databases online.</p> <p>If you use this option, you must stop the Directory and Admin services on all Enterprise Vault servers before you restore the previously mentioned databases. In addition, you must also stop the Accelerator Manager server on all of the Compliance Accelerator servers and the Discovery servers. Only after you stop the Accelerator Manager can you restore the Customer, Configuration, and Custodian databases.</p>
<b>Leave the database ready to use; additional transaction logs or differential backups cannot be restored</b>	<p>Rolls back all uncompleted transactions when you restore the last database, differential, or log backup. After the recovery operation, the database is ready for use. If you do not select this option, the database is left in an intermediate state and is not usable.</p> <p>If you select this option, you cannot continue to restore backups. You must restart the restore operation from the beginning.</p>
<b>Leave the database nonoperational; additional transaction logs or differential backups can be restored</b>	<p>Creates and maintains a standby database.</p> <p>By using this option, you can continue restoring other backups sets for non-operational databases.</p> <p>See your SQL documentation for information on standby databases.</p>

---

**Note:** Symantec recommends that you select all required backup sets when you run a single restore job for a vault store database. All required backup sets can include full, differential, and incremental backup sets. The vault store database should also be restored in a ready-to-use state after the restore job completes.

---

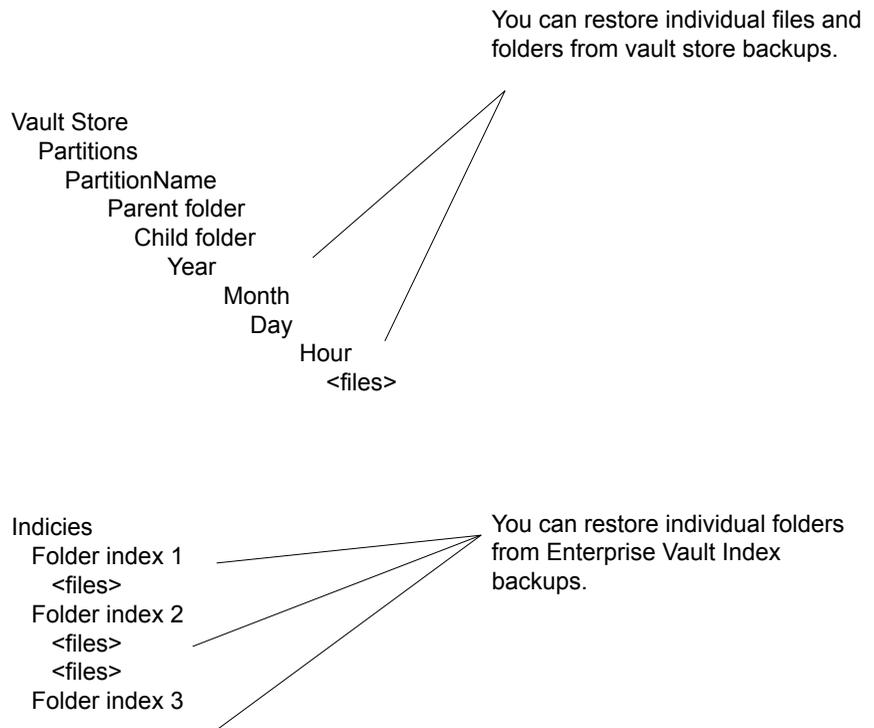
See [“About searching for and restoring data”](#) on page 229.

## About restoring individual files and folders with the Enterprise Vault Agent

The Agent for Enterprise Vault (Enterprise Vault Agent) supports individual file and folder restores from vault store partition backups. You can also restore complete index locations or individual folders from Enterprise Vault index backups.

See [“About searching for and restoring data”](#) on page 229.

**Figure I-1** Restoring individual files from vault store partitions and complete folders from an Enterprise Vault index



## About automatic redirection of Enterprise Vault components under an Enterprise Vault server

You can change the location of the vault store databases, Fingerprint databases, or partitions to a location that differs from where they were backed up. During restores of the vault store database, Fingerprint databases, or partitions, the Agent for Enterprise Vault (Enterprise Vault Agent) detects the location change. It then automatically redirects the component restores to the new location.

---

**Note:** Automatic redirected restores of the vault databases, partitions, or Fingerprint databases occur when you change only the location of these Enterprise Vault components. The names of the partitions, vault stores, and vault store groups must not change from the time the partition was originally backed up.

---

See [“About restoring Enterprise Vault”](#) on page 929.

## About redirecting a restore for an Enterprise Vault component

You can redirect the restore of the Enterprise Vault components.

The following table describes the requirements for redirecting a restore for an Enterprise Vault component:

**Table I-7** Requirements for redirecting a restore for an Enterprise Vault component

Component	Requirement
<b>All Enterprise Vault components</b>	<p>The following are requirements for redirecting the restore of all Enterprise Vault components:</p> <ul style="list-style-type: none"><li>■ All Enterprise Vault components must already exist on the server to which you redirect the restore. If they do not exist, you must create them. See your Enterprise Vault documentation.</li><li>■ The Backup Exec logon account that you use must have the same credentials as the Vault Store service account.</li></ul>
<b>Enterprise Vault databases</b>	<p>The following are requirements for redirecting the restore of the databases:</p> <ul style="list-style-type: none"><li>■ You must create a separate job for each database that you want to redirect.</li><li>■ You must redirect all databases to the same SQL server.</li></ul>

**Table I-7** Requirements for redirecting a restore for an Enterprise Vault component (*continued*)

Component	Requirement
<b>Vault store databases</b>	<p>The following are additional requirements for redirecting the restore of a vault store database:</p> <ul style="list-style-type: none"> <li>■ Ensure that the Directory database already exists on the server to which you redirect the restore.</li> <li>■ Ensure that the Directory database contains an entry for the vault store that uses the new SQL Server name.</li> </ul>
<b>Vault store partition</b>	<p>The following are additional requirements for redirecting the restore of a vault store partition:</p> <ul style="list-style-type: none"> <li>■ The vault store must already contain a vault partition with the same name. If a vault partition does not exist, you must create it.</li> </ul>
<b>Index location</b>	<p>The Directory database must already be configured with the new index location.</p> <p>See your Enterprise Vault documentation.</p>

## Redirection options for Enterprise Vault

You can redirect a restore job for Enterprise Vault components.

See [“About redirecting a restore for an Enterprise Vault component”](#) on page 936.

**Table I-8** Redirection options for Enterprise Vault

Item	Description
<b>To a new Microsoft SQL server</b>	<p>Redirects the restore jobs of Enterprise Vault databases and Accelerator databases to a different SQL Server.</p> <p>Displays the name of the server to which you want to redirect the restore job for a vault store.</p> <p><b>Note:</b> Vault store databases are restored for Enterprise Vault 8.x, 9.x and 10.x only.</p>

**Table I-8** Redirection options for Enterprise Vault (*continued*)

Item	Description
<b>Instance</b>	Displays the name of the instance of the SQL Server to which you want to redirect the restore job for a vault store.
<b>Restore index root to a new location</b>	Redirects the restore job for the index root to a new location.  If you redirect the restore of the Enterprise Vault server, you can specify an alternate path on the destination server. You can also redirect the index root location to an alternate path on the original server.
<b>Path</b>	Displays the path name to which you want to redirect the restore job for an index root.
<b>Restore partition root to a new location</b>	Redirects the restore job for a vault store partition to a new location.  Partitions are restored for Enterprise Vault 8.x, 9.x , and 10.x only.
<b>Path</b>	Displays the path name to which you want to redirect the restore job for a vault store partition.
<b>Enterprise Vault logon account</b>	Specifies the logon account to use.

## Configuring Enterprise Vault to use the name of the new SQL Server that holds the Directory database

Use the following steps to configure Enterprise Vault to use the name of the new SQL Server that holds the Directory database.

**To configure Enterprise Vault to use the name of the new SQL Server that holds the Directory database**

- 1 At each Enterprise Vault server, use Enterprise Vault to change the name of the previous SQL Server computer. Change the name to the name of the SQL Server computer that now holds the Directory database.

See your Enterprise Vault documentation.

- 2 Restart the Enterprise Vault Admin service on all Enterprise Vault servers that use the Directory database.

Two directory names appear in the backup selections view after you restart the Enterprise Vault Admin service on the Enterprise Vault server.

For example, **Directory on <OldSQL\_computer\_name>** and **Directory on <NewSQL\_computer\_name>**).

- 3 On the Backup and Restore tab, right-click the Enterprise Vault server that you want to back up.
- 4 On the Backup menu, select the backup definition that you want to use.
- 5 In the Selections box, click **Edit**.
- 6 Expand **Directory on <SQL server computer where you moved the Directory database>**.
- 7 Expand all items under **Directory on <SQL server computer where you moved the Directory database>**.

The **Directory** and **Monitoring** databases, Enterprise Vault 8.x, 9.x, or 10.x **FSA Reporting** and **Audit** databases, and the Enterprise Vault sites should appear. In addition, the Directory database should display the new SQL Server name and instance where it was redirected.

When you configure a new Directory database backup job, you must select the Directory database from the current Directory server. Backup Exec automatically removes the previous Directory server name 13 days after you complete the Directory database move.

- 8 To manually remove the previous server name, right-click **Directory on <OldSQL\_computer\_name>**.
- 9 Click **Remove**.

See your Enterprise Vault documentation.

## Best practices for the Enterprise Vault Agent

Symantec recommends the following best practices when you use the Agent for Enterprise Vault (Enterprise Vault Agent).

- Back up the Enterprise Vault Directory database after you make any configuration changes in Enterprise Vault.
- Restore the Enterprise Vault Directory database in a separate Backup Exec restore job.
- Restore all Full, Differential, and Incremental backup sets of the vault store database in a single restore job.
- Do not allow the backup window and archive window to overlap.
- Do not allow the backup window and the migration window to overlap.
- Make sure Enterprise Vault components are not in Backup mode before you back up the Enterprise Vault Directory database.
- If you install both the Symantec Backup Exec NDMP Option and the Enterprise Vault Agent, pick only one product to protect an Enterprise Vault partition that resides on NDMP filers.
- Do not change the recovery model of any database that is created by Enterprise Vault. Enterprise Vault configures each database in full recovery mode when it creates them.

See [“About the Agent for Enterprise Vault”](#) on page 917.

## About the Backup Exec Migrator for Enterprise Vault

The Backup Exec Migrator for Enterprise Vault (Backup Exec Migrator) lets you automatically migrate archived Enterprise Vault data to the storage devices that Backup Exec manages. By migrating the archived Enterprise Vault data from a partition, you can reclaim disk space on the Enterprise Vault server without incurring the cost of additional hardware.

By migrating Enterprise Vault archive data to the Backup Exec server storage devices, you also ensure an added level of storage redundancy using an off-host environment.

See [“How the Backup Exec Migrator works”](#) on page 941.

See [“Configuring the Backup Exec Migrator”](#) on page 948.

## Backup Exec Migrator for Enterprise Vault requirements

Before you configure the Backup Exec Migrator, ensure that your Enterprise Vault server meets the following requirements:

- Backup Exec Agent for Enterprise Vault must be installed on the Enterprise Vault server.
- Enterprise Vault migration and collections must be enabled for the Enterprise Vault partition from which you want to migrate data.
- Enterprise Vault 8.0 SP3 or higher must be installed on the Enterprise Vault server.

## How the Backup Exec Migrator works

Enterprise Vault automatically initiates all data migration operations from the Enterprise Vault server after you configure the Backup Exec Migrator. Enterprise Vault makes decisions on what should be migrated based on the archival policies and the data retention policies that you configure in the Enterprise Vault Administration Console. The Backup Exec Migrator then migrates the archived data to a Backup Exec server after Enterprise Vault collects the eligible data from the vault store partitions. When you configure migration options for a partition, you can set the migration period. All migration options are configured at the Enterprise Vault server.

**Table I-9** Enterprise Vault data migration process

Action	Notes
Enterprise Vault archives eligible partition data that is based on the file size or the file creation date.	All data that is eligible for archive is determined in the partition where you want to migrate data.  See your Enterprise Vault documentation.

**Table I-9** Enterprise Vault data migration process (*continued*)

Action	Notes
After Enterprise Vault completes the archival process, an Enterprise Vault collection process collects the archived data.	<p>The collection process places the archived data into Windows .cab files. The .cab files are stored in the partition where the migration occurs.</p> <p>Eligible data can include Enterprise Vault files with the following extensions:</p> <ul style="list-style-type: none"><li>■ .dvf</li><li>■ .dvssp</li><li>■ .dvsc</li><li>■ .dvs</li></ul> <p><b>Note:</b> Some eligible data cannot be compressed into .cab files due to file size restrictions. However, the Backup Exec Migrator still migrates the data during the migration operation.</p> <p>See your Enterprise Vault documentation.</p>

**Table I-9** Enterprise Vault data migration process (*continued*)

Action	Notes
The Backup Exec Migrator initiates the migration of the archived data files to a Backup Exec server.	

**Table I-9** Enterprise Vault data migration process (*continued*)

Action	Notes
	<p>Migration period schedules are determined when you configure migration for a partition and when you configure a collection schedule for the partition.</p> <p>See <a href="#">“Configuring Enterprise Vault collections”</a> on page 949.</p> <p>See <a href="#">“Configuring the Backup Exec Migrator to communicate with Enterprise Vault”</a> on page 953.</p> <p>If you follow the Symantec configuration recommendations for the Backup Exec Migrator and Enterprise Vault partitions, one migration job for each partition runs during a migration period. However, the Backup Exec Migrator may create separate migration jobs for each partition folder if you do not follow the configuration recommendations. If separate jobs are created, the resulting overhead that is required to run the jobs results in degraded migration and retrieval performance.</p> <p><b>Note:</b> If you schedule a file retrieval request from the Enterprise Vault server between migration periods, separate jobs are created even though you followed the configuration recommendations. In this case, the Backup Exec Migrator automatically creates separate jobs to facilitate retrieval of the requested file. During a migration operation, the restore job can be scheduled to run between migration jobs.</p> <p>If you do not follow the configuration recommendations, file retrieval performance can be affected.</p> <p>To ensure the most efficient migration and retrieval performance possible, follow the Symantec recommendations when you configure the Backup Exec Migrator and the Enterprise Vault partitions.</p> <p>See <a href="#">“Configuring the Backup Exec Migrator”</a></p>

**Table I-9** Enterprise Vault data migration process (*continued*)

Action	Notes
	on page 948.
Backup Exec completes the migration process by moving all of the migrated files to storage devices.	Symantec recommends configuring two storage devices for staged migration operations.  See <a href="#">“About using staged migrations with Backup Exec and the Backup Exec Migrator”</a> on page 945.  See <a href="#">“Configuring the Backup Exec Migrator”</a> on page 948.

After Backup Exec migrates the .cab files to the storage devices, you can review migration details by looking at the job history details for each Enterprise Vault server where the migration occurs.

See [“About the Job History”](#) on page 260.

## About using staged migrations with Backup Exec and the Backup Exec Migrator

When you configure Backup Exec to work with the Backup Exec Migrator, Symantec recommends that you configure two storage devices for staged migration operations. When you consider the devices to use, consider selecting a high performance backup-to-disk folder and a slower performance tape device. By using two devices, archived data can be migrated in two stages.

During the first stage, Backup Exec migrates the data it receives from the Backup Exec Migrator to a backup-to-disk folder on a high performance hard drive. By using a backup-to-disk folder, you can minimize the amount of time it takes to perform the initial migration. During the second migration stage, Backup Exec creates a duplicate job to migrate the archived data from the backup-to-disk folder to a tape device. You can schedule the duplicate job to move the archived data to a tape device at times when Backup Exec server activity is low.

See [“Configuring the Backup Exec Migrator to work with a Backup Exec server”](#) on page 951.

See [“Configuring the Backup Exec Migrator to communicate with Enterprise Vault”](#) on page 953.

## About Backup Exec Migrator events

The Backup Exec Migrator generates events that specify the status of the tasks that it runs. The events also provide useful information for troubleshooting purposes. You can view the events on the computer where you installed the Enterprise Vault Storage Service by viewing the Windows Event Viewer. From the Event Viewer, you can see the events under **Enterprise Vault**. You can also view the events in the Enterprise Vault Dtrace Utility.

For more information on the Enterprise Vault Dtrace Utility, see your Enterprise Vault documentation.

See “[About Backup Exec Migrator logs](#)” on page 946.

## About Backup Exec Migrator logs

The Backup Exec Migrator can create log files that log all migration activity. The log files reside on both the Enterprise Vault server and the Backup Exec server. Backup Exec Migrator log files can help you troubleshoot migration issues.

Before you can view the log files, you must enable Backup Exec Migrator logging on the Enterprise Vault server and on the Backup Exec server. To enable Backup Exec Migrator logs on the Enterprise Vault server, edit the Windows registry.

For information on enabling Backup Exec Migrator logging on the Enterprise Vault server, see the following:

<http://entsupport.symantec.com/umi/V-269-27>

You must also enable Backup Exec Migrator logging on the Backup Exec server.

See “[Using the Backup Exec Debug Monitor for troubleshooting](#)” on page 670.

---

**Note:** Partition Recovery Utility log files are enabled by default.

---

After you enable logging on the Enterprise Vault server and on the Backup Exec server, the following types of log files are created:

- VxBSA log files  
For example, <computer\_name>-vxbsa<00>.log
- Partition Recovery Utility log files  
For example, partitionrecovery<00>.log
- Backup Exec server log files  
For example, <computer\_name>-bengine<00>.log

Each time the Backup Exec Migrator is started, separate VxBSA log files are created. As a result, each new log file's sequential number increments by one.

For example, <computer\_name>vxbsa00.log, <computer\_name>vxbsa01.log.

Similarly, a new log file is created each time the Partition Recovery Utility is started. As a result, each new Partition Recovery Utility log file's sequential number increments by one.

For example, partitionrecovery00.log, partitionrecovery01.log

Backup Exec server log file numbers also increment by one as multiple log files are created.

For example, <computer\_name>-bengine00.log, <computer\_name>-bengine01.log

You can find the log files in the following locations.

**Table I-10** Backup Exec Migrator and Partition Recovery Utility log file locations

Log file	Computer	Directory location
VxBSA log files Partition Recovery Utility log files	Enterprise Vault server	C:\Program Files\Symantec\BACKUP EXEC\RAWS\logs
Backup Exec server log files	Backup Exec server	C:\Program Files\Symantec\Backup Exec\Logs

See [“About Backup Exec Migrator events”](#) on page 946.

## About deleting files migrated by Backup Exec Migrator

Enterprise Vault automatically deletes archived items when the item's Enterprise Vault retention periods expire. An Enterprise Vault retention period indicates how long Enterprise Vault retains archived items before it deletes them.

The Backup Exec Migrator maintains existing Enterprise Vault retention periods for archived items when it migrates the archived items to tape. As a result, when an item's data retention period expires, Enterprise Vault issues a command to delete the item from the storage tape that Backup Exec manages. To delete the expired archive item, the .cab file it resides in must be deleted from tape.

---

**Note:** Although the Backup Exec Migrator maintains existing Enterprise Vault retention periods, it does not initiate the deletion of expired archived items or archived partitions from tape. Only Enterprise Vault can initiate the deletion of expired items and partitions.

For more information on deleting expired items, see your Enterprise Vault documentation.

---

Because the .cab files may contain archived items with different retention periods, an expired item may be marked as deleted in the Backup Exec catalogs. However, it may not be immediately deleted from tape. All archived items in a .cab file must have expired retention periods before Enterprise Vault issues a command to delete the .cab file from tape.

Enterprise Vault can also delete entire archived vault store partitions from tape. After you delete an active Enterprise Vault vault store partition by using the Enterprise Vault Administration Console, Enterprise Vault deletes the associated archived partition from tape.

Backup Exec automatically recycles the tapes when all of the items on the tape are marked as deleted in the catalogs. Backup Exec checks for expired Enterprise Vault Migrator media once every 24 hours. If Backup Exec detects such media, it logically moves the media to the Scratch Media set and then generates an information alert informing you of the move.

---

**Note:** Expired Enterprise Vault Migrator media is defined as media that contains only migrated Enterprise Vault data that is marked as deleted in the Backup Exec catalogs.

---

See [“About tape and disk cartridge media”](#) on page 365.

---

**Note:** You should ensure that migrated Enterprise Vault data remains accessible on the tapes that are used for migration purposes until the Enterprise Vault data retention periods expire. Therefore, Symantec recommends that you configure a retention period of 999 years for all tapes that are used for migration purposes.

See [“About media overwrite protection and append periods”](#) on page 369.

---

## Configuring the Backup Exec Migrator

All of the program files that are required to run the Backup Exec Migrator are installed when you install the Agent for Enterprise Vault (Enterprise Vault Agent) on the Enterprise Vault server. However, before you can use the Backup Exec

Migrator, you must configure it to work with both a destination Backup Exec server and the Enterprise Vault server.

**Table I-11** Enterprise Vault configuration process

Step	Description
Step 1	Configure Enterprise Vault collections. See <a href="#">“Vault store partition properties - Collections”</a> on page 950.
Step 2	Configure the Backup Exec Migrator to work with a Backup Exec server. See <a href="#">“Configuring the Backup Exec Migrator to work with a Backup Exec server”</a> on page 951.
Step 3	Configure the Backup Exec Migrator to work with Enterprise Vault. See <a href="#">“Configuring the Backup Exec Migrator to communicate with Enterprise Vault”</a> on page 953.

Use the following configuration recommendations for both the Backup Exec Migrator and the Enterprise Vault partitions:

- Configure the Enterprise Vault partitions to save migrated data locally.  
Do not configure Enterprise Vault partitions to delete files immediately after a migration operation finishes.  
See your Enterprise Vault documentation for details on configuring a partition for migration.
- Configure the Backup Exec server template to run staged migrations.  
See [“About using staged migrations with Backup Exec and the Backup Exec Migrator”](#) on page 945.

Failure to follow the configuration recommendations results in degraded migration and retrieval performance.

## Configuring Enterprise Vault collections

Before you can use the Backup Exec Migrator to migrate Enterprise Vault archived data from a partition, Enterprise Vault first needs to collect the data.

### To configure Enterprise Vault collections

- 1 From the Enterprise Vault Console, navigate to a vault store partition from which you want to migrate data.
- 2 Right-click the partiition, and then click **Properties**.
- 3 On the **Collections** tab, check **Use collection files**.
- 4 Set collection options as appropriate.  
See “[Vault store partition properties - Collections](#)” on page 950.
- 5 Click **OK**.

### Vault store partition properties - Collections

Before you can use the Backup Exec Migrator to migrate Enterprise Vault archived data from a partition, Enterprise Vault needs to collect the data to be migrated.

See “[Configuring Enterprise Vault collections](#)” on page 949.

**Table I-12** Vault store partition properties - Collection options

Item	Description
<b>Use collection details</b>	Lets you set Enterprise Vault as the collector.
<b>Start at</b>	Indicates the local time at which you want collection to start.
<b>End at</b>	Indicates the local time at which you want collection to finish.  Enterprise Vault stops collecting at this time or when it has no more files to collect, whichever comes first.
<b>Limit collection files to &lt;number&gt; megabytes</b>	Indicates the maximum size for collection files.  The default size is 10 MB, although you can specify a file size range from 1 MB to 99 MB.  You may want to change this value to optimize the use of your backup media
<b>Collect files older than</b>	Indicates the amount of time that must elapse since items were archived before they are eligible for collection.

## Configuring the Backup Exec Migrator to work with a Backup Exec server

Use the following steps to configure the Backup Exec Migrator to work with a destination Backup Exec server.

---

**Note:** Symantec recommends that you configure two server storage devices when you configure the Backup Exec Migrator to work with Backup Exec. Configuring two storage devices lets you create a staged migration for your archived Enterprise Vault data.

See [“About using staged migrations with Backup Exec and the Backup Exec Migrator”](#) on page 945.

---

See [“Configuring the Backup Exec Migrator to communicate with Enterprise Vault”](#) on page 953.

### To configure the Backup Exec Migrator to work with a Backup Exec server

- 1 At the Backup Exec server, start Backup Exec.
- 2 Create a logon account that uses the Enterprise Vault server Vault Service account credentials.  
  
Vault Service account credentials are used so that Backup Exec and the Backup Exec Migrator can complete the migration operation  
  
See [“Creating a Backup Exec logon account”](#) on page 500.
- 3 Click the Backup Exec button and then select **Configuration and Settings**.
- 4 Click **Backup Exec Settings**, and then click **DBA-initiated Job Settings**.
- 5 Select the **DEFAULT** template, and then click **Edit**.  
  
You can also use an existing template, or you can create a new template specifically for Enterprise Vault migrations.
- 6 Under **Storage**, select **Any disk storage** as the primary storage location for migrated data, and then set the options you want to use with the device.
- 7 Under **Migrator for Enterprise Vault**, click the down arrow next the field for **Vault Service account credentials**.
- 8 Select the logon account that you created in step 2.  
  
See [“Migrator for Enterprise Vault options”](#) on page 952.
- 9 In the **DBA-initiated Job Settings** dialog box, set other options as appropriate.  
  
See [“Editing DBA-initiated job templates”](#) on page 485.
- 10 Do one of the following:

If you want to configure staged migrations Do the following in the order listed.

See “[About using staged migrations with Backup Exec and the Backup Exec Migrator](#)” on page 945.

- Under **Duplicate Job Settings**, check **Enable settings to duplicate backup sets for this job**.
- In the **Storage** list, select a type of storage.
- Set other options as appropriate. See “[Duplicate job settings for DBA-initiated jobs](#)” on page 494.
- Click **OK**.

If you do not want to configure staged migrations Continue with step 12.

**11** Click **OK**.

**12** Configure Backup Exec Migrator to work with Enterprise Vault.

See “[Configuring the Backup Exec Migrator to communicate with Enterprise Vault](#)” on page 953.

## Migrator for Enterprise Vault options

The Backup Exec Migrator uses the Enterprise Vault server Vault Service account during the Backup Exec Migrator to Backup Exec server authentication process.

**Table I-13** Migrator for Enterprise Vault options

Item	Description
<b>Vault Service account credentials</b>	<p>Specifies the Enterprise Vault server Vault Service account credentials to use so that Backup Exec and the Backup Exec Migrator can complete the migration operation.</p> <p>The Vault Service account must be included in either the Administrators group or the Backup Operators group at the Backup Exec server.</p> <p><b>Note:</b> If the Enterprise Vault server and the Backup Exec server are in different domains, a trust relationship must be established between the domains. The Vault Service account user must be a trusted user at the Backup Exec server. Trust relationships are required so that the Microsoft Security Support Provider Interface (SSPI) can authenticate the Vault Service account user.</p> <p>For more information on domain trust relationships, see your Microsoft documentation.</p>
<b>New</b>	<p>Lets you create a new logon account or edit an existing account.</p> <p>See <a href="#">“Creating a Backup Exec logon account”</a> on page 500.</p>

See [“Configuring the Backup Exec Migrator to work with a Backup Exec server”](#) on page 951.

## Configuring the Backup Exec Migrator to communicate with Enterprise Vault

Use the following steps to configure the Backup Exec Migrator to communicate with Enterprise Vault.

See [“Configuring the Backup Exec Migrator”](#) on page 948.

### To configure the Backup Exec Migrator to communicate with Enterprise Vault

- 1 At the Enterprise Vault server, navigate to a vault store partition from which to migrate data.
- 2 Right-click the vault store partition, and then click **Properties**.

- 3 On the **Migration** tab, check **Migrate files**.
- 4 In **Remove collection files from primary storage**, set the time period for this option to something longer than zero days.

Do not set it to zero days. Setting the time period to zero days causes Enterprise Vault to immediately delete the migrated data from the partition. More importantly, it causes the Backup Exec Migrator to create separate migration jobs for each partition folder being migrated during a migration period. If separate jobs are created, the resulting overhead that is required to run the jobs results in degraded migration and retrieval performance.

See [“Configuring the Backup Exec Migrator”](#) on page 948.

- 5 Set other migration options as appropriate.  
See [“Vault store partition properties - Migration options”](#) on page 955.
- 6 On the **Advanced** tab, ensure that **Symantec Backup Exec** appears in the **List setting from** field.

- 7 In the window below the **List setting from** field, select **Backup Exec server**.

- 8 Click **Modify**.

- 9 Type the name or the IP address of the destination Backup Exec server.

- 10 Click **OK**.

- 11 Select **Backup Exec DBA-initiated template**.

- 12 Click **Modify**.

- 13 Enter the name of an existing template that uses the Enterprise Vault server Vault Service account credentials.

The template that you select must be configured to use the Enterprise Vault server Vault Service account. The template you use must also match the template name that you used when you configured the Backup Exec Migrator to work with a Backup Exec server.

See [“Configuring the Backup Exec Migrator to work with a Backup Exec server”](#) on page 951.

- 14 Click **OK**.

- 15 Ensure that the name of the template that contains the Enterprise Vault server Vault Service account credentials appears in the **Setting** pane.

See [“Configuring the Backup Exec Migrator to work with a Backup Exec server”](#) on page 951.

- 16 To test the communications between the Enterprise Vault server and the Backup Exec server, click **Test Configuration**.

- 17 If the test fails, ensure that you used the correct credentials for the Vault Service account , and then click **Test Configuration** again.
- 18 Click **OK** after the test successfully completes.
- 19 Click **OK**.

### Vault store partition properties - Migration options

Select the Enterprise Vault migration property options that you want to use.

**Table I-14** Vault store partition properties - Migration options

Item	Description
<b>Migrate files</b>	Lets you migrate archived Enterprise Vault data to a Backup Exec storage device.  Migration can help reduce storage costs by moving collection files to tertiary storage devices. However, retrieval times can increase.  See your Enterprise Vault documentation.
<b>Migrator</b>	Indicates the name of the migration application.  <b>Symantec Backup Exec</b> must appear in this field.
<b>Migrate files older than</b>	Indicates the amount of time that must elapse since files were last modified before they are eligible for migration.  See your Enterprise Vault documentation.

**Table I-14** Vault store partition properties - Migration options (*continued*)

Item	Description
<p><b>Remove collection files from primary storage</b></p>	<p>Indicates the age at which migrated collection files are removed from the primary storage location.</p> <p>Files that have been migrated to Backup Exec storage media can remain in their primary location for the period of time you specify.</p> <p><b>Note:</b> Symantec recommends that you set the time period for this option to something longer than zero days, with a longer time period being best. Do not set it to zero days. Setting the time period to zero days causes the Backup Exec Migrator to create separate migration jobs in a migration period for each partition being migrated. If separate jobs are created, the resulting overhead that is required to run the jobs results in degraded migration and retrieval performance.</p> <p>See <a href="#">“Configuring the Backup Exec Migrator”</a> on page 948.</p>

See [“Configuring the Backup Exec Migrator to communicate with Enterprise Vault”](#) on page 953.

## About viewing migrated Enterprise Vault data

The Backup Exec **Backup Sets** view shows the migrated items for the Enterprise Vault partition. In the **Backup Sets** view, backup sets containing the migrated .cab files appear under a partition name that reflects the Enterprise Vault partition from which the data was migrated. Because the **Backup Sets** view displays the archived data in a read-only mode, you cannot select the data for restore. However, you can retrieve the data in the application where the data resides.

See [“Viewing the contents of backup sets”](#) on page 217.

---

**Note:** You can completely retrieve of all archived items that appear in the **Backup Sets** view by using the Partition Recovery Utility.

See [“About the Partition Recovery Utility”](#) on page 958.

---

See [“About retrieving migrated Enterprise Vault data”](#) on page 957.

## About retrieving migrated Enterprise Vault data

All file retrieve operations start from the Enterprise Vault server console. You cannot restore archived Enterprise Vault data from Backup Exec.

When files are migrated from a partition, Enterprise Vault creates a shortcut in the partition that replaces the migrated file. The shortcut also links to the storage location of the migrated file. You retrieve files by double-clicking their shortcuts in the Enterprise Vault partition itself. If a partition retains a local copy of the migrated files, Enterprise Vault retrieves the files from the local copies. If Enterprise Vault deletes the migrated files because the partition's file retention period passes, the requested files must be retrieved from Backup Exec storage media.

**Table I-15** How migrated data is retrieved

Action	Notes
Enterprise Vault works with the Backup Exec Migrator to begin the process.	The Backup Exec Migrator identifies the Backup Exec server where the files are stored.
The Backup Exec Migrator schedules a Backup Exec restore job at the server.	Backup Exec restores the requested files.
The Backup Exec Migrator migrates the restored files to the Enterprise Vault server partition from the Backup Exec server.	The Backup Exec Migrator moves the restored files to a location specified by Enterprise Vault, using the name provided by Enterprise Vault.

The retrieval process is automatic after you start the operation at the Enterprise Vault server. It requires no user intervention other than perhaps placing a tape in the tape device if you removed the storage media.

See [“Retrieving migrated Enterprise Vault data”](#) on page 957.

### Retrieving migrated Enterprise Vault data

Use the following steps to restore migrated Enterprise Vault files.

---

**Note:** To successfully retrieve the files you want, you may need to place a tape in a tape drive at the Backup Exec server.

---

### To retrieve migrated Enterprise Vault data

- 1 At the Enterprise Vault server, navigate to the partition where you want to retrieve the data.
- 2 Double-click the file that you want to retrieve.

## About the Partition Recovery Utility

The Partition Recovery Utility is a command-line application that is automatically installed when you install the Backup Exec Agent for Windows. The utility lets you restore all of a partition's archived files from the Backup Exec storage media in a single operation. You can also use it to recover the archived partition data for each of the Enterprise Vault partitions in a disaster recovery situation.

After you use the Partition Recovery Utility, you can review recovery details by looking at the Backup Exec job history for each Enterprise Vault server where the recovery occurs.

See [“Partition Recovery Utility requirements”](#) on page 958.

See [“Finding an archive ID”](#) on page 959.

See [“Starting the Partition Recovery Utility”](#) on page 959.

### Partition Recovery Utility requirements

You must know the following when you use the Partition Recovery Utility:

- The vault store partition name for the data that you want to recover.
- The Archive ID of the partition data that you want to recover.
- An Enterprise Vault server user account with Vault Service Account privileges.

---

**Note:** If you run the Partition Recovery Utility on a Windows Server 2008/2008 R2 computer, administrator privileges are required.

---

In addition, the Partition Recovery Utility must run at the Enterprise Vault server that originally migrated the data you want to restore.

See [“Finding an archive ID”](#) on page 959.

See [“Starting the Partition Recovery Utility”](#) on page 959.

## Finding an archive ID

You use the archive ID of the data you want to restore along with the vault store partition name when you run the Partition Recovery Utility. The archive ID is an alpha-numeric number of considerable length.

For example, 1D69957C6D917714FB12FEA54C9A8299A1110000ev8archive.EVMBE

You can find the Archive ID listed among the properties of an archived file set.

### To find an archive ID

- 1 In the left view of the the Enterprise Vault Administration Console, expand **Archives**.
- 2 Navigate the folder structure and select the folder of the type for data you want to restore.
- 3 In the right view, right-click an archive, and then select **Properties**.
- 4 On the **Advanced** tab, note the archive ID at the bottom.

See “[Starting the Partition Recovery Utility](#)” on page 959.

## Starting the Partition Recovery Utility

Use the following steps to start the Partition Recovery Utility.

### To start the Partition Recovery Utility

- 1 From the Enterprise Vault server, open a Windows command prompt.
- 2 Navigate to the Enterprise Vault Agent installation directory.  
For example, C:\Program Files\Symantec\Backup Exec\RAWS
- 3 Do the following:

If you start the Partition Recovery Utility on a Windows Server 2008/2008 R2 computer	Type the following command: <pre>runas /user:&lt;domain\administrator&gt; partitionrecovery.exe -vs &lt;vault_store_name&gt; -ap &lt;archive_ID&gt;</pre>
---	--

If you start the Partition Recovery Utility on all other supported Windows operating system versions	Type the following command: <pre>partitionrecovery.exe -vs &lt;vault_store_name&gt; -ap &lt;archive_ID&gt;</pre>
--	---

- 4 Press **Enter**.

See [“About the Partition Recovery Utility”](#) on page 958.

## Best practices for using the Backup Exec Migrator

Consider the following best practices when you use the Backup Exec Migrator:

- Symantec recommends that you regularly back up the Backup Exec catalogs. In the event the catalogs become corrupt, you can restore them from backups. After you restore the catalogs, you must re-catalog the storage media on which Backup Exec Migrator data is stored. Re-cataloging the storage media ensures that the latest catalog entries are available.
- For best performance, configure the Backup Exec Migrator to migrate data to a backup-to-disk folder and then to a tape device by using a duplicate job. See [“About using staged migrations with Backup Exec and the Backup Exec Migrator”](#) on page 945. See [“About duplicating backed up data”](#) on page 218.
- In the Enterprise Vault **Migration** options tab, set the time period for **Remove collection files from primary storage** to something longer than zero days. Setting the time period to zero days causes Enterprise Vault to immediately delete the migrated data from the partition.

If you set the time period to zero days, Symantec recommends the following:

- Increase the number of concurrent jobs that are allowed for the backup-to-disk folder you use for migration purposes. Increase the number of concurrent jobs based on the following formula:  
<number of recommended concurrent jobs> = <number of installed tape drives plus two>

For example, if you have two installed tape drives, you should configure the backup-to-disk folder to allow four concurrent jobs.

Concurrent jobs let the Backup Exec Migrator continue to migrate data to disk storage while tape drives process duplicate jobs in a staged migration environment.

---

**Note:** You can increase the number of concurrent jobs that run by increasing the total concurrency level of the backup-to-disk devices.

---

- Symantec recommends that you first collect all of the archived files in one collection and migration operation and then migrate them in the next collection and migration operation. This process helps ensure that the Backup Exec Migrator creates a single job for each migration operation, which improves the migration performance.

See [“About the Backup Exec Migrator for Enterprise Vault”](#) on page 940.

## Troubleshooting Backup Exec Migrator and Partition Recovery Utility issues

Review the following error messages for possible solutions to errors that you may encounter:

- The Backup Exec Migrator logs migration activity in the Windows Event Viewer and in the Enterprise Vault Dtrace Utility on the Enterprise Vault server. It also logs migration activity on the Backup Exec server. The details that are provided in the log files can help you troubleshoot issues with the Backup Exec Migrator.  
See [“About Backup Exec Migrator events”](#) on page 946.  
See [“About Backup Exec Migrator logs”](#) on page 946.
- The Partition Recovery Utility cannot find any files to be recalled. There are no file to be recalled from the vault store database using the Archive ID that you provided.
- The Partition Recovery Utility operation will be terminated due to a user request. You may have stopped the Partition Recovery Utility operation by pressing **Ctrl + C** or **Ctrl + Break**.
- The migrated file name <file\_name> with ID <migrated\_file\_id> was not found in the Backup Exec backup sets. The recall is skipped for this file. The Partition Recovery Utility skips collection files if they already exist in the vault store database. To restore the files, delete them from the vault store database, and then run the Partition Recovery Utility again.
- The Partition Recovery Utility cannot find any partitions. Ensure that the name of the vault store is valid, and that there are partitions in the vault store. The vault store name that you provided may be invalid.

See [“About the Backup Exec Migrator for Enterprise Vault”](#) on page 940.

See [“About the Partition Recovery Utility”](#) on page 958.



# Symantec Backup Exec Agent for Lotus Domino

This appendix includes the following topics:

- [About the Agent for Lotus Domino Server](#)
- [Lotus Domino Agent requirements](#)
- [About installing the Lotus Domino Agent on the Backup Exec server](#)
- [About the Lotus Domino Agent and the Domino Attachment and Object Service \(DAOS\)](#)
- [Viewing Lotus Domino databases](#)
- [About backing up Lotus Domino databases](#)
- [About restoring Lotus Domino databases](#)
- [How to prepare for disaster recovery on a Lotus Domino server](#)
- [Recovering a Lotus Domino server from a disaster](#)
- [About disaster recovery of a Lotus Domino server using archive logging](#)
- [Disabling the monitor change journal](#)
- [Recovering the Lotus Domino server, databases, and transaction logs when archive logging is enabled](#)
- [Re-enabling the monitor change journal](#)
- [Recovering of a Lotus Domino server that uses circular logging](#)

## About the Agent for Lotus Domino Server

The Symantec Backup Exec Agent for Lotus Domino Server (Lotus Domino Agent) lets you back up and restore Lotus Domino on local Backup Exec servers and on remote computers. The Lotus Domino Agent backs up Lotus Domino databases, Domino Attachment and Object Service (DAOS) - related NLO files, and transaction logs. You can integrate Lotus Domino database backups with regular server backups without separately administering them or using dedicated hardware.

The Lotus Domino Agent provides support for the following:

- Dynamic inclusion
- Full and incremental online backups of Lotus Domino databases, DAOS-related NLO files, and transaction logs using Lotus Domino APIs.
- Restores of Lotus Domino databases, .nlo files, archived transaction logs, and point-in-time restores.
- Recycling of archived Lotus Domino transaction logs after a successful backup.
- Flexible scheduling capabilities.
- Backup of DAOS-related NLO files when DAOS is configured on a remote share.
- Backup and restore of partitioned and clustered Lotus Domino servers.
- Lotus Domino databases in a Microsoft Cluster Server cluster in both Active-Active and Active-Passive configurations.

See [“Backing up data”](#) on page 163.

See [“About stages”](#) on page 183.

See [“Editing backups”](#) on page 170.

See [“Setting default backup job settings”](#) on page 456.

## Lotus Domino Agent requirements

The Agent for Lotus Domino Server (Lotus Domino Agent) supports the backup and restore of Lotus Domino versions 7.x and 8.x.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

Following are the requirements for backing up Lotus Domino database files residing on the Backup Exec server, or for remote Windows computers and workstations.

---

**Note:** Backup Exec does not support two versions of Lotus Domino on the same computer.

---

If the Lotus Domino files you want to back up are on the local Backup Exec server, the server must have the following:

- Backup Exec
- An Intel-compatible processor
- The Lotus Domino data directory on the Lotus Domino server

If the Lotus Domino files you want to back up are on a remote computer, the remote computer must have the following:

- Windows operating system
- Backup Exec Agent for Windows
- An Intel-compatible processor
- Corresponding Windows Administrative Share for each volume that contains Lotus Domino databases
- The Lotus Domino data directory on the Lotus Domino server

The following are required to back up Lotus Domino transaction logs:

- The Lotus Domino archive-style transaction logging must be enabled to perform incremental backups and to perform point in time recovery.

The following are required to back up Lotus Domino DAOS-related NLO files:

- The DAOS state must be in read-only mode or enabled.
- The DAOS catalog should be synchronized.

If the Lotus Domino databases are running in a Microsoft Cluster Server cluster, you must have the following:

- Lotus Domino must be running on a Microsoft Cluster Server cluster. For more information, see your Lotus Domino documentation for instructions for setting up Lotus Domino in a Microsoft Cluster Server cluster.
- The Backup Exec Lotus Domino Agent must be installed on all nodes in the Microsoft Cluster Server cluster.

See [“About installing the Lotus Domino Agent on the Backup Exec server”](#) on page 966.

## About installing the Lotus Domino Agent on the Backup Exec server

The Symantec Backup Exec Agent for Lotus Domino Server (Lotus Domino Agent) is installed as part of the Agent for Applications and Databases. It can back up local or remote Lotus Domino databases.

See [“Using a command prompt to install the Agent for Windows on a remote computer”](#) on page 94.

---

**Note:** If you install Lotus Domino on the same server on which Backup Exec is already installed, you must restart Backup Exec services to display Lotus Domino database selections.

---

See [“About backing up Lotus Domino databases”](#) on page 968.

See [“Starting and stopping Backup Exec services”](#) on page 511.

See [“Editing backups”](#) on page 170.

See [“About searching for and restoring data”](#) on page 229.

## About the Lotus Domino Agent and the Domino Attachment and Object Service (DAOS)

Lotus Domino 8.5 incorporates the Domino Attachment and Object Service (DAOS). DAOS-enabled databases (DAOS databases) save significant hard drive space by sharing data between applications on a server. DAOS databases do not save separate copies of every document attachment. Instead, DAOS databases save a single copy of a file attachment to an internal repository. The databases then create and save reference pointers to the stored file attachments.

File attachments are saved to the internal repository with the .nlo file extension. During a full backup of the entire Lotus Domino server, Backup Exec backs up all .nlo files, along with the Domino <server>.id file.

Backup Exec adds one container per partition under **Lotus Domino Databases** called **Domino Attachment and Object Service** in the restore selections view. All backed up DAOS NLO files reside in backup sets under **Domino Attachment and Object Service**. In addition, all backed up <server>.id files reside in the **Databases** container under **Lotus Domino Databases**.

---

**Note:** Domino uses `<server>.id` for NLO encryption purposes. If you enable NLO file encryption at the Domino server, the `<server>.id` file must be backed up.

---

When you select individual DAOS-enabled databases for backup, the referenced `.nlo` files for each database are included in the backup job. However, the `<server>.id` file is excluded.

With incremental backups, only the databases and the `.nlo` files that are created since the last full backup of the server are backed up.

---

**Note:** In cases where incremental backup jobs fully back up DAOS-enabled databases, all of the `.nlo` files that each database references are backed up. This scenario occurs when DAOS-enabled databases use circular logging, or when DAOS-enabled databases are in archive log mode and their DBIID changes.

---

During a full DAOS-enabled Domino database restore, all database data, `.nlo` files, and the `<server>.id` file are restored. When you restore individual DAOS-enabled databases, Backup Exec restores all database data, including the `.nlo` files. However, Backup Exec does not restore any `.nlo` files that match `.nlo` files in the internal repository. After the DAOS-enabled databases are restored, Backup Exec resynchronizes the Domino DAOS catalog.

During a point-in-time restore of a DAOS-enabled database, some required `.nlo` files may not be generated when the archive transaction logs are replayed. When this condition occurs, Backup Exec reports the names of the missing `.nlo` files. You can individually restore the missing `.nlo` files and then start a Domino DAOS catalog resynchronization operation at the Domino server.

---

**Note:** Only the `.nlo` files that change are backed up when DAOS-enabled databases are in archive log mode and their DBIIDs do not change.

---

For information on Domino DAOS catalog resynchronization operations, see your Lotus Domino documentation.

See [“About the Agent for Lotus Domino Server”](#) on page 964.

## Best practices for restoring the missing `.nlo` files

If you decide to individually restore the missing `.nlo` files, Symantec recommends the following best practices:

- Always restore the `.nlo` files to the internal repository of the current DAOS-enabled Domino server.

- Instead of making random .nlo files selections, select all of them when you make your selections in the restore selections view. Then use the restore option, **Skip if file exists**. By using the **Skip if file exists** option, Backup Exec restores only the missing .nlo files.  
See [“About redirecting the restore of DAOS NLO files”](#) on page 977.

## Viewing Lotus Domino databases

Use the following steps to view Domino databases that are on both local and remote servers.

Lotus Domino transaction logs do not appear under **Lotus Domino Databases**; however, when you select the database for backup, the transaction logs are automatically included.

The same process applies to DAOS NLO files. They do not appear under **Lotus Domino Databases**; however, when you select the database for backup, the .nlo files are automatically included.

See [“About backing up Lotus Domino databases”](#) on page 968.

### To view Lotus Domino databases on both local and remote servers

- 1 On the **Backup and Restore** tab, right-click a Lotus Domino server.
- 2 On the **Backup** menu, select a backup option that you want to use.
- 3 In the selections box, click **Edit**.
- 4 Expand **Lotus Domino Databases**.
- 5 Expand each folder under **Lotus Domino Databases** until a database folder named appears.
- 6 Click each database folder, and then view the Lotus Domino databases in the right pane.

## About backing up Lotus Domino databases

When a Lotus Domino backup job is submitted, Backup Exec uses Lotus Domino APIs to obtain the backup of the database. When you back up a DAOS-enabled Domino database, the DAOS NLO files are automatically included. In addition, the transaction logs associated with the Lotus Domino databases are included in the backup only if archive logging is turned on at the server. If they are backed up, the archive logs and the DAOS NLO files are stored in a separate backup set that is stored along with the Lotus Domino database backup set.

The Agent for Lotus Domino Server (Lotus Domino Agent) supports the backup of the following types of files:

- .ntf - Lotus Notes Template Files
- .nsf - Lotus Notes Database Files
- .box - Lotus Mailbox Files
- .dsk - Cache Files
- .txn - Transaction log files
- .nlo - DAOS attachment files

---

**Note:** Transaction log files and DAOS attachment files do not appear in the Backup Exec backup selections view; however, they do appear in restore selections view.

---

You must back up .nsf, .ntf, and .box files to properly recover Lotus Domino databases. If you want to back up .njf, .ncf, .id, .dic, or notes.ini files, you must select them for backup from the volume in which the Lotus Domino Program directory is located.

The Domino agent uses the full and incremental backup methods to back up Lotus Domino databases. An incremental backup is smaller and faster than a full backup because only archived transaction logs, DAOS NLO files, unlogged databases, and logged databases with DBIIDs that have changed are backed up.

---

**Note:** The full backup method should be used when the DBIID for the database has changed since previous transactions cannot be applied to the new database.

---

Although DAOS and non-DAOS Domino servers use additional Domino-related databases and support files, Backup Exec does not back them up. Domino automatically recreates the items after you restart the Domino servers.

Backup Exec excludes the following support files from backup jobs:

- daos.cfg
- daoscat.nsf
- dbdirman.nsf

---

**Note:** You cannot back up databases to devices that are attached to a computer on which the Remote Media Agent for Linux Servers is installed.

---

See [“Lotus Domino Agent backup options”](#) on page 970.

See [“Backing up data”](#) on page 163.

See [“Editing backups”](#) on page 170.

See [“Editing a stage”](#) on page 184.

## About selecting backup options for Lotus Domino databases

You should back up Lotus Domino databases during off-peak hours and disable third-party Lotus Domino agents before you run the backup. The archived transaction logs are included automatically.

All Lotus Domino databases and transaction logs that reside on single or multiple volumes must be backed up by the same Backup Exec server. In addition, you should not back up a Lotus Domino server simultaneously from multiple Backup Exec servers.

See [“Backing up data”](#) on page 163.

## Lotus Domino Agent backup options

The following option is available for Agent for Lotus Domino Server (Lotus Domino Agent) backup jobs. This option appears when you select **Lotus Domino** on the **Backup Options** dialog box, and when the backup definition for the Domino backup job includes the incremental backup method.

**Table J-1** Lotus Domino Agent incremental backup method option

Item	Description
<b>Mark archive logs for recycling</b>	Reuses the transaction log after it has been backed up.  Backup Exec will not delete the transaction log. Selecting this option only indicates that the transaction log is ready to be reused after it has been backed up successfully; the Lotus Domino server actually deletes the transaction logs.  This option is selected automatically when you select the full backup method. You cannot clear this option when you are using the full backup method.

## About automatic exclusion of Lotus Domino files during volume-level backups

If you select a volume that contains Lotus Domino data for backup, the Agent for Lotus Domino Server (Lotus Domino Agent) determines which Domino data should not be included in a volume level backup. For example, .ntf and .nsf files, nlo files, <server>.id files, as well as any active log files, should not be part of the backup because they are opened for exclusive use by the Lotus Domino system. These files will be automatically excluded for backup by a feature called Active File Exclusion. If this exclusion did not happen during a non-snapshot backup, these files would appear as in use - skipped. If this exclusion did not happen during a snapshot backup, the files would be backed up in a possible inconsistent state, which could create restore issues.

See [“Backing up data”](#) on page 163.

See [“Lotus Domino Agent backup options”](#) on page 970.

## About supported Lotus Domino database configurations

You can back up the following types of Lotus Domino database configurations using the Agent for Lotus Domino Server (Lotus Domino Agent):

- **Domino Server Databases.**

Domino Server databases can be Logged or Unlogged, with their DAOS states being not-enabled, read-only, or enabled. DAOS cannot be enabled on Domino databases that do not use logging. Domino databases are located in a folder in the Domino data directory, typically Lotus\Domino\Data, but may also be linked to the Domino data directory using Lotus Linked Databases.

The following types of Lotus Domino databases are supported:

- **Logged Domino Server Databases.**

A logged Domino Server database logs transactions for one or more Lotus databases. If transaction logging is enabled on the server, all database transactions go into a single transaction log.

- **Unlogged Domino Server Databases.**

An unlogged Domino Server database does not have transaction logging enabled, or the transaction logging has been disabled for specific server databases. Unlogged Domino Server databases will be backed up in their entirety when a full or incremental backup is performed, but the database can only be restored to the point of the latest database backup.

- **Local Databases.**

Lotus databases are considered Local when they cannot be found in the Domino data directory, cannot be shared, and cannot be logged. This type of database

requires a backup of the database itself when using any of the Lotus Domino backup methods. The database can be restored only to the point of the latest database backup.

See [“About Lotus Domino transaction logs”](#) on page 972.

See [“About selecting backup options for Lotus Domino databases”](#) on page 970.

## About Lotus Domino transaction logs

Lotus Domino has the ability to log transactions for one or more Lotus Domino databases. Lotus Domino databases are logged by default when transaction logging is enabled on the Lotus Domino server and the database is in the Domino data directory.

When transaction logging is enabled on the server, each Lotus Domino database is assigned a database instance ID (DBIID). Each transaction recorded in the log includes the DBIID, which is used to match transactions to the database during a restore.

A new DBIID may be assigned to the database when some Lotus Domino operations are performed. When the new DBIID is assigned, all new transactions recorded in the log use the new DBIID; however, previous transactions have the old DBIID and will not match the new DBIID for the database. To prevent data loss, it is recommended that a full backup be performed when a database receives a new DBIID since transactions with the old DBIID cannot be restored to the database. A full backup includes all current transactions on the database and ensures that only the transactions with the new DBIID are needed to restore the database.

You can select only one logging style when transaction logging is enabled on the server.

Following are the two styles of logging for Lotus Domino databases:

- **Archive logging.**

This logging style produces a transaction log that is limited only by the capacity of your mass storage. Archive logging is the recommended logging style to be used with the Lotus Domino Agent since all the transaction logs can be backed up and marked for recycling. When the transaction logs are recycled the Lotus Domino server reuses the existing transaction logs after they are backed up to create space for new transaction logs.

- **Circular logging.**

This logging style reuses the log file after a specific log file size is reached. By reusing the log file you are saving resources; however, you are also limiting your recovery options because the database can only be recovered to the point of the last full backup. If the incremental backup method is selected for a

backup job, a full backup of the changed databases is performed since transaction logs cannot be backed up.

---

**Caution:** When circular logging is enabled, the circular transaction log cannot be backed up, which could result in the loss of changes made to the database since the last backup was performed.

---

See [“About supported Lotus Domino database configurations”](#) on page 971.

See [“About selecting backup options for Lotus Domino databases”](#) on page 970.

## About restoring Lotus Domino databases

To restore data, selections should be made in the Restore Wizard from the backup set that contains the Lotus Domino databases; the required transaction logs and the DAOS NLO files are automatically restored with the selected database.

Lotus Domino data is usually contained in the most recent backup set. However, some subsequent incremental backup jobs run after a full backup job may not contain data in the backup set because only the transaction log was backed up. If the data you want to restore is not located in the most recent backup set, check the previous backup sets until you find the data.

---

**Note:** If a new DBIID has been assigned to databases and you run an incremental backup, the data will be contained in the most recent backup set since transactions with the new DBIID will not match the old DBIID.

---

---

**Note:** When restoring Lotus Domino databases to Microsoft Cluster Server cluster, the virtual computer name or the virtual IP address of the Domino server should be used when browsing or making Domino database selections in the **Resource View** tab in the Restore Wizard.

---

Restore options for Lotus Domino databases are set using the Restore wizard. The wizard provides definitions for Domino-specific restore options.

When you select a Lotus Domino backup set to restore, all database files and necessary transaction logs are automatically restored. You can also choose to restore specific database files.

See [“Lotus Domino Agent restore options”](#) on page 975.

See [“About searching for and restoring data”](#) on page 229.

## Restoring Lotus Domino databases

Restoring a Lotus Domino database is a three-part process.

**Table J-2** Restoring a Lotus Domino database

Step	Description
Step 1	<p>Restore database files to the Domino server.</p> <p>During a restore of the Lotus Domino database, the existing database is taken offline and deleted, the database is restored, and changed records contained in the backup job are applied to the database.</p> <p><b>Note:</b> Domino servers include databases with names such as <code>admin4.nsf</code>, <code>names.nsf</code>, and <code>busytime.nsf</code>. The Notes client computers include databases with names such as <code>bookmark.nsf</code>, <code>cache.dsk</code>, and <code>homepage.nsf</code>. These databases are critical and cannot be taken offline when the Domino server is running. In addition, you should only restore these databases in disaster recovery situation.</p> <p>If the database is unlogged or local, the database is brought back online. If the database is logged and multiple databases are being restored, the database name is added to a list for recovery. During the restore process, Backup Exec assigns a unique name to databases and then before databases are brought online, reassigns the original name. Changing the name during the restore process has no effect on restored databases.</p>
Step 2	Restore DAOS-related NLO files that are missing.

**Table J-2** Restoring a Lotus Domino database (*continued*)

Step	Description
Step 3	<p>Run transaction logs to bring the database up-to-date.</p> <p>The internal Domino recovery process automatically begins after the DAOS NLO files are restored to the server. The database is restored to a point in time using transactions from the required transaction logs. Required transaction logs that were backed up and recycled are also included in the recovery process. After the recovery process completes, the Lotus Domino database is brought online.</p> <p>If you back up your Lotus Domino databases regularly, then restoring the most recent backup set containing the Lotus Domino data is all that is required to restore the most recent backups of your Lotus Domino databases.</p> <p><b>Note:</b> If circular logging is enabled and both the databases and the Domino transaction logs are lost, the database can only be recovered to the point of the last full backup.</p>

Use the same procedures to restore a server in a Microsoft Cluster Server cluster that you use to restore a server in a non-clustered environment.

When restoring a Lotus Domino database to a MCSC cluster and a failover occurs during the restore operation, active restore jobs are paused for 15 minutes as they wait for existing connections to resolve themselves. If the restore job does not restart before the failover time-out period expires, the job fails. If this occurs, the restore job must be resubmitted.

See [“About restoring Lotus Domino databases”](#) on page 973.

## Lotus Domino Agent restore options

The following options are available for Agent for Lotus Domino Server (Lotus Domino Agent) restore jobs. These options appear when you run the **Restore Wizard**.

See [“Lotus Domino Agent backup options”](#) on page 970.

**Table J-3** Lotus Domino restore options

Item	Description
<b>To the latest available backup set time</b>	Uses the latest available backup set time when multiple backup sets are available for restore.
<b>To a point in time in the transaction log up to and including the specified time</b>	<p>Specifies the date and time to restore the database. The option is only available for logged databases when the archive logging style is set. Backup Exec will restore the Lotus Domino database you selected in the Restore selections dialog box and then automatically restore the necessary transaction logs required to bring the databases up to the date and time specified.</p> <p>If a point in time is not specified, the databases will be restored up to the last committed transactions in the log file.</p> <p>This option may require additional time since the archived transaction logs are also restored.</p>
<b>Specify the number of seconds to wait for a database to go offline</b>	Specifies the number of seconds for the restore process to wait for a database that is in use. When a Lotus database is restored it must first be taken offline. This will ensure that the database is not being accessed, closed, or deleted while the restore operation is being processed. If the database is still in use and cannot be taken offline after the specified wait time, the restore will fail.
<b>Retain original database ID</b>	Restores the original database ID.
<b>Assign new database ID</b>	Assigns new IDs to the database.
<b>Assign new database ID and replica ID</b>	Assigns new IDs to the database. A replica ID is used to synchronize two or more databases that are being replicated in the Lotus Domino environment. You can assign a new replica ID during a restore to prevent other databases under replication from overwriting the restored database files.

## About redirecting restore jobs for Lotus Domino databases

The Backup Exec logon account must have administrative credentials on the server to which you want to redirect the backup of the Lotus Domino server. Lotus Domino databases can only be redirected to a different directory on the local server from which the database was backed up. If you are restoring a database to a different location, it must reside in or under the Lotus Domino data directory. Point in time restores cannot be redirected.

---

**Note:** Redirecting the restore of a DAOS-enabled Domino database does not restore the nlo files.

---

See [“About searching for and restoring data”](#) on page 229.

See [“Creating a Backup Exec logon account”](#) on page 500.

## About redirecting the restore of DAOS NLO files

You can restore DAOS NLO files without restoring the entire DAOS-enabled Domino database. When you restore the DAOS NLO files you must specify a redirection destination path. In most cases, the path points to the DAOS internal repository that you set when you configured Lotus Domino.

See [“About searching for and restoring data”](#) on page 229.

See [“About the Lotus Domino Agent and the Domino Attachment and Object Service \(DAOS\)”](#) on page 966.

# How to prepare for disaster recovery on a Lotus Domino server

A Disaster Preparation Plan is necessary for restoring Lotus Domino databases efficiently and effectively in the event of a catastrophic failure. The goal is to minimize the time to recover. Developing a backup strategy for your Windows computers and Lotus Domino databases is the critical part of this plan.

When developing a strategy for backing up your Lotus Domino databases, consider the following recommendations:

- Keep linked databases on one volume. This allows Backup Exec to synchronize the databases before they are backed up.
- Back up active databases often. This reduces the amount of effort required to update the databases to the point following the most recent backup.

- Ensure that the notes.ini, cert.id, and <server>.id files are protected and available if a disaster occurs.
- Configure the DAOS prune period as recommended in the Lotus Domino documentation. However, Symantec recommends that you do not set the DAOS prune period for a period less than the time between two Domino backups.

See [“Recovering a Lotus Domino server from a disaster”](#) on page 978.

See [“About disaster recovery of a Lotus Domino server using archive logging”](#) on page 979.

See [“Recovering of a Lotus Domino server that uses circular logging”](#) on page 982.

## Recovering a Lotus Domino server from a disaster

Recovering a Lotus Domino system can be performed in the following ways:

- Manually  
See [“About manual disaster recovery of Windows computers”](#) on page 637.
- By using Backup Exec’s Simplified Disaster Recovery  
See [“About Simplified Disaster Recovery”](#) on page 704.

When you recover a DAOS-enabled Domino server from a disaster, all of the .nlo files that each recovered Domino database references are automatically restored.

---

**Note:** Disaster recovery of a Lotus Domino server in a Microsoft Cluster Server cluster uses the same steps as recovering a Domino server in a non-clustered environment.

---

Use the following steps as a guide when you want to do a disaster recovery operation on a Lotus Domino server.

**Table J-4** Steps to take to recover a Lotus Domino server form a disaster

Step	Description
Step 1	Recover the Windows computer.
Step 2	Disable the monitor change journal. See <a href="#">“Disabling the monitor change journal”</a> on page 980.

**Table J-4** Steps to take to recover a Lotus Domino server form a disaster  
(continued)

Step	Description
Step 3	<p>Recover or re-install Lotus Domino to the same location as before the disaster occurred.</p> <p>All Lotus Domino system data must be recovered. System data includes log.nsf, names.nsf, template files, notes.ini, mail.box, and ID files.</p> <p><b>Note:</b> If transaction logging is enabled, you must run a disaster recovery operation that is based on the style of logging selected on the Lotus Domino server.</p> <p>After rebuilding the server, you can restore the databases from your most recent backup.</p>
Step 4	<p>Re-enable the monitor change journal.</p> <p>See <a href="#">“Re-enabling the monitor change journal”</a> on page 981.</p>

See [“About searching for and restoring data”](#) on page 229.

See [“Recovering of a Lotus Domino server that uses circular logging”](#) on page 982.

## About disaster recovery of a Lotus Domino server using archive logging

If the active transaction log is lost, you can recover the database only up to the transactions contained in the last transaction log.

However, if all of the transaction logs are lost, you must have the following to recover the database:

- An up-to-date Notes.ini file from the Lotus Domino server.
- The backups of the database.
- All archived log extents.

In addition, if the monitor change journal is enabled, you must disable it in the registry before beginning the Lotus Domino server recovery.

See [“Disabling the monitor change journal”](#) on page 980.

## Disabling the monitor change journal

Use the following steps to disable and re-enable the monitor change journal in the registry. Then you can recover the Lotus Domino server, databases, and transaction logs.

See [“About disaster recovery of a Lotus Domino server using archive logging”](#) on page 979.

### To disable the monitor change journal

- 1 Open the registry and browse to the following key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\SYMANTEC\BACKUP EXEC FOR WINDOWS\BACKUP EXEC\ENGINE\DOMINO
- 2 Disable monitor change journal by setting the value of the key Enable Change Journal to 0.
- 3 Restart the Lotus Domino Agent.

## Recovering the Lotus Domino server, databases, and transaction logs when archive logging is enabled

Use the following steps to recover the Lotus Domino server, databases, and transaction logs.

See [“About searching for and restoring data”](#) on page 229.

See [“About disaster recovery of a Lotus Domino server using archive logging”](#) on page 979.

### To recover the Lotus Domino server, databases, and transaction logs when archive logging is enabled

- 1 Using the Backup Exec Restore Wizard, restore the non-database Domino server files (\*.id and notes.ini) from an NTFS backup.  
  
If necessary, reinstall but do not configure the Domino server and then restore the non-database Domino files, which include the notes.ini and \*.id files. Use the same directory structure, directory location, and logdir path as was created in the original installation. Do not launch the server after reinstalling it.
- 2 Select **Restore over existing files** on the Restore Wizard panel, **How do you want to maintain file integrity and hierarchy for the restored data?**
- 3 Using a text editor, change the TRANSLOG\_Status setting in the notes.ini file on the Domino server to 0.

For example, TRANSLOG\_Status=0

- 4 Using the Backup Exec Restore Wizard, run a redirected restore of the last transaction log backed up prior to the loss of the active transaction log.
- 5 Verify the transaction log restore was successful.
- 6 Shutdown and then restart the Lotus Domino Agent.
- 7 Delete all transaction logs except the transaction log restored in step 4, from the Domino transaction log directory.
- 8 Using a text editor, change the notes.ini file for the Domino server to match the following:  

```
TRANSLOG_Recreate_Logctrl=1  
TRANSLOG_Status=1
```
- 9 Run a full restore of the Domino databases or a point-in-time state within the archived log extents.  

Backup Exec automatically restores all DAOS NLO files along with the DAOS-enabled databases from full backups. In addition, Domino automatically recreates both the `daos.cfg` file and the `daoscat.nsf` when you restart the Domino server.

After the full restore finishes, the `TRANSLOG_Logctrl` parameter in the `notes.ini` file is reset to 0.
- 10 Restore DAOS NLO files from incremental backups.
- 11 Start the Domino server. Disaster recovery is complete.
- 12 If monitor change journal was disabled prior to beginning the disaster recovery process, you must re-enable it.

See [“Re-enabling the monitor change journal”](#) on page 981.

## Re-enabling the monitor change journal

Use the following steps to re-enable the monitor change journal.

See [“About disaster recovery of a Lotus Domino server using archive logging”](#) on page 979.

See [“Lotus Domino Agent restore options”](#) on page 975.

**To re-enable monitor change journal**

- 1 Open the registry and browse to the following key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\SYMANTEC\BACKUP EXEC FOR WINDOWS\BACKUP EXEC\ENGINE\DOMINO
- 2 Enable monitor change journal by setting the value of the key Enable Change Journal to 1.
- 3 Restart the Lotus Domino Agent.

## Recovering of a Lotus Domino server that uses circular logging

If circular logging is enabled and the transaction log is lost, the Domino database can only be recovered to the point of the last backup.

**Table J-5**      Recovering a Lotus Domino server that uses circular logging

Step	Description
Step 1	Restore or re-install the Lotus Domino server program directory (excluding the notes.ini, cert.id, and <server>.id files) to the same location as before the disaster occurred.
Step 2	Check that the log directory (logdir) is created and does not contain old files.  If the log directory was not created, recreate the directory to the same location as before the disaster occurred.  Do not start the Lotus Domino server after performing the previous steps.
Step 3	Restore the notes.ini, cert.id, and <server>.id files from the last full backup of the Lotus Domino server program directory to the same location as before the disaster occurred.
Step 4	To have Lotus Domino create the circular log file in the log directory when the server starts, set the following parameter in the notes.ini file:  translog_path=logdir

**Table J-5** Recovering a Lotus Domino server that uses circular logging  
(continued)

<b>Step</b>	<b>Description</b>
Step 5	Use the Lotus Domino Agent to restore the databases to the Domino data directory.



# Symantec Backup Exec Agent for Microsoft Active Directory

This appendix includes the following topics:

- [About the Agent for Microsoft Active Directory](#)
- [Requirements for the Agent for Microsoft Active Directory](#)
- [About installing the Agent for Microsoft Active Directory](#)
- [How the Agent for Microsoft Active Directory works](#)
- [How Granular Recovery Technology works with Active Directory and ADAM/AD LDS backups](#)
- [Editing defaults for Active Directory and ADAM/AD LDS backup jobs](#)
- [About backing up Active Directory and ADAM/AD LDS](#)
- [About restoring individual Active Directory and ADAM/AD LDS objects](#)
- [About recreating purged Active Directory and ADAM/AD LDS objects](#)
- [Resetting the Active Directory computer object and the computer object account](#)

## About the Agent for Microsoft Active Directory

The Symantec Backup Exec 2012 Agent for Microsoft Active Directory (Active Directory Recovery Agent) uses Granular Recovery Technology (GRT) to restore individual Active Directory objects and attributes without performing an

authoritative or non-authoritative full restore. You can also restore individual Active Directory Application Mode (ADAM) and Active Directory Lightweight Directory Services (AD LDS) objects and attributes.

See [“About the Agent for Microsoft Active Directory”](#) on page 985.

See [“About installing the Agent for Microsoft Active Directory”](#) on page 987.

See [“How the Agent for Microsoft Active Directory works”](#) on page 987.

See [“About restoring individual Active Directory and ADAM/AD LDS objects”](#) on page 991.

## Requirements for the Agent for Microsoft Active Directory

Review the following requirements before you restore individual objects and attributes using the Active Directory Recovery Agent:

- You must have a full mode backup of the ADAM/AD LDS or the Windows System State (where Active Directory is installed).
- You must use one of the following Windows operating systems on the computer where Active Directory is in use:
  - Windows XP Professional x64 Edition
  - Windows Server 2003 with Service Pack 1 or later
  - Windows Server 2003 R2
  - Windows Server 2008
  - Windows Server 2008 R2
- You must use a version of the Windows operating system that supports minifilter drivers on the Backup Exec server that runs the restore job. Minifilter drivers are supported in the following Windows operating systems:
  - Windows Server 2003 with Service Pack 1 or later installed.
  - Windows Server 2003 R2
  - Windows Server 2008
  - Windows Server 2008 R2
- You must run the Backup Exec Agent for Windows on the computer where Active Directory is installed.

- You must designate a location on the Backup Exec server disk where Backup Exec can temporarily place the objects and attributes that are being restored when you restore from tape.
- Make sure you select the option **Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual objects from Active Directory backups**. Individual attributes and properties cannot be restored from full Active Directory and ADAM/AD LDS backups if you do not select this option during backup.

---

**Note:** You cannot restore individual objects and attributes from Active Directory backups for a Read-Only Domain Controller (RODC). You should do GRT backups and restores of the Active Directory to a writable centralized datacenter domain controller.

---

See [“About installing the Agent for Microsoft Active Directory”](#) on page 987.

See [“How the Agent for Microsoft Active Directory works”](#) on page 987.

See [“About restoring individual Active Directory and ADAM/AD LDS objects”](#) on page 991.

## About installing the Agent for Microsoft Active Directory

The Active Directory Recovery Agent is installed as part of the Agent for Applications and Databases.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

## How the Agent for Microsoft Active Directory works

The Active Directory Recovery Agent works with backups of the Windows System State (where Active Directory is installed) and ADAM/AD LDS.

When you back up the Windows System State, the Active Directory is included in the backup job, because Active Directory is a component of Windows System State.

You can also use the Active Directory Recovery Agent to restore individual ADAM/AD LDS objects and attributes. If multiple ADAM/AD LDS instances are backed up, each instance appears under the Active Directory Application Mode node.

The Active Directory Recovery Agent also lets you restore tombstoned objects from the Active Directory Deleted Objects container in the following situations:

- Their tombstone lifetimes have not passed.
- They have not been purged from the Deleted Objects container.
- You are restoring to a Windows Server 2003/2008/2008 R2/XP Professional x64 Edition system.

Symantec recommends that Active directory and ADAM/AD LDS backups be backed up to disk storage before you back them up to tape. This strategy provides you with shorter backup windows. It also lets you administer Active Directory or ADAM/AD LDS without requiring the individual cataloging of the backed up objects and properties.

When you back up any Windows Active Directory or ADAM/AD LDS application database directly to tape, objects and properties that are added or deleted during the backup will not match the individual objects and properties that are available for restore from the backup set. The back up of the database is a snapshot backup of the live Active Directory or ADAM/AD LDS database and the cataloging of the individual Active Directory or ADAM/AD LDS objects occurs after the snapshot is performed. Since the catalog operation catalogs objects and properties from the live Active Directory or ADAM/AD LDS database, object and property changes can occur after the snapshot was taken.

See [“About restoring individual Active Directory and ADAM/AD LDS objects”](#) on page 991.

See [“About recreating purged Active Directory and ADAM/AD LDS objects”](#) on page 992.

## How Granular Recovery Technology works with Active Directory and ADAM/AD LDS backups

Granular Recovery Technology (GRT) lets you restore individual objects and attributes from Active Directory and ADAM/AD LDS backups without performing an authoritative or non-authoritative full restore. To restore individual items, you must enable the Granular Recovery Technology feature when you create a backup job. You should review the requirements for a GRT-enabled backup before you configure it.

See [“How to restore individual items by using Granular Recovery Technology”](#) on page 543.

See [“Recommended devices for backups that use Granular Recovery Technology”](#) on page 545.

See [“About requirements for jobs that use Granular Recovery Technology”](#) on page 547.

## Editing defaults for Active Directory and ADAM/AD LDS backup jobs

You can edit the default settings for all Active Directory and ADAM/AD LDS backup jobs. You also can override these defaults when you set up Active Directory and ADAM/AD LDS backup jobs.

See [“About restoring individual Active Directory and ADAM/AD LDS objects”](#) on page 991.

See [“About recreating purged Active Directory and ADAM/AD LDS objects”](#) on page 992.

### To edit defaults for Active Directory and ADAM/AD LDS backup jobs

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select a backup option.
- 3 On the left, click **Microsoft Active Directory**.
- 4 Select the default backup options for the Active Directory Recovery Agent .  
See [“Microsoft Active Directory backup job options”](#) on page 990.
- 5 Click **OK**.

## About backing up Active Directory and ADAM/AD LDS

Symantec recommends that you use disk storage whenever possible when backing up Active Directory and ADAM/AD LDS. Disk storage provides the most efficient method of storage for GRT-enabled backups, and the most efficient method of restore.

For example, if you back up to tape, you must create a temporary hard disk staging location on a local NTFS volume to restore individual items from GRT-enabled backups on tape. The data is first copied from tape to the temporary staging location before it can be restored. As such, a restore from tape takes more time. For best results, you should specifically select disk storage when you configure your GRT-enabled backup jobs.

---

**Note:** You cannot back up databases to devices that are attached to a computer on which the Media Agent for Linux is installed.

---

See [“Backing up data”](#) on page 163.

See [“Editing backups”](#) on page 170.

See [“About stages”](#) on page 183.

See [“Microsoft Active Directory backup job options”](#) on page 990.

## Microsoft Active Directory backup job options

The can edit the default settings for Active Directory and ADAM/AD LDS backup jobs.

See [“Editing defaults for Active Directory and ADAM/AD LDS backup jobs”](#) on page 989.

**Table K-1** Microsoft Active Directory backup default options

Item	Description
<b>Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual objects from Active Directory backups (not supported for Read-Only Domain Controllers)</b>	Enables the restore of individual items from full backups of the Active Directory or ADAM/ AD LDS.  Ensure that you meet the requirements for Granular Recovery Technology.  See <a href="#">“About requirements for jobs that use Granular Recovery Technology”</a> on page 547.
<b>Perform consistency check before backup when using Microsoft Volume Shadow Copy Service (VSS) snapshot provider (Windows Server 2008 and above)</b>	Checks snapshots for data corruption. This option applies only to snapshots that are performed by the Microsoft Volume Shadow Copy Services (VSS).
<b>Continue with backup if consistency check fails</b>	Enables the backup job to continue even if the consistency check fails. You may want the job to continue if a backup of the database in its current state is better than no backup at all. Or you may want the job to continue if you back up a large database that may have only a small problem.

See [“About backing up Active Directory and ADAM/AD LDS”](#) on page 989.

# About restoring individual Active Directory and ADAM/AD LDS objects

Before starting the restore job, you should review information on finding and viewing specific data to restore, as well as on details on restore options and restore jobs.

When you restore Active Directory and ADAM/AD LDS objects from tape, you must specify an on-disk staging location where the objects will be placed prior to being restored. The staging location must be a path on a local NTFS volume on the Backup Exec server running the restore job and the Backup Exec service account must also have access to it.

System volumes should not be used as a staging location because of the potentially large file sizes that are created on the disk specified in the staging location path.

Because restoring objects from tape requires the creation of a staging location, restoring from tape requires more time than if you are restoring from disk.

By default, the Active Directory Recovery Agent restores deleted Active Directory or ADAM/AD LDS objects from the Active Directory Deleted Objects container if their tombstone lifetimes have not passed.

When objects in Active Directory are deleted, they are removed from their current Active Directory or ADAM/AD LDS container, converted into tombstones, and then placed in the Active Directory Deleted Objects container where their tombstone lifetime is monitored. After their tombstone lifetime passes, the tombstones are purged from the Active Directory Deleted Objects container, which permanently deletes the objects from the Active Directory and ADAM/AD LDS databases.

When you restore data with the ADAM Writer, Backup Exec stops the service for the ADAM instance you want to restore before the restore job starts. However, Backup Exec does not restart the ADAM service when the restore job completes because post-processing jobs, such as authoritative restores using Adamutil.exe, may be needed. You must restart the ADAM service. If Backup Exec cannot stop the ADAM service or if Backup Exec cannot restore all of the ADAM files, the ADAM restore fails.

When you restore Active Directory user objects, you must reset the object's user password and then re-enable the object's user account. For ADAM/AD LDS user objects, you must reset the object's user password and then re-enable the object's user account. For Active Directory user objects, use the Microsoft Active Directory Users and Computers application. For ADAM/AD LDS user objects, use ADSI Edit.

For Active Directory computer objects, you must reset the object's account.

See [“Resetting the Active Directory computer object and the computer object account”](#) on page 993.

---

**Note:** Some objects in the Active Directory Configuration Partition node cannot be reanimated from the Active Directory Deleted Objects container. However, recreated objects may not be recognized by some applications.

---

For more information, see your Microsoft Active Directory documentation.

See [“About searching for and restoring data”](#) on page 229.

See [“About recreating purged Active Directory and ADAM/AD LDS objects”](#) on page 992.

See [“Resetting the Active Directory computer object and the computer object account”](#) on page 993.

## About recreating purged Active Directory and ADAM/AD LDS objects

You can attempt to recreate deleted Active Directory objects and ADAM/LDS objects after they have been purged from the **Active Directory Deleted Objects** container by restoring the object from a previous Active Directory backup.

You can attempt to recreate the deleted objects if their tombstone lifetimes have passed and the objects have been purged from the Active Directory Deleted Objects container.

However, you should be aware of the following:

- Most applications will not recognize a recreated object since recreated objects are not identical to the original deleted object. Recreated objects are assigned new global unique identifiers (GUIDs) and security identifiers (SIDs) that cannot be identified by the applications that created the original object.
- Attributes created by the Windows operating system cannot be recreated when a purged object is recreated. Hence, objects that rely on attributes set by the operating system will not be recognized by Windows when the objects are recreated.

See [“About restoring individual Active Directory and ADAM/AD LDS objects”](#) on page 991.

# Resetting the Active Directory computer object and the computer object account

In Active Directory, computer objects are derived from user objects. Some attributes that are associated with a computer object cannot be restored when you restore a deleted computer object. The attributes can only be restored if the attributes were saved through schema changes before the computer object was originally deleted. Because computer object credentials change every 30 days, the credentials from the backup may not match the credentials that are stored on the actual computer.

---

**Note:** To reset a computer object, you must use the Microsoft Active Directory Users and Computers application.

For more information on resetting a computer object, see your Microsoft Active Directory Users and Computers application documentation.

---

If a computer object's **userAccountControl** attribute was not preserved before the object was deleted, you must reset the object's account after you restore the object.

See [“About recreating purged Active Directory and ADAM/AD LDS objects”](#) on page 992.

## To reset the Active Directory computer object account

- 1 Remove the computer from the domain.
- 2 Re-join the computer to the domain. The SID for the computer remains the same since it is preserved when you delete a computer object. However, if the object's tombstone expires and a new computer object is recreated, the SID is different.



# Symantec Backup Exec Central Admin Server Option

This appendix includes the following topics:

- [About the Central Admin Server Option](#)
- [Requirements for installing CASO](#)
- [How to choose the location for CASO storage and media data](#)
- [About installing the Central Admin Server Option](#)
- [Push-installing a managed Backup Exec server from the central administration server](#)
- [About installing a managed Backup Exec server across a firewall](#)
- [About upgrading an existing CASO installation](#)
- [Changing a Backup Exec server to a central administration server](#)
- [Changing a Backup Exec server to a managed Backup Exec server](#)
- [Changing a managed Backup Exec server to a standalone Backup Exec server](#)
- [About reducing network traffic in CASO](#)
- [About CASO catalog locations](#)
- [Changing the settings for a managed Backup Exec server](#)
- [What happens when CASO communication thresholds are reached](#)

- [About alerts and notifications in CASO](#)
- [Enabling managed Backup Exec servers to use any available network interface card](#)
- [About job delegation in CASO](#)
- [About adding storage devices in a CASO environment](#)
- [How to use Backup Exec server pools in CASO](#)
- [How centralized restore works in CASO](#)
- [About restoring from the central administration server](#)
- [About recovering failed jobs in CASO](#)
- [Pausing a managed Backup Exec server](#)
- [Resuming a paused managed Backup Exec server](#)
- [Stopping Backup Exec services for a managed Backup Exec server](#)
- [Starting Backup Exec services for a managed Backup Exec server](#)
- [Viewing managed Backup Exec server properties](#)
- [Viewing the settings for a central administration server](#)
- [Disaster Recovery in CASO](#)
- [Troubleshooting CASO](#)
- [Running the Backup Exec Utility for CASO operations](#)
- [Uninstalling Backup Exec from the central administration server](#)
- [Uninstalling Backup Exec from a managed Backup Exec server](#)

## About the Central Admin Server Option

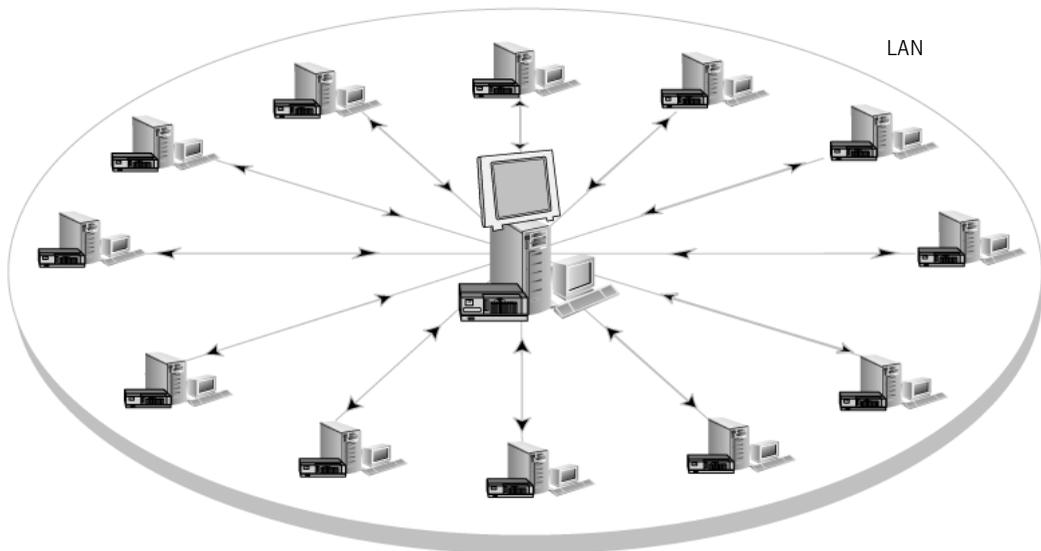
The Symantec Backup Exec Central Admin Server Option (CASO) enables a central administration server to delegate jobs to managed Backup Exec servers across the network. Job delegation is the automatic load balancing of jobs across available managed Backup Exec servers in the CASO environment. If your organization includes more than one Backup Exec server, you can benefit from using CASO.

All backup information in the CASO environment can be centralized on the central administration server. The managed Backup Exec servers perform the actual processing of backup and restore jobs. You create jobs on the central administration

server and then delegate the jobs to run on a managed Backup Exec server. The jobs are delegated, or load-balanced, across the available storage devices on the managed Backup Exec server. Multiple Backup Exec servers can share a storage device when sharing is enabled. Centralized restore jobs can also be delegated to managed Backup Exec servers. Additionally, the central administration server can function as a managed Backup Exec server and process delegated jobs. A managed Backup Exec server can also run jobs that are created locally at its local administration console.

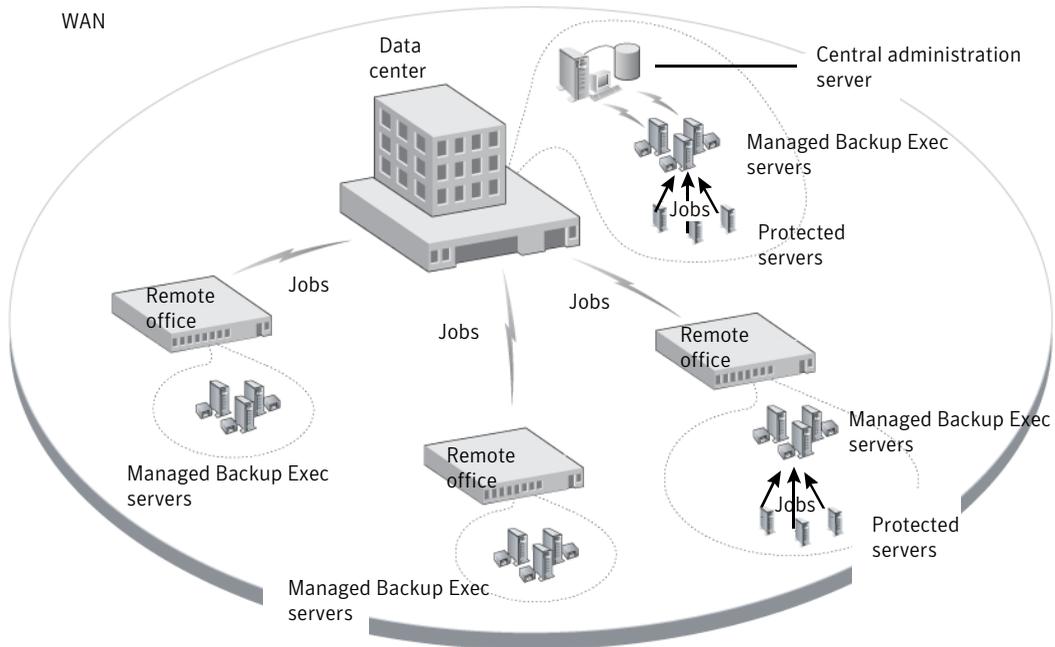
The following graphic shows a local area network (LAN) environment with a central administration server and several managed Backup Exec servers.

**Figure L-1** CASO-configured Backup Exec environment - LAN



The same communications that occur over a LAN between the central administration server and the managed Backup Exec servers take place over a WAN.

**Figure L-2** CASO-configured Backup Exec environment - WAN



See [“About sharing storage devices”](#) on page 418.

See [“How to choose the location for CASO storage and media data ”](#) on page 999.

See [“About installing the Central Admin Server Option”](#) on page 1001.

See [“About upgrading an existing CASO installation”](#) on page 1011.

## Requirements for installing CASO

The system requirements for the Central Admin Server Option (CASO) are the same as the minimum requirements for Backup Exec, with the exception of RAM. However, processor speed, memory, and disk space requirements may increase based on the number of managed Backup Exec servers, the number of servers being backed up, and the amount of catalog storage space that is required.

On the computer on which you install the central administration server, 512 MB RAM is required. One GB RAM is recommended. Other applications on the Backup Exec server also require a certain amount of physical RAM to function properly. The requirements for RAM may also increase when the central administration server manages more Backup Exec servers or tape hardware.

Before you install CASO, do the following:

- Ensure that you have administrative rights on computers on which you want to install CASO.
- Ensure that when you install CASO on Backup Exec servers in multiple domains, the Backup Exec service account is in the trusted domain and has administrative rights on all of the Backup Exec servers that you want to use as managed Backup Exec servers.  
If the Backup Exec database for the central administration server is installed on a SQL Server instance on a different computer, the account must be a domain account with local administrative privileges on that computer as well.
- Ensure that the central administration server and the managed Backup Exec servers are part of a domain or domains. CASO is not supported in a workgroup.
- Use only NetBIOS computer names for managed Backup Exec servers and central administration servers. You cannot enter fully qualified domain names or IP addresses as server names.
- Ensure that you have the appropriate licenses for Backup Exec. A license for Backup Exec is required in addition to a license for CASO.

See [“System requirements”](#) on page 65.

See [“About installing the Central Admin Server Option”](#) on page 1001.

## How to choose the location for CASO storage and media data

During the installation of the managed Backup Exec server feature, you can choose the location of the managed Backup Exec server’s storage and media data.

The following table compares how CASO tasks are performed depending on the location of the managed Backup Exec server’s storage and media data:

**Table L-1** Comparison of CASO tasks

<b>Task</b>	<b>Storage and media data on the central administration server</b>	<b>Storage and media data on the managed Backup Exec server</b>
Delegate jobs from the central administration server to the managed Backup Exec server	Yes	No. Instead, you can create jobs on the central administration server, and then copy them to the managed Backup Exec server.
Manage storage devices and media on the managed Backup Exec server from the central administration server	Yes	No
Hold, delete, run, cancel, and change the priority of copied jobs from the central administration server if the option to monitor jobs is enabled on the managed Backup Exec server	Yes	Yes
Monitor jobs that are created on the local managed Backup Exec server if the option to monitor jobs is enabled on the managed Backup Exec server	Yes	Yes
Send job status updates, job logs, and job histories to the central administration server if the option to monitor jobs is enabled on the managed Backup Exec server	Yes	Yes
Centralize, distribute, or replicate the catalog	Yes	No Only a distributed catalog location can be selected.

**Table L-1** Comparison of CASO tasks (*continued*)

Task	Storage and media data on the central administration server	Storage and media data on the managed Backup Exec server
Run centralized restore	Yes	Yes  You can browse the backup sets and run restore operations for the managed Backup Exec server from the central administration server.

---

**Note:** In a CASO environment, you can add an NDMP Server only to a central administration server or a managed Backup Exec server on which the storage and media database is located.

---

See [“About upgrading an existing CASO installation”](#) on page 1011.

See [“About the Central Admin Server Option”](#) on page 996.

See [“Running the Backup Exec Utility for CASO operations”](#) on page 1044.

## About installing the Central Admin Server Option

The Central Admin Server Option is installed as part of the Enterprise Server Option. After you enter license information for the Enterprise Server Option, on the **Configure Options** panel, you must expand the **Backup Exec Options** item, and then expand the **Enterprise Server Option** item to select the Central Admin Server Option for installation. When you select the Central Admin Server Option for installation, then the central administration server is installed. After the central administration server is installed, you can install managed Backup Exec servers.

---

**Note:** You must use the custom installation option in the installation wizard to install CASO. The typical installation option does not support the installation of CASO.

---

See [“Push-installing a managed Backup Exec server from the central administration server”](#) on page 1002.

Before you start the installation, review the information about the location of storage and media data.

See [“How to choose the location for CASO storage and media data ”](#) on page 999.

## Push-installing a managed Backup Exec server from the central administration server

After you install the central administration server, you can push-install the managed Backup Exec server feature to a standalone server.

Before you install a managed Backup Exec server, decide where to locate the storage and media database for it. During the installation of the managed Backup Exec server, you can choose the location of the managed Backup Exec server’s storage and media data. Your choice affects how you can manage jobs in the CASO environment.

See [“How to choose the location for CASO storage and media data ”](#) on page 999.

### To push-install a managed Backup Exec server from the central administration server

- 1 From the central administration server, click the Backup Exec button, and then select **Installation and Licensing**.
- 2 Select **Install Agents and Backup Exec Servers on Other Servers**.
- 3 In the installation wizard, click **Add**, and then select either **Add a Single Computer** or **Add Multiple Computers with the Same Settings**.
- 4 Select **Symantec Backup Exec**, and then click **Next**.
- 5 In the **Remote computer** field, type the name of the managed Backup Exec server that you want to add, or click **Browse Remote Computers** to locate the server.
- 6 Click **Add to List**.

This option is not necessary if you selected **Add a Single Computer** in step 3.

- 7 Under **Remote computer credentials**, complete the fields as follows:

<b>User Name</b>	Type the user name for an account that has administrative rights on the remote computer.
<b>Password</b>	Type the password for an account that has administrative rights on the remote computer.
<b>Domain</b>	Select the domain in which the remote computer is located.

**8** Click **Next**.

**9** Select one of the following methods to enter license keys:

To enter serial numbers manually	In the <b>Serial number</b> field, type a serial number from your sales certificate, and then click <b>Add</b> .
To import a Symantec license file	Click <b>Import From File</b> , and then navigate to the location of your .slf file.
To install a trial version	Do not enter serial numbers or import license files. Proceed to the next step.

**10** Click **Next**.

**11** After your serial numbers are validated, click **Next**.

**12** On the list of features to install, expand **Backup Exec 2012**, and then select **Managed Backup Exec server**.

**13** Do one of the following:

To change the directory where the Backup Exec files are installed	In the <b>Destination Folder</b> field, type the name of the directory.
To accept the default directory (recommended)	Proceed to the next step.

Symantec recommends that you do not select a mount point as the destination directory because if you delete the mount point, Backup Exec is uninstalled.

**14** Click **Next**.

**15** Provide a user name, password, and domain for an Administrator account that the Backup Exec system services can use, and then click **Next**.

**16** On the **Choose SQL Server** panel, choose the location to store the Backup Exec database, and then click **Next**.

**17** In the **Central Administration Server** field, type the name of the central administration server that will manage this managed Backup Exec server.

Use only NetBIOS computer names for managed Backup Exec servers and central administration servers. You cannot enter fully qualified domain names or IP addresses as server names.

**18** Select from the following options to determine how storage devices and data are managed:

See [“About Managed Backup Exec Server Configuration options”](#) on page 1006.

**Centrally managed Backup Exec server** Enables the central administration server to manage this Backup Exec server, its storage devices, media, and job delegation. This option also enables this Backup Exec server to share storage devices with other managed Backup Exec servers.

**Unrestricted access to catalogs and backup sets for restore** Enables this managed Backup Exec server to have unrestricted access to all centrally stored catalogs. This option also enables this managed Backup Exec server to restore data from any backup set on any storage devices that it shares.

This option can be selected only if the **Centrally managed Backup Exec server** option is selected. Selecting both of these options enables the central administration server to have the greatest amount of control over this managed Backup Exec server.

**Locally managed Backup Exec server** Enables the central administration server to monitor this managed Backup Exec server and create restore jobs for it. However, the server and its devices, media, and backup jobs are controlled locally.

**19** Click **Next**.

**20** Select the Symantec device drivers that you want to use, and then click **Next**.

**21** After Backup Exec validates the remote computers, you can change the list in any of the following ways:

To manually add one remote computer Click **Add**, and then click **Add a Single Server**.

To manually add multiple remote computers Click **Add**, and then click **Add Multiple Servers with the Same Settings**.

To add multiple remote computers by importing an existing list of computers	<p>Click <b>Import and Export</b>, and then select one of the following options:</p> <ul style="list-style-type: none"><li>■ Select <b>Import from File</b> to enable Backup Exec to add the names of the remote computers from a selected list.</li><li>■ Select <b>Import Servers Published to this Backup Exec Server</b> to enable Backup Exec to add the names of all the remote computers that are set up to publish to this Backup Exec server.</li></ul> <p>You must enter remote computer logon credentials for the list of remote computers.</p>
To change the product that you selected to install or to change other properties you selected for this installation	Select the remote computer that you want to change, and then click <b>Edit</b> .
To delete a remote computer from the list	Select the remote computer that you want to delete, and then click <b>Delete</b> .
To save this list of remote computers and the associated remote computer logon credentials	<p>Verify that <b>Save the server list for future remote install sessions</b> is checked.</p> <p>This option enables the names of all of the remote computers and their credentials to be added automatically the next time you want to install Backup Exec or options to these remote computers.</p>
To save this list of remote computers to an XML file	<p>Click <b>Import and Export</b>, and then click <b>Export to File</b>.</p> <p>You can select the location to save the XML file. This option is useful if you want to use the same list for multiple Backup Exec servers. When you import the list, you must re-enter the remote computer logon credentials.</p>
To fix the errors that were located during the validation	Right-click the name of the computer, and then click <b>Fix Errors</b> .
To enable Backup Exec to attempt to re-validate an invalid remote computer	Right-click the name of the computer, and then click <b>Retry Validation</b> .

**22** After all of the computers are validated, click **Next**.

**23** Read the Backup Exec installation review, and then click **Install**.

**24** Click **Next**, and then click **Finish**.

If you did not restart the remote computer, you may need to do it now in order for the configuration to take effect.

## About Managed Backup Exec Server Configuration options

The following information can help you to determine which configuration options to choose when you are installing a managed Backup Exec server.

The following information applies if you select the option **Centrally managed Backup Exec server** and also select the option **Unrestricted access to catalogs and backup sets for restore**:

- This Backup Exec server becomes a managed Backup Exec server.
- A persistent network connection is required between the managed Backup Exec server and the central administration server.
- The catalogs are centralized and are stored on the central administration server. Note that this combination of options may not be suitable if you have a low-bandwidth network connection to the central administration server.
- This managed Backup Exec server can access and restore backup sets for all storage devices that it shares with other Backup Exec servers.
- The backup jobs that are created on the central administration server can be load-balanced and delegated to this managed Backup Exec server.
- A rolling upgrade cannot be performed with this configuration. This managed Backup Exec server must be upgraded at the same time as the central administration server.

The following information applies if you select the option **Centrally managed Backup Exec server**, but do not select the option **Unrestricted access to catalogs and backup sets for restore**:

- This Backup Exec server becomes a managed Backup Exec server.
- A persistent network connection is required between the managed Backup Exec server and the central administration server.
- The catalogs are in distributed mode by default, but can be changed. The catalogs for the jobs that run on this managed Backup Exec server are stored locally.
- This managed Backup Exec server can access and restore any backup set stored on the storage devices that it hosts, regardless of which Backup Exec server ran the backup job. However, for the shared storage devices that other Backup

Exec servers host, this managed Backup Exec server can access and restore only the backup sets that were created from backup jobs it ran.

- The backup jobs that are created on the central administration server can be load-balanced and delegated to this managed Backup Exec server.
- This option is recommended for use with the private cloud configuration.

The following information applies if you select the option **Locally managed Backup Exec server**:

- This Backup Exec server becomes a managed Backup Exec server.
- A persistent network connection is not required between the managed Backup Exec server and the central administration server. Therefore, this option may be useful when a very low-bandwidth connection exists between the managed Backup Exec server and the central administration server. It may also be useful when the managed Backup Exec server cannot always be connected to the central administration server.
- The catalogs are in distributed mode by default. The catalogs for the jobs that run on this managed Backup Exec server are stored locally.
- The central administration server does not delegate jobs to this managed Backup Exec server.
- This managed Backup Exec server cannot be used in a private cloud configuration

See [“Push-installing a managed Backup Exec server from the central administration server”](#) on page 1002.

## About installing a managed Backup Exec server across a firewall

A managed Backup Exec server may be installed outside the firewall that the central administration server is installed in or in a different firewall.

The following rules apply to the managed Backup Exec servers that are installed across a firewall:

- Port 3527 must be open in both directions to enable communication for the Backup Exec Server service.
- Port 10000 must be open for the Agent for Windows, which allows browsing for remote selections.
- A SQL port must be open in both directions to the central administration server’s database to enable database connections.

- A static port must be used.  
The Backup Exec SQL instance is configured by default to use a dynamic port. Each time SQL Server is started, the port number can change. You must change the dynamic port to a static port. After you change the configuration of the port from dynamic to static, you must add the static port to the Windows Firewall Exceptions list.  
See your Windows operating system documentation.  
See [“Changing the dynamic port on the SQL Express instance in CASO to a static port”](#) on page 1008.  
See [“Opening a SQL port in CASO for a SQL 2005 or 2008 instance”](#) on page 1010.

## Changing the dynamic port on the SQL Express instance in CASO to a static port

You must change the port on which the Backup Exec SQL Express instance for the central administration server is running from a dynamic port to a static port. Then, create an alias for the managed Backup Exec server to allow it to connect to the SQL port on the central administration server. After changing the port, you must restart the Backup Exec and Microsoft SQL services on the central administration server.

### To change the dynamic port for a SQL Express instance to a static port

- 1 On the central administration server, click **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.
- 2 Expand **SQL Server 2005 Network Configuration**.
- 3 Click **Protocols for BKUPEXEC**, and then in the right pane, double-click **TPC/IP**.
- 4 On the TCP/IP Properties dialog box, click the IP Addresses tab.
- 5 Under IPAll, in TCP Dynamic Ports, remove the value and leave the field blank.
- 6 Under IPAll, type in a port number for TCP Port.  
The port number can be between 1025 and 65535 and must not be in use by another application.
- 7 Under the heading for the specific network interface card that is being used, such as IP1 or IP2, change Enabled from No to Yes.
- 8 Under that same heading, in TCP Dynamic Ports, remove the value of 0, and type the same port number you entered for TCP Port.
- 9 Click **Apply**.

- 10 You must restart the Backup Exec and SQL services.
- 11 Create an alias for the managed Backup Exec server to allow it to connect to the SQL port on the central administration server.  
See [“Creating an alias for a managed Backup Exec server when a SQL Express instance is used”](#) on page 1009.

## Creating an alias for a managed Backup Exec server when a SQL Express instance is used

You must change the port on which the Backup Exec SQL Express instance for the central administration server is running from a dynamic port to a static port. Then, create an alias for the managed Backup Exec server to allow it to connect to the SQL port on the central administration server. After changing the port, you must restart the Backup Exec and Microsoft SQL services on the central administration server.

### To create an alias when a SQL Express instance is used

- 1 On the managed Backup Exec server, click **Start > SQL Server Configuration Manager**.
- 2 Expand **SQL Native Client Configuration**.
- 3 Click **Aliases**, and then double-click the alias name that contains the central administration server name and the Backup Exec SQL instance name.
- 4 On the alias properties dialog box, enter the appropriate information as described in the following table:

Alias Name	Type the name of the central administration server and the Backup Exec SQL instance name using the format server name\instance name.
Port No	Type the port number of the remote Backup Exec SQL Server instance that you noted in the previous procedure.
Protocol	Select <b>TCP/IP</b> .
Server	Type the name of the central administration server and the Backup Exec SQL instance name using the format server name\instance name.

- 5 Click **Apply**, and then click **OK**.
- 6 Close the SQL Server Configuration Manager utility.

See [“Changing the dynamic port on the SQL Express instance in CASO to a static port”](#) on page 1008.

## Creating an alias for a managed Backup Exec server when a SQL 2005 or SQL 2008 instance is used

You must find the port number on which the Backup Exec SQL 2005 or 2008 instance for the central administration server is running, and then create an alias for the managed Backup Exec server.

### To create an alias when a SQL 2005 or 2008 instance is used

- 1 On the managed Backup Exec server, to create an alias for the managed Backup Exec server, go to `\Windows\System32` and double-click **cliconfg.exe**.
- 2 On the Alias tab, click **Add**.
- 3 In the Server alias field, type:  
  
*server name\instance name*
- 4 Under Network libraries, select **TCP/IP**.
- 5 In the Server name field, type:  
  
*server name\instance name*
- 6 Uncheck **Dynamically determine port**.
- 7 In the Port number field, type the port number of the remote Backup Exec SQL Server instance.

See [“Changing the dynamic port on the SQL Express instance in CASO to a static port”](#) on page 1008.

## Opening a SQL port in CASO for a SQL 2005 or 2008 instance

You must find the port number on which the Backup Exec SQL 2005 or 2008 instance for the central administration server is running, and then create an alias for the managed Backup Exec server.

### To open a SQL port for a SQL 2005 or 2008 instance

- 1 On the central administration server, go to `\Program Files\Microsoft SQL Server\80\Tools\Binn` and double-click **svrnetcn.exe**.
- 2 On the General tab, select the Backup Exec SQL instance.
- 3 Under Enabled Protocols, select **TCP/IP**, and then click **Properties**.

- 4 Note the port number that is displayed.
- 5 Create an alias for the managed Backup Exec server to allow it to connect to the SQL port on the central administration server.

See [“Creating an alias for a managed Backup Exec server when a SQL 2005 or SQL 2008 instance is used”](#) on page 1010.

## About upgrading an existing CASO installation

In an existing CASO environment, upgrade the central administration server, and then upgrade the managed Backup Exec servers.

If necessary, you can perform rolling upgrades in the CASO environment. A rolling upgrade lets you upgrade the central administration server from Backup Exec 2010 to Backup Exec 2012 first, and then upgrade the managed Backup Exec servers from Backup Exec 2010 to Backup Exec 2012 over a period of time. You must have the most recent Backup Exec service pack to perform rolling upgrades.

---

**Note:** Forward compatibility is not supported in rolling upgrades. Therefore, any system that runs Backup Exec 2010 cannot protect a system that runs Backup Exec 2012.

---

Symantec recommends that you do not keep a mix of versions in the CASO installation for an extended time. Key functionality for administering managed Backup Exec servers is missing in a mixed-version environment, which decreases your ability to properly administer the CASO environment.

After you upgrade the central administration server to Backup Exec 2012, the following operations are supported on managed Backup Exec servers that run Backup Exec 2010:

- Backup
- Restore
- Inventory
- Catalog

See [“About CASO catalog locations”](#) on page 1016.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

See [“Upgrading an existing central administration server”](#) on page 1012.

See [“About upgrading an existing managed Backup Exec server”](#) on page 1013.

## Upgrading an existing central administration server

The central administration server must be upgraded before any managed Backup Exec servers are upgraded.

See [“About upgrading an existing CASO installation”](#) on page 1011.

Before upgrading Backup Exec, run a database maintenance job to delete job histories and catalogs that you no longer need in order to shorten the upgrade window.

See [“Changing database maintenance options”](#) on page 467.

---

**Note:** Symantec recommends that you stop all Backup Exec services on each managed Backup Exec server before you upgrade the central administration server.

---

### To upgrade an existing central administration server

- 1 Verify that the latest service pack for Backup Exec is installed.
- 2 Place all scheduled jobs on hold on the central administration server and the managed Backup Exec servers.  
See [“Placing a job on hold”](#) on page 253.
- 3 Allow all active jobs to complete.
- 4 From the installation media browser, select the option to install Symantec Backup Exec.
- 5 On the Welcome panel, click **Next**.
- 6 Select **I accept the terms of the license agreement**, and then click **Next**.
- 7 Check **Local Install**, and then click **Install Backup Exec software and options**.
- 8 Click **Next**.
- 9 Follow the prompts in the wizard.
- 10 On the Back Up Existing Catalog and Data page, enter or browse to a directory to which all existing catalogs and data will be backed up. The default location is:

```
C:\Program Files\Symantec\Backup Exec\Data
```

If you do not want to keep previous catalogs and data, click **Do not back up previous data and catalogs**.

11 Click **Next** to continue.

An upgrade summary is displayed. When the upgrade is complete, communication with the managed Backup Exec servers is automatically enabled.

12 Release all jobs from hold.

See [“Removing the hold on a job”](#) on page 253.

13 Upgrade some or all of the managed Backup Exec servers.

## About upgrading an existing managed Backup Exec server

The central administration server must be upgraded before any managed Backup Exec servers are upgraded. Before upgrading Backup Exec, run a database maintenance job to delete the job histories and the catalogs that you no longer need. This practice shortens the upgrade window.

See [“About upgrading an existing CASO installation”](#) on page 1011.

See [“Changing database maintenance options”](#) on page 467.

## Changing a Backup Exec server to a central administration server

You can change a standalone Backup Exec server to a central administration server.

### To change a Backup Exec server to a central administration server

- 1 On the Backup Exec server that you want to be the central administration server, start Backup Exec.
- 2 Click the Backup Exec button, select **Installation and Licensing**, and then select **Install Options and Licenses on this Backup Exec Server**.
- 3 Select one of the following methods to enter licenses:

To enter licenses manually Do the following in the order listed:

- Type a serial number into the **Serial Number** field.
- Click **Add**.
- Repeat for each serial number for each option or agent that you want to add.

To import licenses from a file Do the following in the order listed:

- Click **Import From File**.
- Select the Symantec license file.

To install a trial version Proceed to the next step.

A license key is not required for a fully functional Trial version.

- 4 Click **Next**.
- 5 On the features list, expand **Backup Exec Options**, expand **Enterprise Server Option**, and then select **Central Admin Server Option**.
- 6 Click **Next**.
- 7 Read the Backup Exec installation review, and then click **Install**.
- 8 Click **Finish**.

See [“Changing a Backup Exec server to a managed Backup Exec server”](#) on page 1014.

## Changing a Backup Exec server to a managed Backup Exec server

To change a Backup Exec server to a managed Backup Exec server, you set the central administration server that will manage the Backup Exec server.

If the managed Backup Exec server does not appear on the **Storage** tab after you follow these instructions, and if your network contains firewalls, you may need to open some ports between the central administration server and the managed Backup Exec server.

### To change a Backup Exec server to a managed Backup Exec server

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Set Central Administration Server**.
- 2 Enter the name of the central administration server that will manage this server.
- 3 Click **OK**.
- 4 Restart the services on the new managed Backup Exec server.

See [“Changing a Backup Exec server to a central administration server”](#) on page 1013.

# Changing a managed Backup Exec server to a standalone Backup Exec server

You can change a managed Backup Exec server to a stand-alone Backup Exec server by deleting it from the **Storage** tab.

## To change a managed Backup Exec server to a standalone Backup Exec server

- 1 On the central administration server's **Storage** tab, right-click the managed Backup Exec server that you want to convert to a standalone Backup Exec server.
- 2 Select **Delete**.
- 3 Click **Yes** to confirm that you want to convert the server to a standalone Backup Exec server.
- 4 After you receive an alert on the central administration server that confirms the deletion of the server, restart the server that was changed to a managed Backup Exec server.

See [“Changing a Backup Exec server to a managed Backup Exec server”](#) on page 1014.

## About reducing network traffic in CASO

To accommodate a low bandwidth network connection or to reduce network traffic, you can do the following:

- Reduce the frequency of job status updates that are sent from the managed Backup Exec servers to the central administration server.
- Prevent jobs that are created on the local managed Backup Exec servers from being monitored by the central administration server.
- Reduce the frequency that job logs and job histories are sent from the managed Backup Exec servers to the central administration server.
- Increase the amount of time that Backup Exec waits before changing the Backup Exec server's status if the Backup Exec server becomes unresponsive.
- Keep the catalogs on the managed Backup Exec server (distributed). If there is a persistent network connection between the central administration server and the managed Backup Exec server, then you can browse the catalog and perform restore operations from both servers, regardless of the catalog location.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

## About CASO catalog locations

In the CASO environment, you can choose the catalog location. Regardless of the catalog location, if a persistent network connection is available between the central administration server and the managed Backup Exec server, then you can browse the backup sets in the catalog and perform restore operations from both servers.

The following catalog locations are available:

**Table L-2**

Item	Description
Distributed	<p>Image files, which are small files that contain information about the backup set, are distributed to the central administration server from every managed Backup Exec server. History files, which contain detailed information about the backup set, remain on the managed Backup Exec server.</p> <p><b>Note:</b> It is important that you back up the catalog files on the managed Backup Exec server since most catalog information is kept here when the distributed catalog location is used.</p> <p>When the catalog is distributed, the view of the restore selections on the central administration server displays only the backup set at the volume level. Backup set details are not displayed if the managed Backup Exec server that created this backup set is not available, but the whole volume can be restored from the central administration server.</p> <p>A distributed catalog provides increased performance, default centralized restore capability, and decreased network traffic. If a managed Backup Exec server does not have a persistent connection to the central administration server, then whenever the managed Backup Exec server does connect, the image files in the catalog are automatically distributed to the central administration server. The temporary increase in network traffic caused by the catalog distribution is not significant.</p>

**Table L-2** (continued)

Item	Description
Centralized	All catalog files and information for the managed Backup Exec server are kept on the central administration server.
Replicated	All catalog files are replicated from the managed Backup Exec server to the central administration server. Both the managed Backup Exec server and the central administration server store the catalogs that are produced by the managed Backup Exec server.  Deletions of catalog files are replicated between the managed Backup Exec server and the central administration server only when the catalog files are deleted by Backup Exec according to the catalog settings. If catalog files on the managed Backup Exec server are deleted as a result of a backup job or a manual deletion, the deletions are replicated the next time that the catalogs are synchronized.

When choosing the catalog location, consider the following:

- If there is enough available disk space on the managed Backup Exec server to keep a distributed or replicated catalog.
- If there is enough network bandwidth to handle the traffic generated by a centralized or replicated catalog. Centralized and replicated catalogs require a high bandwidth network connection.
- If it is important for your data recovery needs to keep catalog information in one location. For example, when the catalog location is centralized or replicated, all catalog information is kept in one location, which makes it easier to back up. When the catalog location is distributed, most catalog information is kept on the managed Backup Exec server.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

# Changing the settings for a managed Backup Exec server

The settings for a managed Backup Exec server determine how the managed Backup Exec server communicates and interacts with the central administration server. For example, you can change the connection type, the catalog location, and the job reporting and monitoring functionality. You can change the settings for a managed Backup Exec server at any time.

---

**Note:** You may need to restart the services on the managed Backup Exec server after you change the settings. For example, if you change the catalog location, you must restart the services to enable the change to take effect.

---

## To change the settings for a managed Backup Exec server

- 1 On the central administration server, on the **Storage** tab, double-click the managed Backup Exec server.
- 2 In the left pane, select **Settings**.
- 3 Select the appropriate options.  
See [“Managed Backup Exec server settings”](#) on page 1018.
- 4 Click **Apply**.

## Managed Backup Exec server settings

You can change the settings that affect how a managed Backup Exec server communicates and interacts with a central administration server.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

See [“About reducing network traffic in CASO”](#) on page 1015.

See [“What happens when CASO communication thresholds are reached”](#) on page 1025.

Table L-3 Settings for managed Backup Exec servers

Item	Description
<b>Connection settings</b>	<p>Lets you select one of the following types of connections with the central administration server:</p> <ul style="list-style-type: none"><li>■ <b>Fast connection</b> Configures frequent communications between the central administration server and the managed Backup Exec server. By default, when you choose this setting, job status updates are sent every 10 seconds to the central administration server. Job logs and job histories are sent whenever a job on the managed Backup Exec server completes.</li><li>■ <b>Slow connection</b> Configures less frequent communications between the central administration server and the managed Backup Exec server. By default, when you choose this setting, job status updates are sent every 120 seconds to the central administration server. Job logs and job histories are sent only when a job on the managed Backup Exec server fails.</li><li>■ <b>Custom</b> Lets you change the thresholds that trigger the communication statuses when managed Backup Exec servers become unresponsive. You can also set how often the managed Backup Exec server sends active job status updates to the central administration server. The frequency affects the network traffic.</li></ul>
<b>Communication stalled</b>	<p><b>Note:</b> This option appears only if <b>Custom</b> is selected in the <b>Connection settings</b> field.</p> <p>Indicates the amount of time before the managed Backup Exec server's status changes to Communication Stalled if the managed Backup Exec server is unresponsive.</p> <p>The central administration server does not delegate jobs to the managed Backup Exec server when it has a status of Communication Stalled. Job delegation resumes if the managed Backup Exec server returns to an Enabled status before the threshold is exceeded.</p> <p>The default threshold is five minutes.</p>

**Table L-3** Settings for managed Backup Exec servers (*continued*)

Item	Description
<p><b>No communication</b></p>	<p><b>Note:</b> This option appears only if <b>Custom</b> is selected in the <b>Connection settings</b> field.</p> <p>Indicates the amount of time before the managed Backup Exec server's status changes from Communication Stalled to No Communication.</p> <p>When the status of the managed Backup Exec server changes from Communication Stalled to No Communication, the central administration server marks the active jobs on the managed Backup Exec server as Failed. The custom error-handling rule Recovered Jobs is applied to any job that is active when the No Communication status appears.</p> <p>The default threshold is 15 minutes.</p>
<p><b>Send active job status updates to the central administration server</b></p>	<p><b>Note:</b> This option appears only if <b>Custom</b> is selected in the <b>Connection settings</b> field.</p> <p>Enables the managed Backup Exec server to send a job status update to the central administration server. You can adjust the number of seconds that a managed Backup Exec server waits between sending job status updates to the central administration server. To preserve network bandwidth when many jobs are running, increase the amount of time between job update statuses. Decrease the amount of time if you want to send more updates.</p> <p>The default is 10 seconds, which provides near real-time monitoring. This setting is recommended only for fast network connections.</p>

Table L-3 Settings for managed Backup Exec servers (*continued*)

Item	Description
<p><b>Send status updates to the central administration server every</b></p>	<p><b>Note:</b> This option appears only if <b>Custom</b> is selected in the <b>Connection settings</b> field and <b>Yes</b> is selected in the <b>Send active job status updates to the central administration server</b> field.</p> <p>Lets you set the amount of time that a managed Backup Exec server waits between sending job status updates to the central administration server. To preserve network bandwidth when many jobs are running, increase the amount of time between job update statuses. Decrease the amount of time if you want to send more updates.</p> <p>The default is 10 seconds, which provides near real-time monitoring. This setting is recommended only for fast network connections.</p> <p>For low-bandwidth network connections, consider a setting of 120 seconds. This frequency allows updates to be displayed for a medium-sized job while still significantly decreasing the network traffic caused by job status updates.</p> <p>If you uncheck the check box, job status updates are not sent. Job progress is not displayed on the central administration server. When the job is complete, the <b>Job History</b> on the central administration server is updated.</p>
<p><b>Send job log details to the central administration server</b></p>	<p>Lets you choose when the job log for the managed Backup Exec server is sent to the central administration server. You can choose the send the job log one time per day, after a job completes, or never.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>■ <b>Never</b> If you select this option, job logs are stored locally at the managed Backup Exec server.</li> <li>■ <b>Once a day</b> If you select this option, the <b>Send job logs at</b> field appears. You must select the time to send the job log to the central administration server.</li> <li>■ <b>On job completion</b> If you select this option, the <b>Send job log only if the job fails</b> field appears. Select <b>Yes</b> to send the job log only for failed jobs. Select <b>No</b> to send the job log regardless of the job disposition.</li> </ul>

**Table L-3** Settings for managed Backup Exec servers (*continued*)

Item	Description
<b>Send job logs at</b>	Lets you choose the time when Backup Exec sends the job logs for the managed Backup Exec server to the central administration server. This option appears only if <b>Once a day</b> is selected in the option <b>Send job log details to the central administration server</b>
<b>Send job jog only if the job fails</b>	Lets you choose whether to send job logs for failed jobs only or for all jobs. Select Yes to send the job log only for failed jobs. Select No to send the job log regardless of the job disposition. This option appears only if <b>On job completion</b> is selected in the option <b>Send job log details to the central administration server</b>
<b>Send job history details to central administration server</b>	<p>Lets you choose when the job history for the managed Backup Exec server is sent to the central administration server.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>■ <b>Never</b> If you select this option, job histories are stored locally at the managed Backup Exec server.</li> <li>■ <b>Once a day</b> If you select this option, the <b>Send job history logs at</b> field appears. You must select the time to send the job history to the central administration server.</li> <li>■ <b>On job completion</b> If you select this option, the <b>Send job history only if the job fails</b> field appears. Select Yes to send the job history only for failed jobs. Select No to send the job history regardless of the job disposition.</li> </ul>
<b>Send job history at</b>	Lets you choose the time when Backup Exec sends the job history for the managed Backup Exec server to the central administration server. This option appears only if <b>Once a day</b> is selected in the option <b>Send job history details to the central administration server</b>
<b>Send job history only if the job fails</b>	Lets you choose whether to send job history for failed jobs only or for all jobs. Select Yes to send the job history only for failed jobs. Select No to send the job history regardless of the job disposition. This option appears only if <b>On job completion</b> is selected in the option <b>Send job history details to the central administration server</b>

Table L-3 Settings for managed Backup Exec servers (*continued*)

Item	Description
<b>Monitor jobs that are created locally on the managed Backup Exec server</b>	<p>Enables you to view delegated jobs and the jobs that are created on the local managed Backup Exec server.</p> <p>You can also hold, delete, run, cancel, and change the priority order of the jobs that are created on or copied to the local managed Backup Exec server.</p>
<b>Display an alert when the time is not synchronized between the managed Backup Exec server and the central administration server</b>	<p>Enables Backup Exec to create an alert if the clock on the managed Backup Exec server differs from the clock on the central administration server. An alert is generated when the number of seconds indicated is exceeded.</p> <p>CASO monitors the internal computer clocks on both the managed Backup Exec servers and the central administration server. If time differences develop between the central administration server and the managed Backup Exec servers, jobs could run at unexpected times. To prevent problems, the time that is reported on managed Backup Exec servers should match the time that is reported on the central administration server. If you receive time difference alerts, reset the clock on the managed Backup Exec server to match the system clock on the central administration server.</p> <p>If you change the system time on either the managed Backup Exec server or the central administration server, you must restart the Backup Exec services on that server.</p>
<b>Send the alert after the servers are not synchronized for</b>	<p>Indicates the number of seconds that the clocks on the managed Backup Exec server and the central administration server must differ before Backup Exec sends an alert.</p> <p><b>Note:</b> This option appears only if <b>Enabled</b> is selected in the <b>Display an alert when the time is not synchronized between the managed Backup Exec server and the central administration server</b> field.</p>
<b>Storage and media database location</b>	<p>Indicates whether the storage and media database is located on the central administration server or a managed Backup Exec server.</p>

**Table L-3** Settings for managed Backup Exec servers (*continued*)

Item	Description
<b>Keep the catalogs on</b>	<p>Lets you set the location of the catalog to one of the following locations:</p> <ul style="list-style-type: none"> <li>■ <b>Managed Backup Exec server (distributed)</b>  Distributes the catalog files between the central administration server and the managed Backup Exec server. If storage and media data is kept in a local database on the managed Backup Exec server, then the distributed location is the only available catalog location. Select this option if you have a low-bandwidth network connection.</li> <li>■ <b>Central administration server (centralized)</b>  Keeps all catalog files on the central administration server. A high-bandwidth network connection is required for this option.</li> <li>■ <b>Both servers (replicated)</b>  Replicates all catalog files from the managed Backup Exec server to the central administration server. If a managed Backup Exec server is unavailable, you can still browse the catalog from the central administration server. However, you cannot restore data because the managed Backup Exec server is unavailable. A high-bandwidth network connection is required for this option.</li> </ul> <p>See <a href="#">“About CASO catalog locations”</a> on page 1016.</p>
<b>Private cloud server</b>	<p>Enables a managed service provider to locate a Backup Exec server in its data center, and then configure it for a CASO environment with other Backup Exec servers that are located across the WAN at the managed service provider's customer locations. As an alternative to shipping tapes off-site for storage, backups can be run and stored locally, and then copied to the cloud server's deduplication disk storage device. Additionally, this feature can be used by customers with widely distributed networks who want to use Backup Exec servers in remote offices for local backups, and then copy the backup sets to a Backup Exec server that is located in a central data center. This option is part of the Cloud Services for Backup Exec feature.</p>

# What happens when CASO communication thresholds are reached

In a CASO environment, communications that occur between managed Backup Exec servers and the central administration server can sometimes be disrupted even if network communications are normal. If job-related communication disruptions occur between a managed Backup Exec server and the central administration server, the managed Backup Exec server's communication status changes from Enabled to Stalled or No Communication. The jobs waiting to be processed by the managed Backup Exec server are held in the managed Backup Exec server's job queue until the communications are restored.

You can set the amount of time that Backup Exec waits before changing the managed Backup Exec server's status if it becomes unresponsive. When a managed Backup Exec server's status changes to Stalled or No Communication, the central administration server changes how it handles current and future jobs delegated to the stalled managed Backup Exec server.

For example, if communications from a managed Backup Exec server are not received at the central administration server after the set amount of time, the central administration server changes the Backup Exec server's communication status to Stalled. Job delegation to the managed Backup Exec server is suspended as it continues to wait for the managed Backup Exec server to return to an Enabled status. Jobs are delegated to other managed Backup Exec servers that are represented in the destination storage device or Backup Exec server pool.

CASO continues to monitor the amount of time during which no communications are received from the managed Backup Exec server. After a set amount of time passes after a Stalled status appears, CASO changes the status of the managed Backup Exec server to No Communication. CASO marks the jobs as Failed, and then begins job recovery by invoking the custom error-handling rule Recovered Jobs for any job that is active at the time the No Communication status appears.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

## Enabling communications between the managed Backup Exec server and the central administration server

You can manually enable communications between the managed Backup Exec server and the central administration server. When communications are disabled, jobs cannot be delegated to the managed Backup Exec server.

**To enable communications between the managed Backup Exec server and the central administration server**

- 1 From the central administration server's **Storage** tab, right-click the managed Backup Exec server for which you want to disable communications.
- 2 Select **Communication Enabled**.

See [“Disabling communications between the managed Backup Exec server and the central administration server”](#) on page 1026.

## Disabling communications between the managed Backup Exec server and the central administration server

You can manually disable communications between the managed Backup Exec server and the central administration server. When communications are disabled, jobs cannot be delegated to the managed Backup Exec server.

**To disable communications between the managed Backup Exec server and the central administration server**

- 1 From the central administration server's **Storage** tab, right-click the managed Backup Exec server for which you want to disable communications.
- 2 Select **Communication Enabled**.

See [“Enabling communications between the managed Backup Exec server and the central administration server”](#) on page 1025.

## About alerts and notifications in CASO

In a Central Admin Server Option (CASO) environment, alerts that are generated on a managed Backup Exec server are automatically rolled up to the central administration server. To see those alerts on the central administration server, you must configure alert categories to enable or disable alerts on each managed Backup Exec server and on the central administration server itself.

After you respond to and clear the active alert on the central administration server, the alert is cleared on the managed Backup Exec server as well.

If you enable Backup Exec alerts on a managed Backup Exec server without enabling alerts on the central administration server, alerts appear only on the managed Backup Exec server where they are generated; they do not appear on the central administration server.

Enable and configure alerts at the central administration server, and then copy the alert configurations to a managed Backup Exec server. When the alert is

generated on a managed Backup Exec server, it appears on both the managed Backup Exec server and the central administration server.

See [“Copying alert configurations to managed Backup Exec servers”](#) on page 1027.

On the central administration server, you can view alerts for all managed Backup Exec servers, or you can filter the alerts to view only those for a specific managed Backup Exec server or Backup Exec server pool.

You can configure a notification on either the central administration server or the managed Backup Exec server. Regardless of where you configure the notification, if it is for a delegated job, it is sent by the central administration server. You can choose to notify the local administrator of the managed Backup Exec server, or the administrator of the central administration server, or both.

## Copying alert configurations to managed Backup Exec servers

Enable and configure alerts at the central administration server, and then copy the alert configurations to a managed Backup Exec server. After the alert configurations are copied, alerts that are generated on a managed Backup Exec server appear on both the managed Backup Exec server and the central administration server.

See [“About alerts and notifications in CASO”](#) on page 1026.

**To copy alert configurations to managed Backup Exec servers.**

- 1 On the central administration server, click the Backup Exec button.
- 2 Select **Configuration and Settings**, and then select **Copy Settings to Backup Exec Servers**.
- 3 Under **Select settings to copy**, check **Alert configuration**.
- 4 Click **Add**.
- 5 Enter the name of a managed Backup Exec server to which you want to copy the alert configuration.
- 6 Click **OK**.
- 7 On the **Copy Settings** dialog box, click **OK**.

An alert on the central administration server will confirm that the copy succeeded.

## Enabling managed Backup Exec servers to use any available network interface card

By default, jobs that are delegated or copied to a managed Backup Exec server from the central administration server use the network and security settings that are set on the managed Backup Exec server.

However, you can select an option on the central administration server to let a job use any network interface to access Backup Exec agents if the selected network interface is unavailable. Enabling this option for a backup job lets the managed Backup Exec server use an alternative network interface to run important backup jobs that would otherwise fail to run.

### To enable managed Backup Exec servers to use any available network interface card

- 1 On the central administration server, click the Backup Exec button.
- 2 Select **Configuration and Settings**, and then select **Backup Job Defaults**.
- 3 Select **Back Up to Disk**, **Back Up to Tape**, or **Back Up to Deduplication Disk Storage Device**, depending on the type of storage device that you use.
- 4 In the left pane, select **Network**.
- 5 Check **Allow managed Backup Exec server to use any network interface to access Backup Exec agents**.  
See “[Network options](#)” on page 195.
- 6 Click **OK**.

## About job delegation in CASO

Job delegation is the automatic load balancing of jobs among the various storage devices that are attached to the managed Backup Exec servers. The job is created on the central administration server, but can be run on any managed Backup Exec server.

When the storage devices are logically grouped in Backup Exec server pools, and as the storage devices become available, they process jobs that are delegated from the central administration server. For example, if a storage pool contains two storage devices and one is busy processing a job, the central administration server automatically delegates another job to the idle storage device.

See “[How to use Backup Exec server pools in CASO](#)” on page 1029.

## About copying jobs instead of delegating jobs in CASO

If the managed Backup Exec server's storage and media data are kept on a local database on the managed Backup Exec server, the central administration server cannot delegate jobs to it. Instead, you can copy job options, default schedules, error-handling rules, and alert configurations from the central administration server to the managed Backup Exec server. A persistent network connection to the central administration server is not needed when the jobs are run locally on the managed Backup Exec server.

Use the same names for objects on the central administration server and all of the managed Backup Exec servers that you want to copy jobs to. For example, use the same name for a storage pool on the central administration server and on the managed Backup Exec server. Then, it is not necessary to customize settings or names for each managed Backup Exec server that you copy jobs to.

See [“Copying configuration settings to another Backup Exec server”](#) on page 519.

## About adding storage devices in a CASO environment

From the central administration server, you can run the **Configure Storage Wizard** to set up devices for the central administration server or for any of the managed Backup Exec servers. After managed Backup Exec servers are installed, they appear on the **Storage** tab of the central administration server. When you start the **Configure Storage Wizard**, you are prompted to select the server for which you want to configure storage. You can choose the central administration server or any managed Backup Exec server that runs the same version of Backup Exec as the central administration server.

## How to use Backup Exec server pools in CASO

In a CASO environment, you can group multiple managed Backup Exec servers together into Backup Exec server pools. If you create a pool of managed Backup Exec servers, all of the pools on those managed Backup Exec servers are available for job delegation. If there are multiple devices attached to each of the managed Backup Exec servers in the Backup Exec server pool, you can create multiple, smaller pools that are made up of fewer storage devices. Use this method to send some jobs to a specific pool in the Backup Exec server pool, and send other jobs to a different pool in the same Backup Exec server pool.

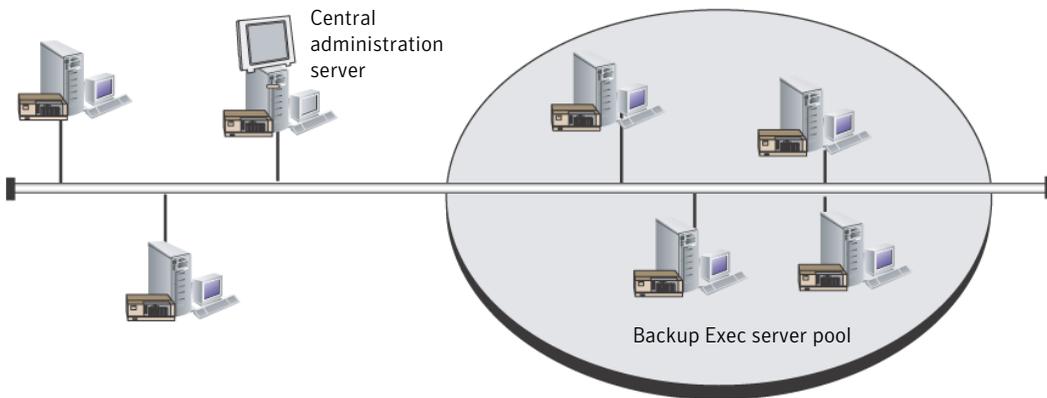
Backup Exec server pools can contain multiple managed Backup Exec servers or just one managed Backup Exec server. A managed Backup Exec server can belong to more than one Backup Exec server pool. The central administration server can

be used as a managed Backup Exec server and can be included in the Backup Exec server pool.

Any managed Backup Exec server or Backup Exec server in a pool must be able to access the destination device for the backup. If there is no intersection between the device and the managed Backup Exec server or Backup Exec server pools, the job does not run. The Jobs list displays the following status: Ready; No Backup Exec server available in Backup Exec server pool.

This graphic shows a Backup Exec server pool.

**Figure L-3** An example of a CASO-configured Backup Exec server pool inside a corporate network



See [“Creating a Backup Exec server pool”](#) on page 1031.

See [“Selecting a Backup Exec server pool for backups”](#) on page 1030.

## Selecting a Backup Exec server pool for backups

You can run a job on storage devices that are on a specific managed Backup Exec server or on storage devices that are in a group of managed Backup Exec servers. This filter lets you control where certain jobs are delegated. For example, to always run backups of Exchange databases only on the devices that are attached to managed Backup Exec servers in a pool named Exchange Backups, you could select this option, and then select the Exchange Backups server pool.

### To select a Backup Exec server pool for backups

- 1 Create a backup definition.
- 2 On the **Backup** box, click **Edit**.
- 3 On the **Backup Options** dialog box, in the left pane, select **Storage**.

- 4 In **Backup Exec server** or **Backup Exec server pool**, select the pool that you want to use for all of the backups in the backup definition.
- 5 Configure any additional options for the backup definition.

See [“How to use Backup Exec server pools in CASO ”](#) on page 1029.

## Creating a Backup Exec server pool

You can group, or pool, Backup Exec servers.

See [“How to use Backup Exec server pools in CASO ”](#) on page 1029.

See [“Adding managed Backup Exec servers to a Backup Exec server pool ”](#) on page 1031.

### To create a Backup Exec server pool

- 1 On the central administration server’s **Storage** tab, in the **Configure** group, select **Configure Storage**.
- 2 Follow the instructions in the Configure Storage wizard.

## Backup Exec server pool properties

The following properties are available for Backup Exec server pools.

See [“Creating a Backup Exec server pool”](#) on page 1031.

**Table L-4** Backup Exec server pool properties

Item	Description
<b>Name</b>	Lets you change the name of the pool.
<b>Description</b>	Lets you change the description of the pool.
<b>Backup Exec servers that belong to the pool</b>	Lists the Backup Exec servers that are in the pool. You can add or remove servers by checking or unchecking the check boxes next to the names of the servers.

## Adding managed Backup Exec servers to a Backup Exec server pool

You can add managed Backup Exec servers to existing Backup Exec server pools.

See [“Creating a Backup Exec server pool”](#) on page 1031.

#### To add managed Backup Exec servers to a Backup Exec server pool

- 1 On the central administration server, select the **Storage** tab.
- 2 Expand **All Storage Pools**, and then double-click a Backup Exec server pool to which you want to add managed Backup Exec servers.
- 3 Under **Backup Exec servers that belong to the pool**, check the check boxes for the Backup Exec servers that you want to add to the pool.
- 4 Click **Apply**.

## Deleting a Backup Exec server pool

You can delete a Backup Exec server pool at any time.

#### To delete a Backup Exec server pool

- 1 On the central administration server, select the **Storage** tab.
- 2 Expand **All Storage Pools**
- 3 Right-click the Backup Exec server pool that you want to delete, and then click **Delete**.
- 4 Click **Yes** to confirm that you want to delete the pool.

See [“Removing a managed Backup Exec server from a Backup Exec server pool”](#) on page 1032.

## Removing a managed Backup Exec server from a Backup Exec server pool

Removing a managed Backup Exec server deletes it from a Backup Exec server pool, but does not remove it from Backup Exec.

#### To remove a managed Backup Exec server from a Backup Exec server pool

- 1 On the central administration server, select the **Storage** tab.
- 2 Expand **All Storage Pools**, and then double-click the Backup Exec server pool that contains the server you want to delete.
- 3 Under **Backup Exec servers that belong to the pool**, uncheck the check boxes for the Backup Exec servers that you want to remove from the pool.
- 4 Click **Apply**.

See [“How to use Backup Exec server pools in CASO ”](#) on page 1029.

## How centralized restore works in CASO

Depending on whether the required storage media resides in storage devices or is stored offsite, initiating restore operations from the central administration server can be an automated process with little user intervention necessary.

When you use centralized restore with online media, you run the restore wizard at the central administration server. During the data selection process, CASO determines which media are required to complete the restore operation, and then queries the Backup Exec storage and media database to determine the identity of the storage device where the media reside. After you run the restore wizard, CASO begins the restore operation by delegating the jobs to the central administration server or managed Backup Exec servers that control the selected storage devices. If the data that is being restored spans multiple storage media, you are prompted to load additional media as needed to successfully complete the restore operation.

When you use centralized restore with offline media, you run the restore wizards at the central administration server. During the data selection process, CASO determines the media required to complete the restore operation, and then queries the Backup Exec storage and media database to determine the identity of the storage device where the primary media resides. If the media is not found in a storage device, the media is considered offline. CASO then presents you with a selection of drive pools and storage devices that are compatible with the type of media being used during the restore operation, thus giving you the flexibility of choosing a storage device in which to load your media.

After noting the identity and location of the storage device you have selected to run the job, you do the following:

- Submit the restore job on hold as a scheduled job
- Retrieve the media, place it in the storage device
- Remove the job from hold at the central administration server, at which time the restore job begins.

CASO then delegates the job to the managed Backup Exec server that controls the selected storage device. If the data being restored spans multiple storage media, you are prompted to load additional media as needed to successfully complete the restore operation.

Before restore operations from the central administration server can be initiated, the following requirements must be met:

- Managed Backup Exec server communication status must be Enabled.
- Managed Backup Exec servers must be online with all Backup Exec server statuses showing Online.

See [“Best practices for centralized restore in CASO”](#) on page 1035.

## How CASO restores data that resides on multiple storage devices

If the data selected for restore is located on a single device attached to a managed Backup Exec server, then a single restore job is created at, and then delegated from, the central administration server. However, if the data being selected for restore is located on multiple devices in the CASO environment, then the single restore job is split into separate restore jobs, depending on the number of devices involved.

All split restore jobs have the same name as the original job, but are differentiated and linked with a subscript numeral that is appended to the job name.

For example, if you create a restore job and the data you select for restore resides in one device on a managed Backup Exec server, CASO creates one restore job. However, if you create one restore job and the data you select resides on two or more devices that are attached to a managed Backup Exec server, CASO creates two or more restore jobs.

See [“Best practices for centralized restore in CASO”](#) on page 1035.

The following graphic shows how CASO restores data that is stored on a single device.

**Figure L-4** For data stored on a single storage device

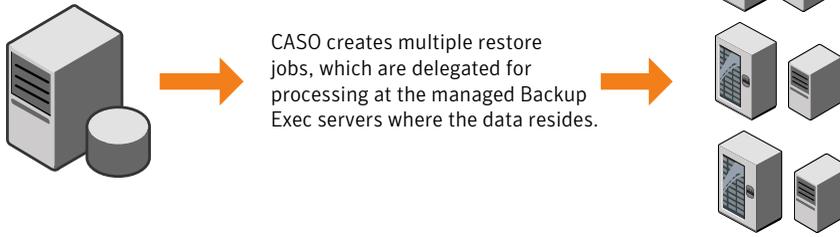
You select the data to restore from the administration console of the central administration server.



The following graphic shows how CASO restores data that is stored on multiple devices.

**Figure L-5** For data stored on multiple storage devices

You select the data to restore from the administration console of the central administration server.



## Best practices for centralized restore in CASO

Symantec recommends the following best practices when using centralized restore:

- Select only one resource to restore for each job.
- Select the same restore device or Backup Exec server for all of the selections that are in the same restore job.
- Select a Backup Exec server that has compatible devices for all media that is required for the restore job.

See [“About restoring from the central administration server”](#) on page 1035.

## About restoring from the central administration server

Use the Restore Wizard to restore data from the central administration server. Before you create a restore job, review the best practices for centralized restore.

See [“Best practices for centralized restore in CASO”](#) on page 1035.

See [“How centralized restore works in CASO”](#) on page 1033.

## About recovering failed jobs in CASO

The Backup Exec error-handling rule named Recovered Jobs is a custom error-handling rule that is used by CASO to recover jobs that failed because of issues with internal job communications. This rule is created when Backup Exec is installed and is enabled by default.

The retry options for this rule are to retry the job twice, with an interval of five minutes between the retry attempts. During the first retry attempt, CASO attempts to re-delegate the jobs to another available managed Backup Exec server.

If this attempt fails, CASO makes a second attempt at finding another available managed Backup Exec server to process the jobs. If no managed Backup Exec servers are available, the final job disposition is to place the job on hold until you have fixed the error condition.

---

**Note:** If the Checkpoint Restart error-handling rule is enabled, then recovered jobs are not resubmitted to a Backup Exec server pool to be run on a different server. The Checkpoint Restart error-handling rule reschedules the job to run on the original server when that server comes online. To enable a recovered job to be resubmitted to a Backup Exec server pool, you must disable the Checkpoint Restart error-handling rule.

---

**Note:** If you target a job to a Backup Exec server pool that contains multiple managed Backup Exec servers and a job failure occurs, the recovery process uses only the managed Backup Exec servers in the Backup Exec server pool. Managed Backup Exec servers that are not in the Backup Exec server pool are not used for job recovery.

---

When you open the job history entry for a Recovered job, the reason for the failure is listed as Job Errors, with an explanation of the type of internal communication error that occurred. The job history entry also indicates that the job was recovered.

---

**Note:** Job logs are not created for jobs that are recovered.

---

The following table describes the CASO error codes that are selected by default for the Recovered Jobs custom error-handling rule:

**Table L-5** Error codes for Recovered Jobs custom error-handling rule

Error code	Description
0xE000881B JOBDISPATCH	The displayed message is: Job failed while being dispatched. The job will be recovered.

**Table L-5** Error codes for Recovered Jobs custom error-handling rule  
(continued)

Error code	Description
0xE000881D JOB_CASO_QUEUE FAILURE	The displayed message is: The job could not be delegated to the destination managed Backup Exec server. The managed Backup Exec server may not be online, or there may be a communications failure. The job will be recovered.
0xE000881E JOB_CASO_REMOTEMMS_STARTFAILURE	The displayed message is: The job failed to start on the destination managed Backup Exec server, possibly because a database error occurred. The job will be recovered.

See [“About error-handling rules for failed or canceled jobs”](#) on page 270.

See [“Custom error-handling rule for recovered jobs”](#) on page 275.

See [“Changing the settings for a managed Backup Exec server”](#) on page 1018.

## Pausing a managed Backup Exec server

You can pause and resume a managed Backup Exec server from the central administration server.

Pausing a managed Backup Exec server prevents the central administration server from delegating jobs to it. When paused, the managed Backup Exec server’s status changes from Online to Paused

---

**Caution:** When installing Backup Exec options at a managed Backup Exec server, the managed Backup Exec server must be paused so that no further jobs are delegated to it from the central administration server while the installation process occurs. If jobs are running, let them finish or cancel them before beginning the installation.

---

#### To pause a managed Backup Exec server

- 1 From the central administration server's **Storage** tab, right-click the managed Backup Exec server that you want to pause.
- 2 Click **Pause**.

See [“Resuming a paused managed Backup Exec server”](#) on page 1038.

## Resuming a paused managed Backup Exec server

When you resume a paused managed Backup Exec server, the following changes occur:

- Jobs can be delegated from the central administration server to the managed Backup Exec server.
- The managed Backup Exec server's status changes from Paused to Online in the **State** column on the **Storage** tab.

#### To resume a paused managed Backup Exec server

- 1 From the central administration server's **Storage** tab, right-click the managed Backup Exec server that you want to resume.
- 2 Click **Pause** to remove the check mark next to **Pause**.

See [“Pausing a managed Backup Exec server”](#) on page 1037.

## Stopping Backup Exec services for a managed Backup Exec server

You can stop the Backup Exec services on a managed Backup Exec server from the central administration server.

#### To stop Backup Exec services for a managed Backup Exec server

- 1 On the central administration server's **Storage** tab, right-click the managed Backup Exec server for which you want to stop services.
- 2 Select **Backup Exec Services**.
- 3 On the **Backup Exec Services Manager** dialog box, click **Stop all services**.
- 4 Click **Close**.

See [“Starting Backup Exec services for a managed Backup Exec server”](#) on page 1039.

# Starting Backup Exec services for a managed Backup Exec server

You can start the Backup Exec services on a managed Backup Exec server from the central administration server.

## To start Backup Exec services for a managed Backup Exec server

- 1 On the central administration server's **Storage** tab, right-click the managed Backup Exec server for which you want to stop services.
- 2 Select **Backup Exec Services**.
- 3 On the **Backup Exec Services Manager** dialog box, click **Start all services**.
- 4 Click **Close**

See [“Stopping Backup Exec services for a managed Backup Exec server”](#) on page 1038.

# Viewing managed Backup Exec server properties

From the central administration server, you can view properties for managed Backup Exec servers.

## To view managed Backup Exec server properties

- 1 On the central administration server's **Storage** tab, double-click the managed Backup Exec server for which you want to view properties.
- 2 In the left pane, select **Properties**.

See [“Properties for central administration servers and managed Backup Exec servers”](#) on page 1039.

# Properties for central administration servers and managed Backup Exec servers

See [“Viewing managed Backup Exec server properties”](#) on page 1039.

**Table L-6** Properties for a central administration server or a managed Backup Exec server

Item	Description
Name	Displays the name of the managed Backup Exec server or the central administration server.

**Table L-6** Properties for a central administration server or a managed Backup Exec server *(continued)*

<b>Item</b>	<b>Description</b>
<b>Description</b>	Indicates whether the server is a managed Backup Exec server or a central administration server. You can change this description.
<b>Server status</b>	Indicates the current status of the server, such as online, paused, unavailable, or offline.
<b>Version</b>	Indicates the version of Backup Exec that is installed.
<b>Licnese</b>	Provides information about the Backup Exec license that is installed on the server.
<b>Time zone</b>	Indicates the time zone that is set for the server.
<b>Start date and time</b>	Indicates when the server was started.
<b>Current date and time</b>	Indicates the current data and time on the server.
<b>Operating system type</b>	Indicates the type of operating system that is installed on the server.
<b>Operating system version</b>	Indicates the version of the operating system that is installed on the server.
<b>Operating system build</b>	Indicates the build number of the operating system that is installed on the server.
<b>Procesor type</b>	Indicates the type of processor that the server has.
<b>Number of processors</b>	Indicates the number of processors that the server has.
<b>Total physical memory</b>	Indicates the total amount of physical memory that the server has.
<b>Available physical memory</b>	Indicates the amount of physical memory that is available on the server.
<b>Total virtual memory</b>	Indicates the total amount of virtual memory that the server has.

**Table L-6** Properties for a central administration server or a managed Backup Exec server (*continued*)

Item	Description
Available virtual memory	Indicates the amount of virtual memory that is available on the server.
Total pagefile size	Indicate the total amount of memory that is available in the server's pagefile.

## Viewing the settings for a central administration server

If you have the Central Admin Server Option (CASO), you can view information about the location of the databases for Backup Exec. The databases include the Backup Exec Database, the device and media database (ADAMM), and the catalog database.

During Backup Exec installation, if you chose the default option to create a local Backup Exec SQL Express instance on which to store the Backup Exec Database, the databases are all located on the local Backup Exec server. If you chose another instance on the network on which to store the Backup Exec Database, then the databases are all located on the Microsoft SQL Server that contains that instance.

### To view the settings for a central administration server

- 1 Do one of the following:
  - Click the Backup Exec button, select **Configuration and Settings**, and then click **Local server properties**.
  - On the **Storage** tab, double-click the central administration server.
- 2 In the left pane, click **Settings**.  
See "[Settings for a central administration server](#)" on page 1041.

## Settings for a central administration server

If you have the Central Admin Server Option (CASO), you can view information about the location of the databases for Backup Exec. The databases include the Backup Exec Database, the device and media database (ADAMM), and the catalog database.

See "[Viewing the settings for a central administration server](#)" on page 1041.

**Table L-7** Settings for a central administration server

Item	Description
<b>Server</b>	Shows the name of the Microsoft SQL Server that contains the Backup Exec Database .
<b>Instance</b>	Shows the name of the instance that the Backup Exec Database is installed on.
<b>Name</b>	Shows the Microsoft SQL Server name of the Backup Exec Database .
<b>Path</b>	Shows the path of the Backup Exec Database .
<b>Server</b>	Shows the name of the Microsoft SQL Server that contains the Advanced Device and Media Management (ADAMM) database.
<b>Instance</b>	Shows the name of the instance that the Advanced Device and Media Management (ADAMM) database is installed on.
<b>Name</b>	Shows the Microsoft SQL Server name for the Advanced Device and Media Management (ADAMM) database.

**Table L-7** Settings for a central administration server (*continued*)

Item	Description
<b>Path</b>	Shows the path of the Advanced Device and Media Management (ADAMM) database.
<b>Server</b>	Shows the name of the Microsoft SQL Server that contains the Backup Exec catalog database.
<b>Instance</b>	Shows the Database instance that contains the catalog database.
<b>Name</b>	Shows the Microsoft SQL Server name for the Backup Exec catalog database.
<b>Path</b>	Shows the path of the Backup Exec catalog database.
<b>Private cloud server</b>	Indicates if the private cloud server option is enabled or disabled.

## Disaster Recovery in CASO

Use the Symantec Backup Exec Simplified Disaster Recovery (SDR) option to protect both managed Backup Exec servers and the central administration server in a CASO environment.

See [“About Simplified Disaster Recovery”](#) on page 704.

Before implementing the SDR option in a CASO environment, review the following:

- To create recovery media for any managed Backup Exec server or central administration server, the **Create Simplified Disaster Recovery Disk Wizard**

must be run at the central administration server. If you use a remote administration environment, connect to the central administration server.

- If you want managed Backup Exec servers to be protected using a bootable disk image, you must run the **Create Simplified Disaster Recovery Disk Wizard** at each of the managed Backup Exec servers where a bootable disk device is installed.
- You must locally back up and restore a central administration server.

## Troubleshooting CASO

If you encounter issues with CASO, review the following questions and answers.

**Table L-8** Troubleshooting CASO

Question	Answer
I received error 1065 that says "Database specified does not exist". What causes this error?	<p>This error can occur for the following reasons:</p> <ul style="list-style-type: none"> <li>■ UDP traffic is blocked on the network between the central administration server and the managed Backup Exec server.</li> <li>■ The SQL configuration on the central administration server is not set correctly.</li> <li>■ When the central administration server is installed to a named SQL instance and the SQL browser service is not running..</li> <li>■ The Named Pipes or TCP/IP protocols are not enabled or are not set for remote connections.</li> </ul>
I changed the system time, but the change hasn't gone into effect on my managed Backup Exec servers or central administration server. Why?	If you change the system time on either the managed Backup Exec server or the central administration server, you must restart the Backup Exec services. Backup Exec processes the time change when the services restart.

See [“About the Central Admin Server Option”](#) on page 996.

## Running the Backup Exec Utility for CASO operations

A separate application called Backup Exec Utility is available to help you perform the following CASO operations:

- Move a managed Backup Exec server.
- Disable or enable communication with a managed Backup Exec server.

Use the Backup Exec Utility only with the guidance of Symantec Technical Support. Improper use of this utility can result in configuration changes that may prevent Backup Exec from running.

#### To run the Backup Exec Utility

- 1 From the Backup Exec installation directory, in `\Program Files\Symantec\Backup Exec`, double-click **BEUtility**.
- 2 On the Backup Exec Utility menu, click **Help** to learn about how to use BEUtility..

## Uninstalling Backup Exec from the central administration server

Before you uninstall Backup Exec from the central administration server, you must delete all managed Backup Exec servers from the **Storage** tab on the central administration server.

---

**Caution:** Failure to uninstall in the following sequence may result in long delays when shutting down Backup Exec services during the uninstall of Backup Exec on the managed Backup Exec servers.

---

#### To uninstall Backup Exec from the central administration server

- 1 On the central administration server's **Storage** tab, right-click a managed Backup Exec server.
- 2 Select **Delete**.
- 3 Click **Yes** to confirm that you want to delete.
- 4 Repeat steps 1 through 3 for each managed Backup Exec server that the central administration server manages.
- 5 Uninstall Backup Exec from the central administration server.  
See "[Uninstalling Backup Exec](#)" on page 128.

## Uninstalling Backup Exec from a managed Backup Exec server

You must delete the managed Backup Exec server from the **Storage** tab on the central administration server before you uninstall Backup Exec.

To uninstall Backup Exec from a managed Backup Exec server

- 1 On the central administration server's **Storage** tab, right-click a managed Backup Exec server.
- 2 Select **Delete**.
- 3 Uninstall Backup Exec from the managed Backup Exec server.

See [“Uninstalling Backup Exec”](#) on page 128.

# Symantec Backup Exec Advanced Disk-based Backup Option

This appendix includes the following topics:

- [About the Advanced Disk-based Backup Option](#)
- [About installing the Advanced Disk-based Backup Option](#)
- [About the synthetic backup feature](#)
- [About true image restore for synthetic backups](#)
- [About off-host backup](#)
- [Troubleshooting the off-host backup](#)

## About the Advanced Disk-based Backup Option

The Advanced Disk-based Backup Option provides the following features:

- **Synthetic backup**  
This feature enables a full backup to be assembled, or synthesized, from a baseline full backup and subsequent incremental backups.  
The benefits of using a synthetic backup include the following:
  - A reduced backup window since the synthetic backup can be scheduled outside of the time-critical backup window.
  - Reduced network traffic since the synthetic backup does not need to access the network.

- True image restore, which enables Backup Exec to restore the contents of directories to what they were at the time of any synthetic full or incremental backup.
- Off-host backup  
This feature enables the backup operation to be processed on a Backup Exec server instead of on the remote computer or host computer. Moving the backup from the remote computer to the Backup Exec server enables better backup performance and frees the remote computer as well.

See [“About the synthetic backup feature”](#) on page 1048.

See [“About off-host backup ”](#) on page 1052.

See [“About installing the Advanced Disk-based Backup Option”](#) on page 1048.

## About installing the Advanced Disk-based Backup Option

The Advanced Disk-based Backup Option (ADBO) is installed as part of the Enterprise Server Option, for which you must enter a license on the Backup Exec server.

See [“About installing Backup Exec”](#) on page 58.

## About the synthetic backup feature

The synthetic backup feature eliminates the need to perform recurring full backups for supported remote resources. The synthetic backup is assembled from a full backup (called a baseline) and subsequent incremental backups.

The resulting synthetic backup then becomes the new baseline. Only incremental backups are required until the next synthetic backup is created. The synthetic backup is as current as the last incremental backup that it contains.

The components of a synthetic backup are as follows:

- Baseline backup.  
The baseline backup is the first full backup to run that is associated with the synthetic backup. The full baseline backup runs one time only, and backs up all of the files on the selected computer when it runs.
- Recurring incremental backups.  
Incremental backup jobs back up the files that change after the baseline backup.
- Recurring synthetic backups.

The synthetic backup process combines the data from the baseline backup and the incremental backups to form a synthesized full backup of the selected computer. This synthesized full backup becomes a new baseline backup, which is combined with subsequent incremental backup sets to form a new synthesized full backup.

For any of the backups in a synthetic backup, you can add a stage to duplicate the backup data to tape.

See [“About duplicating backed up data”](#) on page 218.

True image restore is automatically enabled for synthetic backups. True image restore lets you restore directories as they existed at the time of the synthetic backup. Files that were deleted before the time of the synthetic backup are not restored. In true image restore, only the correct versions of files are restored from the appropriate synthetic full or incremental backups that contain them.

Only file system data is supported for synthetic backup. Supported data includes common file system objects, such as volumes, drives, and folders.

See [“Requirements for synthetic backup”](#) on page 1049.

See [“About true image restore for synthetic backups”](#) on page 1050.

## Requirements for synthetic backup

Before you create a synthetic backup, review the following information:

- If you use an encryption key, all of the associated backups must use the same encryption key. Do not change the encryption key after the backups are created. The encryption key that is selected in the associated backups is automatically applied to the synthetic backup.
- You must configure disk storage before you can create a synthetic backup. For synthetic backups, incremental backups must use disk storage. The baseline full backup and the synthetic full backup can use tape or disk storage. See [“About the Configure Storage wizard”](#) on page 145.
- If you send the baseline backup job to tape storage, and you want to use tape storage for the synthetic backup job, you must have two tape drives. You must use a tape drive to mount the baseline backup, and use a tape drive to mount the synthetic backup.
- You can select file system data only for synthetic backup.

## About true image restore for synthetic backups

True image restore is automatically enabled for synthetic backups. True image restore enables Backup Exec to restore the contents of directories to what they were at the time of any full backup or incremental backup. Restore selections in backup sets are made from a view of the directories as they existed at the time of the synthetic backup. Files that were deleted before the time of the backup are not restored. In true image restore, only the correct versions of files are restored from the appropriate full or incremental backups that contain them. Previous versions are not restored and then overwritten.

Backup Exec collects the information that is required to detect the files and directories that have been moved, renamed, or newly installed from a tape archive (tar) or a compressed archive. Depending on how the files were packaged and how they were installed, some newly installed files are not backed up by normal incremental backups. With true image restore enabled, Backup Exec compares path names with path names from the previous full or incremental backup. If a name is new or changed, the file or directory is backed up.

The following are examples where using true image restore backs up the files that would not otherwise be backed up:

- A file named C:\pub\doc is moved to or installed in C:\spec\doc. Here, the archive bit is unchanged for files and subdirectories inside that directory, but C:\pub\doc is new in the C:\spec\ directory and is backed up.
- A directory named C:\security\dev\ is renamed as C:\security\devices\. Here, the archive bit is unchanged for files and subdirectories inside that directory, but C:\security\devices\ is a new directory and is backed up.

The following table lists the files that are backed up in the C:\user\doc directory during a series of backups between December 1, 2012 and December 4, 2012:

**Table M-1** Example table of files backed up because true image restore is enabled

Day	Type of backup	Backed up files in C:\user\doc					
December 1, 2012	Full	file1	file2	dirA\fileA	dirB\fileB	file3	
December 2, 2012	Incremental	file1	file2	dirA\fileA	—————	—————	
December 3, 2012	Incremental	file1	file2	dirA\fileA	—————	—————	
December 4, 2012	Incremental	file1	file2	—————	—————	—————	file4

---

**Note:** Dashes (-----) indicate that the file was deleted before this backup.

---

Assume that you want to restore the December 4, 2012 version of the C:\user\doc directory.

You perform a regular restore of the full backup set followed by a regular restore of subsequent incremental backup sets. The restored directory contains all files and directories that ever existed in C:\user\doc from December 1, 2012 (last full backup) through December 4, 2012.

For example, the following files and directories are included:

- file1
- file2
- dirA\fileA
- dirB\fileB
- file3
- file4

In a true image restore of the December 4, 2012 backup, the restored directory has only the files and directories that existed at the time of the incremental backup on December 4, 2012.

The following list includes the files and directories that existed:

- file1
- file2
- file4

Backup Exec does not restore any of the files that were deleted before the December 4, 2012 incremental backup.

The restored directory does not include the 'dirA' subdirectories, even though they were backed up on December 4, 2012. Backup Exec does not restore these directories because they did not exist at the time of the incremental backup, which was the reference for the true image restore.

A true image restore preserves the files that are currently in the directory but were not present when the backup was completed. Assume that you created a file named file5 after the incremental backup that occurred on December 4, 2012, but before doing the restore.

In this case, the directory contains the following files after the restore:

- file1

- file2
- file4
- file5

## About off-host backup

Off-host backup enables Backup Exec to move backup processing from the host computer to the Backup Exec server. The off-host backup creates a snapshot of the volume or volumes that are selected for backup on the remote computer. The snapshots are then imported to the Backup Exec server, where they are backed up.

After the backup, the snapshots are exported from the Backup Exec server and mounted back on the remote computer and resynchronized with the source volume. This process requires solutions from the hardware providers or the software providers that can support transportable snapshots. Transportable snapshots are snapshots you can import to and export from the Backup Exec server. The Microsoft Volume Shadow Copy Services (VSS) provider that you select is used for each volume in the off-host backup. An off-host backup job is performed on one remote computer at a time.

You can find a list of hardware snapshot providers at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

Off-host backup supports the following:

- Microsoft Volume Shadow Copy Service (VSS).
- Backups for the NTFS volumes that use the full, incremental, and differential backup methods.
- SQL Agent backups for Microsoft SQL Server 2000 databases.
- Exchange Agent backups for Microsoft Exchange Server 2003 (Service Pack 1)/ 2007 instances that run on Windows Server 2003. Support for the option to use Backup Exec Granular Recovery Technology for Exchange Agent backups is included.

Advanced Disk-based Option off-host backup does not support the following:

- The option **Checkpoint Restart**.
- Volumes that run Windows BitLocker Drive Encryption.

See “[Requirements for off-host backup](#)” on page 1053.

See “[Backing up data](#)” on page 163.

See “[Editing backups](#)” on page 170.

See [“Setting default backup job settings”](#) on page 456.

See [“Advanced Disk-based Backup options”](#) on page 1054.

See [“Best practices for off-host backup ”](#) on page 1053.

## Requirements for off-host backup

The following are requirements for off-host backup:

**Table M-2** Off-host backup requirements

Item	Description
Backup Exec server	The Advanced Disk-based Backup Option must be installed.
Remote computer	The Agent for Windows must be installed on the remote computer.
Backup Exec server and the remote computer	The following must be installed on both the Backup Exec server and on the remote computer: <ul style="list-style-type: none"> <li>■ The same operating system, either Microsoft Windows Server 2003 with Service Pack 2 or Windows Server 2008.</li> <li>■ The most recent Volume Shadow Copy Services (VSS) patches.</li> <li>■ The Microsoft VSS hardware or software snapshot provider that you want to use. Otherwise, the snapshots of the volumes cannot be exported to the Backup Exec server.</li> <li>■ Ability to access the disk storage that is shared between the Backup Exec server and the remote computer.</li> </ul>
GRT-enabled off-host backup of Exchange Server resources	Either of the following must be installed on the Exchange Server: <ul style="list-style-type: none"> <li>■ Microsoft Exchange Server 2003 (Service Pack 2) or Exchange Server 2007 (Service Pack 3) instances that run on Windows Server 2003.</li> <li>■ Microsoft Exchange Server 2010 (Service Pack 1) instances that run on 64-bit Windows Server 2008/2008 R2.</li> </ul>
Central Admin Server Option	If the Central Admin Server Option (CASO) is installed, do not let the central administration server delegate the job. It can delegate the job to a managed Backup Exec server that does not have off-host capability. You must manually select the storage device for the CASO jobs that use the off-host backup method.

See [“Best practices for off-host backup ”](#) on page 1053.

## Best practices for off-host backup

The following best practices are recommended:

- Keep source volumes and snapped volumes from sharing the same physical disks. Otherwise, any attempt to split the snapshot volume from the original volume fails.
- Most hardware and software providers have some limitation about the types of volumes that are transportable. Therefore, Symantec recommends that you use off-host backup jobs only for backing up data for which all dependent volumes can be imported and exported.
- The off-host backup fails if any one volume that you select for backup cannot be imported or exported. The off-host backup also fails if the required VSS hardware provider is not on a Symantec-approved compatibility list. You can choose to continue the backup if the off-host backup fails.  
You can find a list of compatible types of storage at the following URL:  
<http://entsupport.symantec.com/umi/V-269-2>
- The Hitachi Raid Manager log cannot be on a volume that is being snapped. Hitachi executes I/O to its Raid Manager log file during the snapshot commit process, and the VSS coordinator blocks I/O to any drive being snapped. Therefore, if the log directory for Raid Manager is on the volume that is being snapped, then log I/O is blocked and the snap process is deadlocked.
- If the Central Admin Server Option (CASO) is installed, you must manually select the storage for the off-host backup. Otherwise, the job may be delegated to a Backup Exec server that does not have off-host capability.  
See “[How to use Backup Exec server pools in CASO](#)” on page 1029.
- When you run an off-host backup that uses a VSS hardware provider in a Microsoft Cluster (MSCS) environment, the Backup Exec server and the remote computer must not be in the same cluster group. The cluster applications cannot support the devices’ logical unit numbers (LUNs) that have duplicate signatures and partition layouts. The snapshots containing the LUNs must be transported to a host computer that is outside the cluster.

See “[Troubleshooting the off-host backup](#)” on page 1055.

See “[Off-host backup issues with hardware providers](#)” on page 1058.

See “[Off-host backup issues with hardware providers](#)” on page 1058.

## Advanced Disk-based Backup options

The following options are available for the Advanced Disk-based Backup Option for off-host backup jobs. These options appear when you select the Advanced Disk-Based Backup Option on the **Backup Job Defaults** dialog box and on the **Options** dialog box for a backup job.

See “[Backing up data](#)” on page 163.

See “[Setting default backup job settings](#)” on page 456.

**Table M-3** Advanced Disk-based Backup options

Item	Description
<b>Use offhost backup to move backup processing from the remote computer to the Backup Exec server</b>	Indicates if off-host backup is enabled. See “ <a href="#">About off-host backup</a> ” on page 1052.
<b>Continue the backup job (offhost backup is not used)</b>	Lets the backup job complete without using the off-host feature if the following conditions occur: <ul style="list-style-type: none"> <li>■ The selected volumes do not support off-host backup.</li> <li>■ An error occurs that is related to the snapshot import or the volume import.</li> </ul>
<b>Fail the backup job (further selections are not backed up after failure occurs)</b>	Fails the backup job if the following conditions occur: <ul style="list-style-type: none"> <li>■ The selected volumes do not support off-host backup.</li> <li>■ An error occurs that is related to the snapshot import or the volume import.</li> </ul>
<b>Process logical volumes for offhost backup one at a time</b>	Enables the backup of multiple volumes in one job, while a snapshot is created of only one logical volume at a time. To ensure database integrity, or if a volume contains mount points, multiple volumes may need to be snapped at one time.  After the logical volume is snapped and backed up, the snapshot is deleted before the next logical volume is snapped. This option increases the ability to meet the minimum quiet time that is needed to complete a snapshot.  A logical volume can comprise multiple physical volumes. A single logical volume can encompass all of the volumes on which databases reside.

## Troubleshooting the off-host backup

Off-host backup requires that the VSS providers and the volumes that are to be transported are set up correctly. Not all arrays are supported with the Advanced Disk-based Option.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

To troubleshoot off-host backup issues, Symantec recommends that you use the tools that are available from the VSS provider to verify the required setup for off-host backup.

The minimum setup requirements are as follows:

- Volumes that you want to back up are snappable.
- Volumes are shared between the remote computer and the Backup Exec server.
- An off-host backup job can only contain the volumes that can be transported to the Backup Exec server for backup.

Other factors to consider are as follows:

- Microsoft Windows Server 2003 with Service Pack 2 or Windows Server 2008 with Service Pack 2 must be installed on both the Backup Exec server and on the remote computer. Both computers must have the most recent Volume Shadow Copy Services (VSS) patches.
- Microsoft XML Core Services (MSXML4) must be installed and running on both the Backup Exec server and the remote computer.

Troubleshooting off-host backup issues depends to an extent on the VSS provider that is used for the snapshots.

The following setup issues that are common to all providers may cause off-host backup to fail:

**Table M-4** Common setup issues for off-host backup

Issue	Solution
The volumes are not shared.	You must ensure that all of the volumes reside on the disks that are shared between the remote computer and the Backup Exec server. If the volumes are not shared, the import operation fails. You may need to clean up the snapshots and resynchronize the volumes manually.
The VSS provider is not installed on the Backup Exec server and the remote computer.	The provider that is used for the snapshot must be installed on both the Backup Exec server and on the remote computer. If the provider is not installed on the Backup Exec server, the import operation fails. You may need to clean up the snapshots and resynchronize the volumes manually.

**Table M-4** Common setup issues for off-host backup (*continued*)

Issue	Solution
All volumes are not transportable.	All of the volumes that are selected for backup must be transportable to the Backup Exec server. If Microsoft SQL or Exchange, or other database applications are selected for backup, make sure that the databases and log files reside on transportable volumes.
The VSS provider cannot snap all of the selected volumes.	All of the volumes that are selected for backup must be transportable to the Backup Exec server. All volumes that you select for backup must be snappable by the same provider. You must ensure that the same VSS provider supports all of the volumes in a backup job.
The log path location is incorrect.	If the provider or the supporting application creates log files during normal snapshot operation, the log files should not reside on any of the volumes that are being snapped. VSS cannot flush the write buffers, and the snapshot times out. Change the log path to another volume.
The provider or VSS services are not started.	The provider service should be running and the Microsoft Windows "Volume Shadow Copy" service should not be disabled.
The credentials are incorrect.	The machine-level credentials that are used for the job should be the same on both the Backup Exec server and the remote computer. Incorrect credentials cause snapshots or the backup to fail.
The VSS provider is not installed on all Backup Exec servers in a Central Admin Server Option (CASO) environment.	If you configure a backup job in a CASO environment, you must send the job to managed Backup Exec servers on which the selected VSS provider is installed. You should not let the central administration server delegate the job. Otherwise, the job may be delegated to a managed Backup Exec server that does not have off-host capability.

**Table M-4** Common setup issues for off-host backup *(continued)*

Issue	Solution
<p>The Backup Exec server and the remote computer are in the same cluster group.</p>	<p>For an off-host backup in a Microsoft Cluster environment, the Backup Exec server and the remote computer must not be in the same cluster group. The cluster applications cannot support the devices' logical unit numbers (LUNs) that have duplicate signatures and partition layouts. Therefore, you must transport the snapshots that contain the LUNs to a Backup Exec server that is outside the cluster in which the host cluster resides.</p> <p>See <a href="#">“How Backup Exec works in a Microsoft Cluster Server environment”</a> on page 675.</p> <p>If you use a Hitachi 9970 and attempt to back up Microsoft Cluster data by using the Advanced Disk-based Backup Option, you may receive the following error message:</p> <p>The job failed with the following error: A fault occurred while querying the Writer status.</p> <p>To correct this problem, ensure that the RM Shadow Copy Provider for Volume Snapshot Service is present and running. If the service is not running, run RMVSSPRV.exe from c:\horcm\tool. If the service is still not running, contact Hitachi for support.</p>

See [“Off-host backup issues with hardware providers”](#) on page 1058.

## Off-host backup issues with hardware providers

Hardware disk array vendors may support VSS snapshots and the transporting of volumes to the Backup Exec server for backup in a SAN environment. Using hardware providers requires a sound understanding of how disk arrays are configured for shared access between the remote computer and the Backup Exec server in a SAN.

Consult the documentation for your hardware disk array on how to set up such disk arrays for off-host backup . Specifically, note any limitations on using the disk arrays in context with VSS snapshots, and note how to verify that the volumes

are transportable. Symantec recommends that you make use of any tools that vendors provide to help verify the setup and to troubleshoot issues.

An off-host backup issue that can occur when you use Hitachi hardware may be that Hitachi supports only basic disks for off-host backup. The off-host backup feature is not supported if a computer uses a combination of dynamic and basic disks, and the Hitachi provider.

See [“Troubleshooting the off-host backup ”](#) on page 1055.



# Symantec Backup Exec NDMP Option

This appendix includes the following topics:

- [About the NDMP Option](#)
- [Requirements for using the NDMP Option](#)
- [About installing the NDMP Option](#)
- [About adding an NDMP server to Backup Exec](#)
- [About sharing the devices on an NDMP server between multiple Backup Exec servers](#)
- [About backing up NDMP resources](#)
- [About including and excluding directories and files for NDMP backup selections](#)
- [How to use patterns to exclude files and directories from an NDMP backup selection](#)
- [How to duplicate backed up NDMP data](#)
- [About restoring NDMP data](#)
- [About redirecting restored NDMP data](#)
- [Setting the default options for NDMP](#)
- [Viewing the properties of an NDMP server](#)

## About the NDMP Option

The Symantec Backup Exec NDMP Option uses the Network Data Management Protocol (NDMP) to back up and restore Network Attached Storage (NAS) devices.

You can back up data from a NAS device to the following locations:

- A storage device that is directly connected to the NDMP-enabled NAS device (direct-attached)
- A storage device that is connected to another NDMP-enabled NAS device (3-way)
- A backup-to-disk device on a Backup Exec server (remote)
- A tape device that is attached to a Backup Exec server (remote)
- A shared tape device or backup-to-disk folder that is connected to a SAN with Backup Exec servers.

---

**Note:** You cannot back up NDMP data to a simulated tape library or to a tape device that is attached to a Backup Exec Remote Media Agent for Linux Servers.

---

You can restore data from a storage device on a Backup Exec server to a NAS device. However, you cannot redirect NDMP data to a computer that runs the Windows or Linux operating systems.

You can share tape devices between single or multiple Backup Exec servers and NAS devices by using the Backup Exec Enterprise Server Option.

See “[Requirements for using the NDMP Option](#)” on page 1062.

See “[About installing the NDMP Option](#)” on page 1063.

## Requirements for using the NDMP Option

To use the NDMP Option, the Backup Exec server must have the following items installed:

- Windows Server 2003/Server 2008/Server 2008 R2.
- Backup Exec.  
See “[Installing a custom installation of Backup Exec](#)” on page 70.

In addition, you must have an NDMP server with version 4 of the Network Data Management Protocol enabled.

You can find a list of compatible types of storage at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

## About installing the NDMP Option

The NDMP Option is installed locally on the Backup Exec server as a separate add-on component of Backup Exec. No files are copied to the NDMP server.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

## About adding an NDMP server to Backup Exec

To configure Backup Exec to use the NDMP option, you must add the NDMP server to Backup Exec by using the **Configure Storage** wizard. If any storage devices are attached to the NDMP server, Backup Exec discovers them automatically after the services are restarted, and then adds them to the list of storage devices.

In a CASO environment, you can add an NDMP server only to the following servers:

- A central administration server
- A managed Backup Exec server on which the device and media database is located

See [“About the Configure Storage wizard”](#) on page 145.

## About sharing the devices on an NDMP server between multiple Backup Exec servers

If you use the Backup Exec Central Admin Server Option, you can select which Backup Exec servers can share the devices that are attached to an NDMP server. When you add an NDMP server, the Backup Exec server that you used to add the server is automatically selected for sharing.

---

**Note:** If you upgraded from an earlier version of Backup Exec, your existing configuration is preserved, so you do not have to set up sharing for existing configurations.

---

See [“Sharing a storage device”](#) on page 419.

## About backing up NDMP resources

Before you back up NDMP resources, review the following information:

- Backup Exec cannot gather sufficient file and directory information on an NDMP backup to accurately populate the **Job Summary** and **Set Detail Information** sections of the job history. Therefore, the number of files, directories, files skipped, corrupt files, and files in use always appears as 0.
- If your environment includes NAS devices from more than one provider, you should create separate backup definitions for each provider. The options for some providers are incompatible with other providers, which may cause problems with your backup jobs.

See [“Backing up data”](#) on page 163.

See [“Backup options for NDMP”](#) on page 1064.

## Backup options for NDMP

When you create a backup job for NDMP, you can set any of the following options that are appropriate for the job and the NDMP provider.

See [“About backing up NDMP resources”](#) on page 1063.

The following backup options are available for NetApp, IBM, and Fujitsu:

**Table N-1** NDMP backup options for NetApp/IBM/Fujitsu

Item	Description
<b>Back up Access Control Lists</b>	Backs up NetApp Access Control Lists.
<b>Enable file history</b>	Enables the generation of file history data. File history is used to optimize recovery of selected subsets of data from the backup image. File history generation and processing increase the backup time. Disabling this option improves backup time. If file history is made unavailable and you must restore data later, restore the entire backup image.
<b>Backup method</b>	Specifies the backup level. Level 0 provides a full backup. Levels 1 through 9 provide various levels of incremental backups. Level 1 backup method backs up new or modified files since the level 0 backup. Level 2 backup method backs up new or modified files since the level 1 backup, and so on.

The following backup options are available for EMC:

**Table N-2** NDMP backup options for EMC

Item	Description
<b>Backup type</b>	<p>Determines the backup type for this backup job.</p> <p>The following backup types are available:</p> <ul style="list-style-type: none"> <li>■ VBB</li> <li>■ Dump</li> </ul>
<b>Back up with integrated checkpoints (SnapSure)</b>	<p>Enables Backup Exec to create a backup set that uses the EMC SnapSure feature. For more information about SnapSure, see your EMC documentation.</p>
<b>Enable file history</b>	<p>Enables the generation of file history data. File history is used to optimize recovery of selected subsets of data from the backup image. File history generation and processing increase the backup time. Disabling this option improves backup time. If file history is made unavailable and you must restore data later, restore the entire backup image.</p>
<b>Backup method</b>	<p>Specifies the backup level. Level 0 provides a full backup. Levels 1 through 9 provide various levels of incremental backups. Level 1 backup method backs up new or modified files since the level 0 backup. Level 2 backup method backs up new or modified files since the level 1 backup, and so on.</p>

For NDMP providers other than NetApp, IBM, Fujitsu, and EMC, Backup Exec displays the appropriate environment variables for the provider. The values for most variables, such as the backup level and file history option, can be changed. Some variables can be changed to a predefined option, some variables can be changed to any value, and some variables cannot be changed at all. Symantec has tested the variables that appear for each NDMP provider. The NDMP provider may support additional variables. However, Symantec does not support them at this time. Backup Exec does not validate the values that you enter for the variables, so you should ensure that you enter the values correctly. See the documentation from your NDMP provider for information about the values that you use for the variables that appear.

## About including and excluding directories and files for NDMP backup selections

When you create a backup, you can do the following:

- Select specific directories to include in the backup job.
- Select specific directories and files to exclude from the backup job.

**Table N-3** What you can include and exclude for NDMP backup selections

Type of NDMP backup selection	Include	Exclude
NetApp/IBM/Fujitsu	Single or multiple directories	Directories and files
EMC	Single directory	Directories and files (only if you select the "dump" backup type)
Other	Single or multiple directories, depending on the NDMP provider.	Directories and files

When you create a backup, you can select the NDMP resources that you want to include from either the main resource selection area or from the **Include/Exclude** dialog box.

The following limitations apply when you select NDMP resources from the main resource selection area instead of from the **Include/Exclude** dialog box:

- You can include entire volumes for any NDMP provider.
- You can include subfolders for NetApp/IBM/Fujitsu providers only.
- You cannot exclude files or directories. You must use the **Include/Exclude** dialog box to exclude NDMP resources from a backup job.

See [“How to use patterns to exclude files and directories from an NDMP backup selection”](#) on page 1066.

## How to use patterns to exclude files and directories from an NDMP backup selection

When you exclude files and directories from a backup selection for an EMC Celerra Server or a NetApp/IBM/Fujitsu appliance, you must use patterns. You should enter patterns carefully to ensure that you exclude the correct files and directories.

## How to use patterns to exclude files and directories from an NDMP backup selection

Backup Exec does not verify the validity of exclude patterns. If you enter an invalid pattern, the pattern is ignored and therefore the files or directories are not excluded.

For details about how to use patterns, see your NDMP vendor's documentation.

The following example shows a pattern to exclude files and directories from a backup selection for a NetApp/IBM/Fujitsu appliance:

**Table N-4** Example pattern for NetApp/IBM/Fujitsu appliances

Pattern	Example
tmp	Excludes all files and directories that have the name "tmp".
*.core	Excludes all files and directories that end with ".core".

To exclude directories for an EMC Celerra Server, do not include the name of the EMC Celerra Server or the name of the file system in the pattern. The names of the NDMP server and the file system are already included in the **Resource name** text box. If you repeat the name of the NDMP server and the file system in the pattern, the EMC Celerra Server ignores the exclusion. Type the path from the root directory to the directory that you want to exclude. Do not include an initial forward slash (/).

The following example shows a pattern to exclude directories from a backup selection for an EMC Celerra Server:

**Table N-5** Example pattern to exclude directories for an EMC Celerra Server

Pattern	Description
test_exclusion/subdir1	Excludes only the "subdir1" directory on the file system that is listed in the <b>Resource name</b> text box.
test_exclusion/d*	Excludes all directories that start with the letter "d" under the directory "/test_exclusion"

The following example shows a pattern to exclude files from a backup selection for an EMC Celerra Server:

**Table N-6** Example pattern to exclude files for an EMC Celerra Server

Pattern	Description
*.mp3	Excludes all files that end with “.mp3”.
temp	Excludes all files that have the name “temp”.

See [“About including and excluding directories and files for NDMP backup selections”](#) on page 1066.

## How to duplicate backed up NDMP data

You can create a job to duplicate backup data. When you create a duplicate job, you can select a device that is attached to a Backup Exec server or to a NAS sever. You can use tape devices, backup-to-disk devices, or virtual tape libraries.

Backup Exec supports the following configurations:

- Two tape devices that are attached locally to the Backup Exec server.
- Two tape devices that are attached locally to a NAS server.
- One tape device that is attached locally to a NAS server and one tape device that is attached locally to another NAS server.
- One tape device that is attached locally to a Backup Exec server and one tape device that is attached locally to a NAS server.

The procedure to duplicate NDMP data is the same as the procedure to duplicate any other type of data. However, for NetApp/IBM/Fujitsu, you must select the logon credential for the source NDMP server.

See [“Duplicating backup sets”](#) on page 219.

---

**Note:** If the data that you want to duplicate is hardware-encrypted, you should choose a destination device that allows hardware encryption. Otherwise, the duplicate job fails.

---

## About restoring NDMP data

To restore NDMP data, use the Restore Wizard on the **Backup and Restore** tab. During the restore process, you can select individual files for restore if file history was enabled for the backup job.

Backup Exec cannot gather sufficient file and directory information on an NDMP restore job to accurately populate the **Backup Set Summary** and **Backup Set**

**Information** sections of the job history. Therefore, the number of files, directories, files skipped, corrupt files, and files in use always appears as 0.

NDMP backup sets cannot be cataloged unless the following option is selected as a catalog default:

**Use storage-based catalogs**

See [“Editing global options for catalogs”](#) on page 242.

---

**Note:** You cannot exclude files and directories from restore jobs on NDMP servers. Excluded directories and files are restored.

---

## NDMP restore options

When you create a restore job for NDMP, the options that appear in the Restore Wizard vary depending on the type of NDMP server that is being used.

See [“About restoring NDMP data”](#) on page 1068.

**Table N-7** NDMP restore options for NetApp/IBM/Fujitsu

Item	Description
<b>Restore Access Control Lists</b>	Restores NetApp Access Control Lists.
<b>Enable Direct Access Recovery</b>	Enables Backup Exec to use Direct Access Recovery (DAR) during the restore job. With DAR-enabled recovery, Backup Exec can specify the exact location of a file in a backup data stream. The NDMP server can then read the data applicable to the single file being restored. This practice reduces the amount of information that is processed and significantly reduces recovery time. If DAR is not available, the restore may take significantly longer.
<b>Restore without writing data to disk (Verify data without doing a restore)</b>	Tests the validity of the data that you selected for the restore job. Backup Exec does not restore the data. For NetApp/IBM filers, you should use this option to verify data instead of Backup Exec's verify backup job option.

**Table N-7** NDMP restore options for NetApp/IBM/Fujitsu (*continued*)

Item	Description
<b>Recreate the directory structure from the backup when the data is restored; otherwise, all data is restored without any directory structure</b>	Restores the data with its original directory structure intact.

**Table N-8** NDMP restore options for EMC

Item	Description
<b>Enable Direct Access Recovery</b>	Enables Backup Exec to use Direct Access Recovery (DAR) during the restore job. With DAR-enabled recovery, Backup Exec can specify the exact location of a file in a backup data stream. The NDMP server can then read the data applicable to the single file being restored,. This practice reduces the amount of information that is processed and significantly reduces recovery time. If DAR is not available, the restore may take significantly longer.
<b>Recreate the directory structure from the backup when the data is restored; otherwise, all data is restored without any directory structure</b>	Restores the data with its original directory structure intact.
<b>Restore over existing files</b>	Overwrites files on the target resource that have the same name as files that are being restored. Use this option only when you are sure that you want to restore an older version of a file.

For NDMP providers other than NetApp, IBM, Fujitsu, and EMC, Backup Exec displays the appropriate variables for the NDMP provider that is being used and sets the values for the variables by default. However, you can change the values to meet your needs. Variables that begin with the prefix "@@" are specific to Backup Exec rather than to a specific NDMP vendor. Symantec has tested the variables that appear for each NDMP provider. The NDMP provider may support additional variables. However, Symantec does not support them at this time. Backup Exec does not validate the values for the variables that you enter, so you should ensure that you enter the values correctly. See the documentation from your NDMP provider for information about the values that you use for the variables.

## About redirecting restored NDMP data

You can redirect NDMP data from one NDMP server to another NDMP server.

When you redirect NDMP data, be aware of the following limitations:

- You cannot redirect NDMP data to a computer that runs the Windows or Linux operating systems.
- You cannot redirect non-NDMP data, such as NTFS or SQL data, to an NDMP server.
- The server to which you want to redirect the restored data must be from the same vendor as the server from which the data was backed up.

See [“About searching for and restoring data”](#) on page 229.

## Setting the default options for NDMP

You can use the defaults that Backup Exec sets during installation for all NDMP backup jobs, or you can choose your own defaults. You can also change the defaults for any specific backup job.

### To set default options for NDMP

- 1 Click the Backup Exec button, and then select **Configuration and Settings**.
- 2 Select **Backup Job Defaults**, and then select a backup option.
- 3 In the left pane, select **NDMP**.
- 4 Select the appropriate options.  
See [“Backup options for NDMP”](#) on page 1064.
- 5 Click **OK**.

## Viewing the properties of an NDMP server

Follow these steps to view the properties of an NDMP server.

### To view the properties of an NDMP server

- 1 On the **Storage** tab, double-click the NDMP server.
- 2 In the left pane, select **Properties**.  
See [“NDMP server properties”](#) on page 1072.

## NDMP server properties

You can view the following properties for an NDMP server.

See “[Viewing the properties of an NDMP server](#)” on page 1071.

**Table N-9** NDMP server properties

Item	Description
<b>Server name</b>	Indicates the name of the NDMP server.
<b>Description</b>	Shows the user-defined description of the server.
<b>State</b>	
<b>Port</b>	Lists the port that is used for communications between the Backup Exec server and the NDMP server.
<b>Use ICMP ping operations to detect the server</b>	Indicates whether ICMP ping is enabled. ICMP ping enables Backup Exec to use ping to locate the NDMP server.
<b>Logon account</b>	Indicates the name of the logon account for the NDMP server. You can add a new logon account or edit an existing account.
<b>Host ID</b>	Displays the identifier number that the NDMP server generates.
<b>System version</b>	Indicates the software version that is installed on the NDMP server.

# Symantec Backup Exec Agent for Linux

This appendix includes the following topics:

- [About the Agent for Linux](#)
- [About open files and the Agent for Linux](#)
- [Requirements for the Agent for Linux](#)
- [About installing the Agent for Linux](#)
- [About establishing trust for a remote Linux computer in the Backup Exec list of servers](#)
- [Adding additional Backup Exec servers to which the Agent for Linux can publish information](#)
- [About configuring the Agent for Linux](#)
- [About excluding files and directories from backup jobs for Linux computers](#)
- [Editing configuration options for Linux computers](#)
- [About backing up a Linux computer by using the Agent for Linux](#)
- [About restoring data to Linux computers](#)
- [Edit the default backup job options for Linux computers](#)
- [Uninstalling the Agent for Linux](#)
- [Starting the Agent for Linux daemon](#)
- [Stopping the Agent for Linux daemon](#)

- [Troubleshooting the Agent for Linux](#)

## About the Agent for Linux

The Backup Exec Agent for Linux (Linux Agent) is installed as a separate add-on component. The Linux Agent enables network administrators to perform backup and restore operations on Linux servers that are connected to the network. The Linux Agent must be installed on the Linux servers before you can perform backup or restore operations.

See [“About open files and the Agent for Linux”](#) on page 1074.

See [“Requirements for the Agent for Linux”](#) on page 1074.

See [“About installing the Agent for Linux”](#) on page 1075.

## About open files and the Agent for Linux

The Agent for Linux uses advanced open file and image technologies that are designed to alleviate issues that are sometimes encountered during backup operations, such as backing up open files.

After you make file and folder selections and the job is submitted for backup, the Linux Agent automatically makes a snapshot of the volume or volumes. Making snapshot of a volume provides a point-in-time record of the data. When it creates a snapshot, the Linux Agent uses snapshot technologies to momentarily suspend write activity to a volume so that a snapshot of the volume can be created. During the backup, files can be open and data can be changed.

The Linux Agent supports Simple, Logical Volume Manager (LVM), and RAID volume configurations.

See [“Requirements for the Agent for Linux”](#) on page 1074.

## Requirements for the Agent for Linux

The following items are required to install the Agent for Linux (Linux Agent):

- The Backup Exec server must have TCP/IP installed.
- You must have a root logon account on the Linux servers.
- You must have the Backup Exec installation media.
- You must enter a license for the Linux Agent on the Backup Exec server.

---

**Note:** Some versions of Linux may require that you install the `libstdc++.so.5` package.

---

See “[Troubleshooting the Agent for Linux](#)” on page 1104.

Symantec recommends that you use the Secure Shell (SSH) protocol when you push-install the Linux Agent from one Linux server to another Linux server. You must enable SSH before you push-install the Linux Agent.

Backup Exec automatically installs the Remote Media Agent for Linux when it installs the Agent for Linux on a Linux server. However, you must enter a separate license for the Remote Media Agent for Linux before it is available for use.

See “[About the Remote Media Agent for Linux](#)” on page 1132.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

See “[About installing the Agent for Linux](#)” on page 1075.

See “[Requirements for backing up Novell Open Enterprise Server on SUSE Linux Enterprise Server](#)” on page 1094.

## About installing the Agent for Linux

Use the Backup Exec installation media to do the following:

- Install the Agent for Linux (Linux Agent) on a local Linux server.
- Push-install the Linux Agent from one Linux server to other remote Linux servers.
  - If you push-install the Linux Agent, the RSH (Remote Shell) is used by default. Symantec recommends that you use SSH (Secure Shell) instead. To use SSH, you must enable it before you install the Linux Agent. Refer to your operating system documentation for more information about SSH.

When you install the Linux Agent, Backup Exec creates the `beoper` group and adds `root` as a member. The `beoper` group contains the names of the users who have permission to back up and restore the Linux servers. However, if Backup Exec detects an NIS server during the Linux Agent installation, then the `beoper` group is not created. You must create the `beoper` group manually on the Linux servers on which you want to install the Linux Agent.

When the installation is complete, Backup Exec saves the install log file to the following location on the server on which the Linux Agent is installed:

`/var/tmp/vxif/installralus<summary file number>/installralus.log`

See [“Installing the Agent for Linux”](#) on page 1076.

See [“Troubleshooting the Agent for Mac”](#) on page 1128.

## Installing the Agent for Linux

You can install the Agent for Linux (Linux Agent) on a local Linux server. You can then push-install the Linux Agent from the local Linux server to one or more remote Linux servers.

---

**Note:** You must unzip the `RALUS_RMALS_RAM_<version number>.gz` file on a Linux server. The installation does not run if it is unzipped on a computer that runs the Windows operating system.

---

See [“About installing the Agent for Linux”](#) on page 1075.

### To install the Agent for Linux

- 1 At a Linux server, place the Backup Exec installation media in the appropriate drive.
- 2 Log on as root on the server on which you want to install the Linux Agent.
- 3 Navigate to the following directory on the installation media.  
<LinuxUnixMac>
- 4 Copy the `RALUS_RMALS_RAM_<version number>.gz` file in this directory to a directory on the local computer.

- 5 Unzip the file.

For example:

```
gunzip RALUS_RMALS_RAM_<version number>.gz
```

- 6 Untar the file.

For example:

```
tar -xf RALUS_RMALS_RAM_<version number>.tar
```

- 7 Do one of the following:

To install the Linux Agent on the local Linux server

Start the `installralus` script.

For example: `./installralus`

To install the Linux Agent from the local Linux server to one remote Linux server

Do the following in the order listed:

- Start the **installralus** script using the -SSH switch.  
For example: `./installralus -usessh`
- Type the name, IP address, or fully qualified domain name of a Linux server.

To install the Linux Agent from the local Linux server to multiple remote Linux servers

Do the following in the order listed:

- Start the **installralus** script using the -SSH switch.  
For example: `./installralus -usessh`
- Type the names, IP addresses, or fully qualified domain names of the Linux servers. Leave a space between each identifier.

- 8 After the installer checks for a valid Linux operating system during the initial system check, press **Enter**.
- 9 Review the package installation summary, and then press **Enter**.
- 10 After the system installation requirements check completes, press **Enter**.
- 11 Start the prerequisites check by pressing **Enter**.
- 12 Type the name, IP address, or fully qualified domain name of the Backup Exec server (directory host) that you want to back up the Linux Agent.
- 13 Type any additional names, IP addresses, or fully qualified domain names of Backup Exec servers that you want to back up this Linux Agent.
- 14 Do one of the following:
  - If the name, IP address, or fully qualified domain name is correct Press **Enter** to continue the installation.
  - If you want to change the name, IP address, or fully qualified domain name Type **N**, press **Enter**, and then change the information.
- 15 Start the NIS server scan by pressing **Enter**.
- 16 Examine the results of the NIS server scan, and then do one of the following:

If an NIS server is detected

The Linux Agent installer cannot create the beoper group. You must create it manually after the Linux Agent installation is complete.

Continue with the next step.

If an NIS server is not detected

Use the installer to create the beoper group.

Do the following in the order listed:

- To let the installer create the beoper group, type **y**.
- To select the next available Group ID, type **n**.
- To add the root user account to the beoper group, type **y**.
- Continue with the next step.

**17** Start the installation by pressing **Enter**.

**18** After installation completes, press **Enter** to start the post-installation configurations and installation of SymSnap drivers.

**19** Press **Y** to automatically start the Beremote service; otherwise, press **N** to start the service later.

**20** After the configuration process completes, press **Enter** to save the installation log to the following file:

*/var/tmp/vxif/installralussummary file number/installralus.log*

**21** If the Linux Agent installer did not create a beoper group, you must create it.

See [“Creating the Backup Exec operators group manually”](#) on page 1079.

**22** Start the Agent for Linux daemon.

See [“Starting the Agent for Linux daemon”](#) on page 1103.

**23** Configure the Agent for Linux as appropriate.

See [“About configuring the Agent for Linux”](#) on page 1081.

## About the Backup Exec operators group for the Agent for Linux

The Backup Exec operators (**beoper**) group contains the names of the users who have permission to back up and restore the Linux servers.

When you install the Agent for Linux (Linux Agent), Backup Exec creates the **beoper** group and adds root as a member. Any Linux user that you add to the **beoper** group gets the necessary permissions to back up and restore the servers.

However, if an NIS server is detected during the Linux Agent installation, Backup Exec cannot create the **beoper** group. You must create the **beoper** group manually on the Linux servers on which you want to install the Linux Agent. You must create the **beoper** group before you start backup and restore operations. Otherwise, connections fail between the Linux servers and the Backup Exec server.

Before the members of the **beoper** group can perform backup or restore operations, they must have a Backup Exec logon account.

See [“Creating the Backup Exec operators group manually”](#) on page 1079.

See [“Creating a Backup Exec logon account”](#) on page 500.

## Creating the Backup Exec operators group manually

You must create a beoper group on each server on which you want to install the Agent for Linux (Linux Agent).

See [“About the Backup Exec operators group for the Agent for Linux”](#) on page 1078.

---

**Note:** Ensure that you understand how to set security for groups on Linux servers before you assign a Group ID for the beoper group.

---

**Table O-1** How to manually create the beoper group

Step	Action	More Information
Step 1	Navigate to the Linux server on which you want to install the Linux Agent.  If the Linux server is in an NIS domain, navigate to the NIS domain's group file.	Refer to the NIS documentation for information on how to add a group to an NIS domain group file.
Step 2	Create a group with the following case-sensitive name:  <b>beoper</b>	See the operating system's documentation for more information about how to create a group.
Step 3	In the beoper group, add the users that you want to have permission to back up and restore the Linux server.	See the operating system's documentation for more information about how to add users to a group.

**Table O-1** How to manually create the beoper group (*continued*)

Step	Action	More Information
Step 4	Create a Backup Exec logon account for each user that you add to the beoper group.	See <a href="#">“Creating a Backup Exec logon account”</a> on page 500.

## About establishing trust for a remote Linux computer in the Backup Exec list of servers

When you connect to a Linux computer from the Backup Exec server, you must establish trust between the Backup Exec server and the remote Linux computer. You must also establish trust if you want to configure a remote Linux computer to perform client-side deduplication.

See [“About establishing a trust between the Backup Exec server and a remote computer”](#) on page 734.

See [“Establishing trust and adding a remote Linux computer to the Backup Exec list of servers”](#) on page 1080.

## Establishing trust and adding a remote Linux computer to the Backup Exec list of servers

You can add one or more remote Linux computers to the list of servers that appear on the **Backup and Restore** tab. When you add remote Linux computers, you must establish a trust between the Backup Exec server and the remote Linux computers to ensure secure communication.

### To establish trust and add a remote Linux computer to the Backup Exec list of servers

- 1 On the **Backup and Restore** tab, in the **Servers** group, click **Add**.
- 2 Click **Linux computer**.
- 3 Follow the on-screen prompts.

See [“Adding additional Backup Exec servers to which the Agent for Linux can publish information”](#) on page 1081.

See [“About configuring the Agent for Linux”](#) on page 1081.

# Adding additional Backup Exec servers to which the Agent for Linux can publish information

You can specify additional Backup Exec servers to which the Agent for Linux (Linux Agent) can publish information.

Each Backup Exec server to which the Linux Agent publishes information appears in the Backup Exec **Servers** list.

**To add additional Backup Exec servers to which the Agent for Linux can publish information**

- 1 Use a text editor to open the following file:  
`/etc/VRTSralus/ralus.cfg`
- 2 Add the following string:  
`Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List unique identifier number = IP address or DNS name of Backup Exec server`
- 3 Save and close the file.
- 4 Move to the Backup Exec server to which the Linux Agent is publishing itself and add the Linux server to the **Servers** list.

See [“Adding servers to the list of servers”](#) on page 158.

## About configuring the Agent for Linux

Backup Exec creates a file named `ralus.cfg` on each Linux server on which the Agent for Linux (Linux Agent) is installed. You can edit the strings, identifiers, and variables in this file to add or edit options for the Linux Agent.

Options that you can edit in the `ralus.cfg` file include the following:

- The port to which the Linux Agent must send publishing messages.
- The logging level for Oracle database operations that use the Backup Exec Linux Agent Utility, and for NDMP information.
- The settings to allow the Linux Agent to publish to one or more Backup Exec servers.
- The files and directories on Linux servers that you want to exclude from backups.
- The setting for a Target Service Agent File System backup for Novell OES.

The ralus.cfg format contains three components. The first component (A) in the following example is a required string.

The second component (B) is a unique identifier followed by an equal sign (=). A unique identifier can consist of sequential numbers, letters, or alpha-numeric characters. For example, 1, 2, 3 or A, B, C. You can also use AA, BB, CC, or A1, A2, B1, B2.

The third component of the ralus.cfg format is the NetBIOS name, fully qualified domain name, or IP address of the Backup Exec server.

The ralus.cfg includes a registry key that works with the Linux Agent's open file technology. The name of the key is DisableOFO and appears in the ralus.cfg file in the following form:

```
Software\Symantec\Backup Exec for Windows\Backup  
Exec\Engine\RALUS\DisableOFO=0
```

By default, the DisableOFO key is set to 0, meaning that the Linux Agent is active, letting the Linux Agent back up the open files that it encounters. However, you can disable the open file technology by changing the value of the key to "1", and then restarting the Linux Agent daemon.

**Figure O-1** Example of the ralus.cfg file

```
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 1=svr.mycompany.com  
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 2=datasrv  
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 3=66.35.250.151
```

The diagram shows three lines of text from the ralus.cfg file. Brackets above the lines indicate the components: 'A' covers the first line, 'B' covers the second line, and 'C' covers the third line.

- A = Required string
- B = Required and unique identifier (the order or appearance is irrelevant)
- C = File or directory to be excluded

See [“Editing configuration options for Linux computers”](#) on page 1083.

See [“Configuration options for Linux computers”](#) on page 1083.

See [“Stopping the Agent for Linux daemon”](#) on page 1103.

See [“Starting the Agent for Linux daemon”](#) on page 1103.

## About excluding files and directories from backup jobs for Linux computers

You can exclude specific files and directories on the Linux computers from all backup jobs. Edit the ralus.cfg file to specify the excluded files.

The following is an example of strings in the ralus.cfg file that excludes files and directories from all backup jobs.

**Figure O-2** Example of file and directory exclusions in the ralus.cfg format

	A	B	C
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude1=	dev/*.*		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude2=	proc/*.*		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude3=	mnt/nss/pools/		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude4=	mnt/nss/.pools/		

A = Required string

B = Required and unique identifier (the order or appearance is irrelevant)

C = File or directory to be excluded

To exclude files and directories for specific backup jobs, specify the exclusions in the backup job properties.

See [“Editing configuration options for Linux computers”](#) on page 1083.

## Editing configuration options for Linux computers

You can edit configuration options for the Agent for Linux.

See [“About configuring the Agent for Linux”](#) on page 1081.

### To edit configuration options for Linux computers

- 1 Use a text editor to open the following file:

/etc/VRTSralus/ralus.cfg

- 2 Change the appropriate string in the file.

See [“Configuration options for Linux computers”](#) on page 1083.

## Configuration options for Linux computers

You can edit options to configure the Agent for Linux (Linux Agent).

See [“Editing configuration options for Linux computers”](#) on page 1083.

**Table O-2** Configuration options for Linux computers

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agent Browser\TcpIp\AdvertisementPort=6101	Lists the port to which the Linux Agent must send publish and purge messages.

**Table O-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Debug\AgentConfig=0	Enables logging for the Linux Agent utility that Oracle operations use. Values include the following: <ul style="list-style-type: none"> <li>■ 0 Logging is not enabled.</li> <li>■ 1 Logging is enabled. Backup Exec automatically generates the log file.</li> </ul> This option does not apply to the Agent for Mac.
Software\Symantec\Backup Exec for Windows\Backup Exec\Debug\VXBSAlevel=0	Enables logging for the Linux Agent for Oracle operations. Values include the following: <ul style="list-style-type: none"> <li>■ 0 Logging is not enabled.</li> <li>■ 5 Normal logging is enabled.</li> <li>■ 6 Advanced logging is enabled. Large log files may be created.</li> </ul> This option does not apply to the Agent for Mac.

**Table 0-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Agents\Advertise All=1	<p>Enables the Linux Agent to publish information to all of the Backup Exec servers that are listed in the \Agents\Agent Directory List strings.</p> <p>Values include the following:</p> <ul style="list-style-type: none"><li>■ 1 The Linux Agent publishes information to every Backup Exec server in the Agent Directory List.</li><li>■ 0 The Linux Agent publishes information to the first Backup Exec server in the Agent Directory List. If the attempt is successful, the Linux Agent does not publish information to any other Backup Exec servers. If the attempt is not successful, the Linux Agent attempts to publish information to the next Backup Exec server in the list. Attempts continue until the Linux Agent reaches the end of the list.</li></ul>

**Table O-2** Configuration options for Linux computers (*continued*)

String and default values	Description
<p>Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertise Now=0</p>	<p>Enables the Linux Agent to start a new publishing cycle after you add or edit any settings in the ralus.cfg file.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 The Linux Agent publishes information according to its regular cycle, set in the string \Agents\Advertising Interval Minutes. Any changes to the ralus.cfg file take effect when a new publishing cycle begins.</li> <li>■ 1 The Linux Agent starts a new publishing cycle. Any changes to the ralus.cfg file take effect immediately.</li> </ul> <p>If the Backup Exec server does not receive the publishing information, the Linux Agent makes ten more attempts. Each attempt to publish information to the Backup Exec server is one minute apart. If the information is not sent at the end of the ten attempts, the Linux Agent skips that Backup Exec server until the next publishing cycle. The publishing cycle is the number of minutes set in the string \Agents\Advertising Interval Minutes.</p>

**Table 0-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertisement Purge=0	<p>Lets the Linux Agent send a purge message to all of the Backup Exec servers in the string \Agents\Advertisement Purge. When a Backup Exec server receives a purge message, it removes the Linux Agent from Backup Exec's list of available servers. The Linux Agent continues to function.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 Do not purge the Linux Agent from any Backup Exec servers that are listed in the \Agents\Advertisement Purge string.</li> <li>■ 1 Purge the Linux Agent from one or more Backup Exec servers in the \Agents\Advertisement Purge string.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertising Disabled=0	<p>Enables the Linux Agent to publish to Backup Exec servers.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 The Linux Agent attempts to publish information to the Backup Exec servers that are listed in the string \Agents\Agent Directory List.</li> <li>■ 1 The Linux Agent does not publish information to Backup Exec servers.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertising Interval Minutes=240	<p>Sets the number of minutes that the Linux Agent must wait between publishing cycles. The default number of minutes is 240. The range of minutes is from 1 minute to 720 minutes.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Agent Directory List 1=<Backup Exec server name>	<p>Displays the list of NetBIOS names, fully qualified domain names, or IP addresses to which the Linux Agent publishes information.</p> <p>The Backup Exec server from which the Linux Agent is push installed is added to the Agent Directory List by default.</p>

**Table O-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Auto Discovery Enabled=1	<p>Adds a Backup Exec server to the string \Agents\Agent Directory List if the Backup Exec server performs a backup job with which the Linux Agent is associated.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 1 Adds the Backup Exec server that performs the backup job to the Agent Directory List. The Linux Agent can publish information to the Backup Exec server.</li> <li>■ 0 The Backup Exec server that performs the backup job is not added to the Agent Directory List.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Logging\RANT NDMP Debug Level=0	<p>Displays the level of verbosity for logging NDMP information for the Linux Agent.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 Logs only the NDMP errors.</li> <li>■ 1 Logs the NDMP errors and warnings.</li> <li>■ 2 Logs the NDMP errors, warnings, and message information that is sent between the remote computer and the Backup Exec server.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\Encoder=	<p>Displays the encoder that you can add if the default encoder incorrectly displays characters on the user interface.</p>

**Table O-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\ShowTSAFS=	<p>Lets you perform a Target Service Agent file system (TSAFS) backup for applications on Novell Open Enterprise Services. By default, this option is not enabled.</p> <p>The Linux Agent backs up all file systems using the Root object. If ShowTSAFS is enabled, the Novell Open Enterprise Services resource appears in the backup selection list. If you select the whole computer for backup, then redundant backups are performed. Symantec recommends that you do not enable this option.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ Blank or 0 The file system TSA does not appear for backup selection.</li> <li>■ 1 The file system TSA resource appears for backup selection.</li> </ul> <p>This option does not apply to the Agent for Mac.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemExclude1=	<p>Lists the files that you want to exclude from all Linux Agent backup jobs.</p> <p>See <a href="#">“About excluding files and directories from backup jobs for Linux computers”</a> on page 1082.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemFSTypeExclude1	<p>Lists the type of file system that you want to exclude from the Linux Agent backup.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\ Engine\RALUS\vfmpath= /opt/VRTSralus/VRTSvxms	<p>Displays the path to the Veritas Mapping Service libraries that the Linux Agent uses.</p>

**Table O-2** Configuration options for Linux computers (*continued*)

String and default values	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RMAL\DisableRMAL=0	<p>Lets you use the Remote Media Agent for Linux to back up the Linux server on which it is installed. By default, this option is not enabled.</p> <p>If you install RMAL to an unsupported version of Linux, RMAL is unavailable for use. You cannot create the jobs that run on the devices that are attached to the Linux server. However, you can back up the Linux server by using the Agent for Linux component. This component is installed with RMAL. You must change the value of this string to 1 to use the Agent for Linux component.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 You can create backup, restore, and utility jobs on the Backup Exec server that run on the Linux server's storage devices.</li> <li>■ 1 You can only use the Agent for Linux component to back up the Linux server on which it is installed.</li> </ul> <p>See <a href="#">“Troubleshooting the Agent for Linux”</a> on page 1104.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\DisableOFO=0	<p>Lets you disable or enable the Linux Agent's open file technology.</p> <p>By default, the DisableOFO key is set to 0, meaning that the Linux Agent is active, letting the Linux Agent back up the open files that it encounters. However, you can disable the open file technology by changing the default value of the key to 1 and then restarting the Linux Agent daemon.</p>

## About backing up a Linux computer by using the Agent for Linux

The following backup methods appear when you use the Agent for Linux (Linux Agent) to back up data:

- Full - Using modified time
- Differential - Using modified time
- Incremental - Using modified time

However, when you select a backup job method for the Agent for Linux, only full backups are supported. If you select any other backup method, a full backup runs instead.

See [“Linux backup options”](#) on page 1091.

See [“About stages”](#) on page 183.

See [“Editing a stage”](#) on page 184.

See [“About backing up Novell Open Enterprise Server \(OES\) components ”](#) on page 1093.

## Linux backup options

The following Agent for Linux (Linux Agent) options are available when you back up Linux computers.

See [“About backing up a Linux computer by using the Agent for Linux”](#) on page 1090.

**Table O-3** Backup job options for Linux computers

Item	Description
<b>Preserve file and directory timestamps during backups</b>	<p>Prevents the Linux Agent from changing an object's attributes when a backup occurs. An object is a file or a directory.</p> <p>This option is not selected by default.</p> <p>During a backup, Backup Exec preserves an object's last access timestamp by resetting the last access timestamp to the value before the backup occurred. When Backup Exec modifies the object's last access timestamp, the operating system internally updates the object's ctime.</p> <p>An object's ctime is the time when an object's attributes such as permissions and timestamps are modified. If the Linux Agent does not change the attributes after a backup, the object's ctime is not changed.</p> <p>This option does not affect the object attributes that are set during restore operations.</p>
<b>Follow local mount points</b>	<p>Lets Backup Exec follow local mount points when it backs up data.</p> <p>This option is enabled by default.</p> <p>For more information on local mount points, see your operating system's documentation.</p>

**Table O-3** Backup job options for Linux computers (*continued*)

Item	Description
<b>Follow remote mount points</b>	<p>Lets Backup Exec follow remote mount points when it backs up data.</p> <p>This option is not selected by default.</p> <p>When you use this option, the following limitations apply:</p> <ul style="list-style-type: none"><li>■ The data that is mounted must reside on a computer type that Backup Exec supports. You can find a list of supported operating systems, platforms, and applications at the following URL: <a href="http://entsupport.symantec.com/umi/V-269-1">http://entsupport.symantec.com/umi/V-269-1</a></li><li>■ If the mount point leads to an operating system that Backup Exec does not support, contact the operating system's vendor to resolve any issues.</li></ul> <p>For more information on remote mount points, see your operating system's documentation.</p>
<b>Lock remote files to prevent applications from modifying them during backups</b>	<p>Lets the Linux Agent have exclusive access to the files on the remote servers that are connected through Network File System (NFS). Locking remote files prevents other applications from modifying the data during the backup.</p>
<b>Backup method for eDirectory</b>	<p>Deletes a backup method for backing up eDirectory data for Novell OES on SUSE Linux Enterprise Server.</p> <p><b>Note:</b> This option is not supported for Macintosh computers.</p> <p>See "<a href="#">About restoring Novell OES components</a>" on page 1095.</p>

## About backing up Novell Open Enterprise Server (OES) components

Before you can back up Novell OES components, the Agent for Linux must be installed on the server where the Novell OES components reside.

Backup Exec supports the following Novell Open Enterprise Server (OES) components:

- Novell iFolder
- Novell eDirectory
- Novell Group Wise
- Novell Storage Services (NSS)

See [“Requirements for backing up Novell Open Enterprise Server on SUSE Linux Enterprise Server”](#) on page 1094.

## Requirements for backing up Novell Open Enterprise Server on SUSE Linux Enterprise Server

Backup Exec requires the following to back up Novell OES:

- Novell OES must have Service Pack 1 installed.
- Novell OES 2 must have the Target Service Agent for NDS (TSANDS) loaded. The TSANDS protects eDirectory on Novell Open Enterprise Server 2. By default, TSANDS is not loaded on Novell Open Enterprise Server 2. You must manually load TSANDS before eDirectory can appear as a resource that is available for backup. See your Novell documentation for information about how to load TSANDS.
- The Target Service Agents must be enabled for the following:
  - Novell eDirectory
  - Novell iFolder
  - Novell Group Wise
- A local UNIX user name that is the equivalent of the admin-level eDirectory user in the beoper group. Backup Exec does not support eDirectory users. See [“About the Backup Exec operators group for the Agent for Linux”](#) on page 1078.
- A Backup Exec logon account that contains the credentials for the equivalent admin-level eDirectory user must exist before you can perform backup jobs for eDirectory.

See [“Backing up data”](#) on page 163.

See [“About backing up a Linux computer by using the Agent for Linux”](#) on page 1090.

# About restoring data to Linux computers

You can specify restore job options to restore Linux computers.

---

**Note:** You cannot perform a cross-platform restore of HP/UX file system backups for which compression or encryption is enabled. You must restore these backups to their respective platforms.

---

See [“About searching for and restoring data”](#) on page 229.

See [“Restore job options for Linux computers”](#) on page 1095.

## About restoring Novell OES components

When Backup Exec restores Novell OES components, it restores the entire Novell NDS database to a set of on-disk DIB files. Then, the NDS database is taken offline. The DIB files are renamed to NDS, which overwrites the offline NDS database.

See [“About searching for and restoring data”](#) on page 229.

## Restore job options for Linux computers

The following are restore job options for Linux computers.

See [“About restoring data to Linux computers”](#) on page 1095.

**Table O-4** Restore job options for Linux computers

Item	Description
<b>Lock remote files if the mount points have necessary permissions</b>	Lets Backup Exec have exclusive access to the files on the remote computers that are connected through the Network File System (NFS).  This option is enabled by default.
<b>Restore DIB set</b>	Restores the Directory Information Base (DIB), also known as the Novell directory services (NDS) database.

**Table O-4** Restore job options for Linux computers (*continued*)

Item	Description
<b>Activate DIB after verify</b>	<p>Lets Backup Exec rename the database from .RST to .NDS after the verification process completes successfully. If the verify operation fails, the .RST file is deleted and the original .NDS file is kept intact.</p> <p>If you do not select this option, after the database is restored, the .RST file is available for you to perform manual activation or manual disaster recovery.</p>
<b>Open database when finished</b>	<p>Lets Backup Exec open the database after the restore completes.</p> <p>If you want to perform maintenance tasks before the database opens, do not select this option.</p>
<b>Verify database after restore</b>	<p>Lets Backup Exec verify the database after the restore completes.</p>
<b>Roll forward log directory</b>	<p>Displays the location of the roll forward log directory.</p>
<b>Leave backup file on disk</b>	<p>Keeps the Novell DIB fileset on the hard drive.</p> <p>See “<a href="#">About restoring Novell OES components</a>” on page 1095.</p>

## Edit the default backup job options for Linux computers

You can edit the existing default options for all backup and restore jobs for Linux systems.

### To edit default backup job options for Linux systems

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Job Defaults**.
- 2 Select either **Back Up to Disk** or **Back Up to Tape**, and then select **Linux and Macintosh**.
- 3 Set the appropriate options.  
See “[Default backup job options for Linux computers](#)” on page 1097.
- 4 Click **OK**.

## Default backup job options for Linux computers

You can set default backup job properties for all jobs on Linux computers.

See “[Edit the default backup job options for Linux computers](#)” on page 1096.

You can find a list of supported operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

**Table O-5** Default backup job options for Linux computers

Item	Description
<p><b>Preserve file and directory timestamps during backups</b></p>	<p>Prevents the Linux Agent from changing an object's attributes when a backup occurs. An object is a file or a directory.</p> <p>This option is not selected by default.</p> <p>During a backup, Backup Exec preserves an object's last access timestamp by resetting the last access timestamp to the value before the backup occurred. When Backup Exec modifies the object's last access timestamp, the operating system internally updates the object's ctime.</p> <p>An object's ctime is the time when an object's attributes such as permissions, timestamps, etc., have been modified. If the Linux Agent does not change the attributes after a backup, the object's ctime is not changed.</p> <p>This option does not affect the object attributes that are set during restore operations.</p>
<p><b>Follow local mount points</b></p>	<p>Lets Backup Exec follow local mount points when it backs up data.</p> <p>This option is enabled by default.</p> <p>For more information on local mount points, see your operating system's documentation.</p>

**Table 0-5** Default backup job options for Linux computers (*continued*)

Item	Description
<b>Follow remote mount points</b>	<p>Lets Backup Exec follow remote mount points when it backs up data.</p> <p>This option is not selected by default.</p> <p>When you use this option, the following limitations apply:</p> <ul style="list-style-type: none"><li>■ The data that is mounted must reside on an operating system that Backup Exec supports.</li><li>■ If the mount point leads to an operating system that Backup Exec does not support, contact the operating system's vendor to resolve any issues.</li></ul> <p>For more information on remote mount points, see your operating system's documentation.</p>
<b>Backup method for eDirectory</b>	<p>Displays a backup method for backing up eDirectory data for Novell OES on SUSE Linux Enterprise Server.</p> <p><b>Note:</b> This option is not supported for Macintosh computers.</p> <p>See <a href="#">“About backing up Novell Open Enterprise Server (OES) components”</a> on page 1093.</p>
<b>Lock remote files to prevent applications from modifying them during backups</b>	<p>Lets the Linux Agent have exclusive access to the files on the remote servers that are connected through Network File System (NFS). Locking remote files prevents other applications from modifying the data during the backup or restore job.</p>

# Uninstalling the Agent for Linux

An automated uninstall process for the Agent for Linux (Linux Agent) is available on the Backup Exec installation media.

`/opt/VRTS/install/logs/uninstallralus<summary file number>.summary`

## To uninstall the Agent for Linux

- 1 On the Linux server, place the Backup Exec installation media in the appropriate device.
- 2 Log on as root to the server from which you want to uninstall the Linux Agent.
- 3 Navigate to the following directory on the Backup Exec installation media:  
<LinuxUnixMac>

- 4 Start the **uninstallralus** script.

For example:

```
./uninstallralus
```

- 5 Do one of the following:

To uninstall the Linux Agent from one server

Type the name, IP address, or fully qualified domain name of a Linux server.

To uninstall the Linux Agent from multiple servers

Type the names, IP addresses, or fully qualified domain names of the Linux servers. Leave a space between each identifier.

- 6 Press **Enter**.
- 7 After the Linux Agent package check completes successfully, press **Enter**.
- 8 When you are prompted to uninstall the RALUS packages, press **Enter**.
- 9 When you are prompted to uninstall the SymSnap driver, press **Enter**.
- 10 To save the uninstall summary to the following location on the Linux server, press **Enter**:

`/opt/VRTS/install/logs/uninstallralus<summary file number>.summary`

See “[Installing the Agent for Linux](#)” on page 1076.

## Manually uninstalling the Agent for Linux

You can manually uninstall the Agent for Linux (Linux Agent).

**To manually uninstall the Agent for Linux**

- 1 Use a terminal session to connect to the Linux server as the root user.
- 2 Change to the following directory:

```
/opt/VRTSralus/bin
```

For example:

```
cd /opt/VRTSralus/bin
```

- 3 Delete the following line if it is found in the /etc/inittab file:

```
/opt/VRTSralus/bin/VRTSralus.init
```

For example:

```
rm -r /opt/VRTSralus/bin/VRTSralus.init
```

- 4 Stop the Linux Agent daemon.

See [“Stopping the Agent for Linux daemon”](#) on page 1103.

- 5 Remove the Linux Agent package from the Linux server.

For example:

```
Debian GNU/Linux, Ubuntu          dpkg -r VRTSralus
```

```
Linux                               rpm -e VRTSralus
```

- 6 Change back to the root directory.

For example:

```
cd /
```

- 7 Remove the following files:

```
/etc/VRTSralus
```

```
/opt/VRTSralus
```

```
/var/VRTSralus
```

For example:

```
rm -r /etc/VRTSralus /opt/VRTSralus /var/VRTSralus
```

- 8 Type **y** if you are prompted to descend into the directories.

**9** Type **y** if you are prompted to delete a directory.

**10** Remove runtime scripts if they are present.

See “[Runtime scripts to remove when manually uninstalling the Agent for Linux](#)” on page 1102.

## Runtime scripts to remove when manually uninstalling the Agent for Linux

When you manually uninstall the Agent for Linux (Linux Agent), remove the following runtime scripts if they are present.

**Table O-6** Runtime scripts to remove when manually uninstalling the Linux Agent

Operating system	Runtime scripts to remove
Debian, Ubuntu	<p><b>/etc/rc5.d/S95VRTSralus.init</b>  <b>/etc/rc3.d/S95VRTSralus.init</b>  <b>/etc/rc2.d/S95VRTSralus.init</b>  <b>/etc/init.d/VRTSralus.init</b></p> <p>For example:  <pre>rm /etc/rc5.d/S95VRTSralus.init</pre></p>
Red Hat Linux, Asianux	<p><b>/etc/rc.d/rc5.d/S95VRTSralus.init</b>  <b>/etc/rc.d/rc3.d/S95VRTSralus.init</b>  <b>/etc/rc.d/rc2.d/S95VRTSralus.init</b>  <b>/etc/rc.d/init.d/VRTSralus.init</b></p> <p>For example:  <pre>rm /etc/rc.d/rc5.d/S95VRTSralus.init</pre></p>
Novell Open Enterprise Server 1.0/ SUSE Linux Enterprise Server 9 (32-bit only)	<p><b>/etc/init.d/rc5.d/SxxVRTSralus.init</b>  <b>/etc/init.d/rc3.d/SxxVRTSralus.init</b>  <b>/etc/init.d/rc2.d/SxxVRTSralus.init</b>  <b>/etc/init.d/VRTSralus.init</b></p> <p>For example:  <pre>rm /etc/init.d/rc5.d/SxxVRTSralus.init</pre></p>

**Table O-6** Runtime scripts to remove when manually uninstalling the Linux Agent (*continued*)

Operating system	Runtime scripts to remove
Novell Open Enterprise Server 2.0/ SUSE Linux Enterprise Server 10 (32-bit and 64-bit)	<b>/etc/init.d/VRTSralus.init,start=2,3,5</b> <b>/etc/init.d/VRTSralus.init</b> For example: <pre>rm /etc/init.d/VRTSralus.init</pre>

See [“Manually uninstalling the Agent for Linux ”](#) on page 1100.

## Starting the Agent for Linux daemon

If necessary, you can start the Agent for Linux (Linux Agent) daemon after the operating system starts.

See [“Stopping the Agent for Linux daemon”](#) on page 1103.

### To start the Agent for Linux daemon

- 1 Use a terminal session to connect to the Linux server as the root user.
- 2 Navigate to the following directory:

```
/etc/init.d/
```

For example:

```
cd /etc/init.d/
```

- 3 Start the Linux Agent daemon.

For example:

```
/etc/init.d/VRTSralus.init start
```

## Stopping the Agent for Linux daemon

You can stop the Agent for Linux (Linux Agent) daemon.

See [“Starting the Agent for Linux daemon”](#) on page 1103.

**To stop the Agent for Linux daemon**

- 1 Use a terminal session to connect to the Linux server as the root user.
- 2 Navigate to the following directory:

`/etc/init.d/`

For example:

```
cd /etc/init.d/
```

- 3 Stop the Linux Agent daemon:

For example:

```
/etc/init.d/VRTSralus.init stop
```

- 4 Restart the daemon when necessary.

## Troubleshooting the Agent for Linux

If you experience problems with the Agent for Linux (Linux Agent) review the following questions and answers.

See “[About the Agent for Linux](#)” on page 1074.

**Table O-7** Troubleshooting the Linux Agent

Question	Answer
Some characters do not appear correctly in the terminal session during the installation. What should I do?	This error occurs when the system location uses a non-English language character-set on the computer on which you install the Linux Agent. You can switch to another location setting of the same language to try to resolve this issue.
The Linux Agent installer is unable to install the Linux Agent. The following error is reported in the <b>installralus</b> log file:  <b>VxIF::Error:: Unable to compress files. Hash(0x8711e8)-&gt;({GUNZIP}not found on &lt;hostname&gt;</b>	To support the uncompressing of the Linux Agent platform-specific packages, you can install the GNU data compression utility. Install this utility on the computer on which you want to install the Linux Agent.  The utility is available at the following URL:  <a href="http://www.gzip.org">http://www.gzip.org</a>

**Table O-7** Troubleshooting the Linux Agent (*continued*)

Question	Answer
<p>The Agent for Linux is installed on a Linux server in an NIS domain. Backup Exec is unable to browse resources on the server. What should I do?</p>	<p>Verify if the group line and the password line in the <code>nsswitch.conf</code> file are set to compatibility mode. If they are, then you must configure the <code>/etc/passwd</code> and <code>/etc/group</code> files. Refer to the <code>nsswitch.conf</code> man pages for additional information on how to configure the <code>nsswitch.conf</code> to use compatibility mode.</p> <p>Alternatively, change the password line and the group line to NIS files so that the Linux server validates the user through NIS. If the NIS server is unavailable or if the user is not found, the local files are used for validation.</p>
<p>I cannot load the Linux Agent. When I attempt to load the Linux Agent in console mode, <code>/beremote --log-console</code> shows the following message:</p> <p><b>ACE_SV_Semaphore_Complex: no space left on device.</b></p> <p>What should I do?</p>	<p>This issue occurs when the computer reaches its maximum limit on allowable semaphores. It can occur after an unexpected termination of the Linux Agent. When the Linux Agent unexpectedly terminates, it is unable to clean up some of the semaphore resources that it used. Other processes may have caused the use of semaphores to reach the limit. You must restart the computer to safely recover it from this condition.</p> <p>If other processes are running, it may not be feasible to restart the computer. Instead, you can use the commands that let you list and then remove all semaphores in use by the operating system. Be careful when you select semaphores to remove. Semaphores that are in use by the Linux Agent cannot be identified. If you remove semaphores of other programs that are in use, those programs can become unstable.</p> <p>To list semaphores, you can type the following command:</p> <pre>ipcs -a</pre> <p>To remove semaphores for each identifier that is listed, you can type the following command:</p> <pre>ipcrm -s &lt;id&gt;</pre>

**Table O-7** Troubleshooting the Linux Agent (*continued*)

Question	Answer
<p>I cannot load the Linux Agent. When I attempt to load the Linux Agent in console mode, /beremote --log-console shows the following message:  <b>Error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory.</b></p> <p>What should I do?</p>	<p>This error indicates that the <b>libstdc++.so.5</b> library is not in the /usr/lib directory. This library is necessary to let the Linux Agent start and function. To resolve this issue, install the <b>libstdc++5</b> package.</p> <p>You can install this package from the media on which your copy of Linux was provided. Or, you can run the following command from a computer that has Internet access:</p> <pre>apt-get install libstdc++5</pre> <p>For SUSE Linux Enterprise Server 11, run the following command:</p> <pre>zypper install libstdc++5</pre>

# Symantec Backup Exec Agent for Mac

This appendix includes the following topics:

- [About the Agent for Mac](#)
- [Requirements for the Agent for Mac](#)
- [About the Backup Exec admin group on Macintosh systems](#)
- [About installing the Agent for Mac](#)
- [Uninstalling the Agent for Mac](#)
- [About configuring the Agent for Mac](#)
- [Starting the Agent for Mac](#)
- [Stopping the Agent for Mac](#)
- [About establishing trust for a remote Macintosh system in the Servers list](#)
- [Adding additional Backup Exec servers to which the Agent for Mac can publish information](#)
- [About backing up data by using the Agent for Mac](#)
- [About restoring Macintosh systems](#)
- [Troubleshooting the Agent for Mac](#)

## About the Agent for Mac

The Agent for Mac (Mac Agent) is installed as a separate add-on component. The Mac Agent enables Windows Servers network administrators to perform backup and restore operations on Macintosh systems that are connected to the network. The Mac Agent must be installed on the Macintosh systems before you can perform backup or restore operations.

See “[Requirements for the Agent for Mac](#)” on page 1108.

See “[About installing the Agent for Mac](#)” on page 1110.

## Requirements for the Agent for Mac

The following are required to install the Agent for Mac (Mac Agent):

- The Backup Exec server must have TCP/IP installed.
- You must be a member of the admin group on the Macintosh system on which you want to install the Mac Agent.
- You must have the Backup Exec installation media.
- You must enter a license for the Mac Agent on the Backup Exec server.

Symantec recommends that you use the Secure Shell (SSH) protocol when you push-install the Mac Agent from a local Macintosh system to other remote Macintosh systems. You must enable SSH before you install the Mac Agent.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

See “[About installing the Agent for Mac](#)” on page 1110.

See “[About the Backup Exec admin group on Macintosh systems](#)” on page 1108.

## About the Backup Exec admin group on Macintosh systems

The Backup Exec admin group contains the name of the users who have permission to back up and restore the Macintosh systems.

When you install the Agent for Mac (Mac Agent), Backup Exec creates the admin group and adds root as a member. Any Macintosh user that you add to the admin group gets the necessary permission to back up and restore the Macintosh systems.

However, if an NIS server is detected during the Mac Agent installation, Backup Exec cannot create the admin group. After the installation, you must create the admin group manually on the Macintosh system. You must create the admin group before you start backup and restore operations. Otherwise, connections fail between the Macintosh system and the Backup Exec server .

Before the members of the admin group can perform backup or restore operations, they must have a Backup Exec logon account.

See [“Creating the Backup Exec admin group manually on Macintosh systems”](#) on page 1109.

See [“Creating a Backup Exec logon account”](#) on page 500.

## Creating the Backup Exec admin group manually on Macintosh systems

You must create an admin group on each Macintosh system on which you want to install the Mac Agent (Mac Agent).

See [“About the Backup Exec admin group on Macintosh systems”](#) on page 1108.

---

**Note:** Ensure that you understand how to set security for groups on Macintosh systems before you assign a Group ID for the admin group.

---

**Table P-1** How to manually create the admin group

Step	Action	More Information
Step 1	Navigate to the Macintosh system on which you want to install the Mac Agent.  If the Macintosh system is in a NIS domain, navigate to the NIS domain's group file.	See the NIS documentation for information on how to add a group to a NIS domain group file.
Step 2	Create a group with the following case-sensitive name:  admin	See the Macintosh documentation for more information about how to create a group.
Step 3	In the admin group, add the users that you want to have permission to back up and restore the Macintosh system.	See the Macintosh documentation for more information about how to add users to a group

**Table P-1** How to manually create the admin group (*continued*)

Step	Action	More Information
Step 4	Create a Backup Exec logon account for each user that you add to the admin group.	See “ <a href="#">Creating a Backup Exec logon account</a> ” on page 500.

## About installing the Agent for Mac

Use the Backup Exec installation media to do the following:

- Install the Agent for Mac (Mac Agent) on a local Macintosh system.
- Push-install the Mac Agent from a local Macintosh system to other remote Macintosh systems. If you push-install the Mac Agent, the RSH (Remote Shell) is used by default. Symantec recommends that you use SSH (Secure Shell) instead. To use SSH, you must enable it before you install the Mac Agent. See your Macintosh documentation for more information about SSH.

When the installation is complete, Backup Exec saves the install log file to the following location on the system on which the Mac Agent is installed:

***/var/tmp/vxif/installrams <unique identifier number> for installs***

---

**Note:** Some characters may not appear correctly in the terminal session during the installation. This error occurs when the system location uses a non-English language character-set on the computer on which you install the Mac Agent. You can switch to another location setting of the same language to try to resolve this issue.

---

See “[Installing the Agent for Mac](#)” on page 1110.

## Installing the Agent for Mac

You can install the Agent for Mac (Mac Agent) on a local Macintosh system. You can also push-install the Mac Agent from a local Macintosh system to one or more remote Macintosh systems.

See “[About installing the Agent for Mac](#)” on page 1110.

---

**Note:** You must unzip the RALUS\_RMALS\_RAMs\_<version number>.gz file on a Macintosh system. The installation does not run if it is unzipped on a computer that runs the Windows operating system.

---

### To install the Agent for Mac

- 1 At a Macintosh system, place the Backup Exec installation media in the appropriate drive.
- 2 Navigate to the following directory on the installation media:  
<LinuxUnixMac>
- 3 Copy the RALUS\_RMALS\_RAMs\_<version number>.gz file in this directory to a directory on the local system.
- 4 Unzip the file.  
For example:  

```
gunzip RALUS_RMALS_RAMs_<version number>.gz
```
- 5 Untar the file.  
For example:  

```
tar -xf RALUS_RMALS_RAMs_<version number>.tar
```
- 6 Open **Finder**, and then browse to **Applications > Utilities**.
- 7 Open **Terminal**.
- 8 Do one of the following:

To install the Mac Agent on a local system Do the following in the order listed:

- Start the **installrams** script by typing the following command:  

```
sudo ./installrams
```
- Press **Enter**.

To install the Mac Agent from a local Macintosh computer to a remote Macintosh system

Do the following in the order listed:

- Start the **installrams** script using the **- usesh** switch by typing the following command:  

```
sudo ./installrams -usesh
```
- Press **Enter**.
- Type the name, IP address, or fully qualified domain name of a Macintosh system.

To install the Mac Agent from a local Macintosh computer to one or multiple remote Macintosh systems

Do the following in the order listed:

- Start the **installrams** script using the **- usessh** switch by typing the following command:

```
sudo ./installrams -usessh
```

- Press **Enter**.
- Type the names, IP addresses, or fully qualified domain names of the Macintosh systems. Leave a space between each identifier.

**9** Enter the password for the user name that is currently logged on.

**10** Press **Enter**.

**11** After the installer checks for a valid Macintosh system operating system during the initial system check, press **Enter**.

**12** Review the package installation summary, and then press **Enter**.

**13** After the system installation requirements check completes, press **Enter**.

**14** Start the prerequisites check by pressing **Enter**.

**15** Type the name, IP address, or fully qualified domain name of the Backup Exec server that you want to back up the Mac Agent.

**16** Press **Enter**.

**17** Type any additional names, IP addresses, or fully qualified domain names of the Backup Exec servers that you want to back up this Mac Agent.

**18** Do one of the following:

If the name, IP address, or fully qualified domain name is correct Press **Enter** to continue the installation.

If you want to change a name, IP address, or fully qualified domain name Type **N**, press **Enter**, and then change the information.

**19** Start the NIS server scan by pressing **Enter**.

**20** Examine the results of the NIS server scan, and then do one of the following:

If an NIS server is detected	The Mac Agent installer cannot create the admin group for Backup Exec operators. You must create it manually after the Mac Agent installation is complete.  Continue with the next step.
If a NIS server is not detected	Use the installer to create the admin group.  Do the following in the order listed: <ul style="list-style-type: none"><li>■ To let the installer create the admin group, type <b>y</b>.</li><li>■ To select the next available Group ID, type <b>n</b>.</li><li>■ To add the root user account to the admin group, type <b>y</b>.</li><li>■ Continue with the next step.</li></ul>

- 21 Press **Enter** to begin the installation.
- 22 After a message appears stating that the installation has completed successfully, press **Enter**.
- 23 Start the Mac Agent.  
See [“Starting the Agent for Mac”](#) on page 1122.
- 24 Create the admin group if the installation did not create it automatically.  
See [“Creating the Backup Exec admin group manually on Macintosh systems”](#) on page 1109.
- 25 Perform additional configuration as appropriate.  
See [“About configuring the Agent for Mac”](#) on page 1116.

## Uninstalling the Agent for Mac

An automated uninstall process for the Mac Agent (Mac Agent) is available on the Backup Exec installation media.

You can also manually uninstall the Mac Agent.

See [“Manually uninstalling the Agent for Mac”](#) on page 1114.

The uninstall summary is saved to the following location on the Macintosh system:

**`/var/tmp/vxif/uninstallrams<unique identifier number>.summary`**

The uninstall log file is saved to the following location on the Macintosh system:

**`/opt/VRTS/install/logs/uninstallrams<summary file number>.log`**

After the log files are saved, the uninstall process is complete.

#### **To uninstall the Agent for Mac**

- 1** On a Macintosh system, place the Backup Exec installation media in the appropriate drive.
- 2** On the Macintosh system from which you want to uninstall the Mac Agent, log on using Admin privileges.
- 3** Navigate to the following directory on the Backup Exec installation media:  
<LinuxUnixMac>
- 4** Start the **uninstallrams** script.

For example:

```
./uninstallrams
```

- 5** Do one of the following:

To uninstall the Mac Agent from one system

Type the name, IP address, or fully qualified domain name of the Macintosh system.

To uninstall the Mac Agent from multiple systems

Type the names, IP addresses, or fully qualified domain names of the Macintosh systems. Leave a space between each identifier.

- 6** Press **Enter**.
- 7** After the Mac Agent package check completes successfully, press **Enter**.
- 8** When you are prompted to uninstall the RALUS packages, press **Enter**.
- 9** When the uninstall process is complete, press **Enter**.

## Manually uninstalling the Agent for Mac

You can manually uninstall the Agent for Mac (Mac Agent) from Macintosh systems.

You can also use the Backup Exec installation media to uninstall the Mac Agent.

See [“Uninstalling the Agent for Mac”](#) on page 1113.

**To manually uninstall the Agent for Mac**

**1** Use a logon account with Admin privileges to log on to a terminal session to connect to the Macintosh system.

**2** Change to the following directory:

```
/opt/VRTSralus/bin
```

For example:

```
cd /opt/VRTSralus/bin
```

**3** Delete the following line if it is found in the /etc/inittab file:

```
/opt/VRTSralus/bin/VRTSralus.init
```

For example:

```
rm -r /opt/VRTSralus/bin/VRTSralus.init
```

**4** Stop the Mac Agent daemon.

See [“Stopping the Agent for Mac ”](#) on page 1123.

**5** Remove the Mac Agent package from the Linux server.

**6** Change back to the root directory.

For example:

```
cd /
```

**7** Remove the following files:

```
/etc/VRTSralus
```

```
/opt/VRTSralus
```

```
/var/VRTSralus
```

For example:

```
rm -r /etc/VRTSralus /opt/VRTSralus /var/VRTSralus
```

**8** Type **y** if you are prompted to descend into the directories.

**9** Type **y** if you are prompted to delete a directory.

**10** Remove the /Library/StartupItems/VRTSrams folder.

For example:

```
rm -r /Library/StartupItems/VRTSrams
```

**11** Type **y** if you are prompted to delete a directory.

## About configuring the Agent for Mac

Backup Exec creates a file named `ralus.cfg` on each Macintosh system on which the Agent for Mac (Mac Agent) is installed.

You can edit the following strings, identifiers, and variables for the Mac Agent in the `ralus.cfg` file:

- The port to which the Mac Agent must send publishing messages.
- The settings to allow the Mac Agent to publish to one or more Backup Exec servers.
- The files and directories on Macintosh systems that you want to exclude from backups.

The `ralus.cfg` format contains three components. The first component (A) in the following example is a required string.

The second component (B) is a unique identifier followed by an equal sign (=). A unique identifier can consist of sequential numbers, letters, or alpha-numeric characters. For example, 1, 2, 3 or A, B, C. You can also use AA, BB, CC, or A1, A2, B1, B2.

The third component of the `ralus.cfg` format is the NetBIOS name, fully qualified domain name, or IP address of the Backup Exec server.

**Figure P-1** Example of the `ralus.cfg` file

```
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 1=svr.mycompany.com
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 2=datasrv
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 3=66.35.250.151
```

- A = Required string
- B = Required and unique identifier (the order or appearance is irrelevant)
- C = File or directory to be excluded

See [“Editing the default backup options for Macintosh systems”](#) on page 1125.

See [“Adding servers to the list of servers”](#) on page 158.

See [“About excluding files and directories from backup jobs for Linux computers”](#) on page 1082.

## Editing configuration options for Macintosh computers

You can edit configuration options for the Agent for Mac (Mac Agent).

See [“About excluding files and directories from backup jobs for Macintosh computers”](#) on page 1127.

See “[Configuration options for Macintosh computers](#)” on page 1117.

### To edit configuration options for Macintosh computers

- 1 Use a text editor to open the following file:  
`/etc/VRTSralus/ralus.cfg`
- 2 Change the appropriate string in the file.

## Configuration options for Macintosh computers

You can edit options to configure the Agent for Mac (Mac Agent).

Table P-2

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agent Browser\TcpIp\AdvertisementPort=6101	Lists the port to which the Mac Agent must send publish and purge messages.
Software\Symantec\Backup Exec for Windows\Backup Exec\Debug\VXBSAlevel=0	Enables logging for the Linux agent for Oracle operations. Values include the following: <ul style="list-style-type: none"><li>■ 0 Logging is not enabled.</li><li>■ 5 Normal logging is enabled.</li><li>■ 6 Advanced logging is enabled. Large log files may be created.</li></ul> This option does not apply to the Agent for Mac.

**Table P-2** (continued)

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Agents\Advertise All=1	<p>Enables the Mac Agent to publish information to all of the Backup Exec servers that are listed in the \Agents\Agent Directory List strings.</p> <p>Values include the following:</p> <ul style="list-style-type: none"><li>■ 1 The Mac Agent publishes information to every Backup Exec server in the Agent Directory List.</li><li>■ 0 The Mac Agent publishes information to the first Backup Exec server in the Agent Directory List. If the attempt is successful, the Mac Agent does not publish information to any other Backup Exec servers. If the attempt is not successful, the Mac Agent attempts to publish information to the next Backup Exec server in the list. Attempts continue until the Mac Agent reaches the end of the list.</li></ul>

Table P-2 (continued)

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertise Now=0	<p>Enables the Mac Agent to start a new publishing cycle after you add or edit any settings in the ralus.cfg file.</p> <p>Values include the following:</p> <ul style="list-style-type: none"><li data-bbox="821 470 1247 673">■ 0 The Mac Agent publishes information according to its regular cycle, set in the string \Agents\Advertising Interval Minutes. Any changes to the ralus.cfg file take effect when a new publishing cycle begins.</li><li data-bbox="821 682 1247 1147">■ 1 The Mac Agent starts a new publishing cycle. Any changes to the ralus.cfg file take effect immediately. If the Backup Exec server does not receive the publishing information, the Mac Agent makes ten more attempts. Each attempt to publish information to the Backup Exec server is one minute apart. If the information is not sent at the end of the ten attempts, the Mac Agent skips that Backup Exec server until the next publishing cycle. The publishing cycle is the number of minutes set in the string \Agents\Advertising Interval Minutes.</li></ul>

**Table P-2** (continued)

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertisement Purge=0	<p>Lets the Mac Agent send a purge message to all of the Backup Exec servers in the string \Agents\Advertisement Purge. When a Backup Exec server receives a purge message, it removes the Mac Agent from Backup Exec's list of available servers. The Mac Agent continues to function.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 Do not purge the Mac Agent from any Backup Exec servers that are listed in the \Agents\Advertisement Purge string.</li> <li>■ 1 Purge the Mac Agent from one or more Backup Exec servers in the \Agents\Advertisement Purge string.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertising Disabled=0	<p>Enables the Mac Agent to publish to Backup Exec servers.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 The Mac Agent attempts to publish information to the Backup Exec servers that are listed in the string \Agents\Agent Directory List.</li> <li>■ 1 The Mac Agent does not publish information to Backup Exec servers.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Advertising Interval Minutes=240	<p>Sets the number of minutes that the Mac Agent must wait between publishing cycles. The default number of minutes is 240. The range of minutes is from 1 minute to 720 minutes.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Agent Directory List 1=<Backup Exec server name>	<p>Displays the list of NetBIOS names, fully qualified domain names, or IP addresses to which the Mac Agent publishes information.</p> <p>The Backup Exec server from which the Mac Agent is push installed is added to the Agent Directory List by default.</p>

Table P-2 (continued)

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Agents\Auto Discovery Enabled=1	<p>Adds a Backup Exec server to the string \Agents\Agent Directory List if the Backup Exec server performs a backup job with which the Mac Agent is associated.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 1 Adds the Backup Exec server that performs the backup job to the Agent Directory List. The Mac Agent can publish information to the Backup Exec server.</li> <li>■ 0 The Backup Exec server that performs the backup job is not added to the Agent Directory List.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Logging\RANT NDMP Debug Level=0	<p>Displays the level of verbosity for logging NDMP information for the Mac Agent.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ 0 Logs only the NDMP errors.</li> <li>■ 1 Logs the NDMP errors and warnings.</li> <li>■ 2 Logs the NDMP errors, warnings, and message information that is sent between the remote computer and the Backup Exec server.</li> </ul>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\Encoder=	<p>Displays the encoder that you can add if the default encoder incorrectly displays characters on the user interface.</p>

**Table P-2** (continued)

Item	Description
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS>ShowTSAFS=	<p>Lets you perform a Target Service Agent file system (TSAFS) backup for applications on Novell Open Enterprise Services. By default, this option is not enabled.</p> <p>The Mac Agent backs up all file systems using the Root object. If ShowTSAFS is enabled, the Novell Open Enterprise Services resource appears in the backup selection list. If you select the whole computer for backup, then redundant backups are performed. Symantec recommends that you do not enable this option.</p> <p>Values include the following:</p> <ul style="list-style-type: none"> <li>■ Blank or 0 The file system TSA does not appear for backup selection.</li> <li>■ 1 The file system TSA resource appears for backup selection.</li> </ul> <p>This option does not apply to the Agent for Mac.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemExclude1=	<p>Lists the files that you want to exclude from all Mac Agent backup jobs.</p> <p>See <a href="#">“About excluding files and directories from backup jobs for Macintosh computers”</a> on page 1127.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemFSTypeExclude1	<p>Lists the type of file system that you want to exclude from the Mac Agent backup.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\vfmpath= /opt/VRTSralus/VRTSvxms	<p>Displays the path to the Veritas Mapping Service libraries that the Mac Agent uses.</p>

## Starting the Agent for Mac

You can manually start the Agent for Mac (Mac Agent).

See [“Stopping the Agent for Mac”](#) on page 1123.

#### To manually start the Agent for Mac

- 1 Use a terminal session to connect to the target Macintosh system as the root user.
- 2 From the root prompt, start the VRTSrams service.

For example:

```
SystemStarter start VRTSrams
```

## Stopping the Agent for Mac

You can manually stop the Agent for Mac (Mac Agent).

See [“Starting the Agent for Mac”](#) on page 1122.

#### To manually stop the Agent for Mac

- 1 Use a terminal session to connect to the target Macintosh system as the root user.
- 2 From the root prompt, stop the VRTSrams service:

For example:

```
SystemStarter stop VRTSrams
```

## About establishing trust for a remote Macintosh system in the Servers list

When you connect to a Macintosh system from the Backup Exec server, you must establish trust between the Backup Exec server and the remote Macintosh computer. You must also establish trust if you want to configure a remote Macintosh computer to perform client-side deduplication.

See [“About establishing a trust between the Backup Exec server and a remote computer”](#) on page 734.

See [“Establishing trust and adding a remote Macintosh computer to the Backup Exec Servers list”](#) on page 1124.

## Establishing trust and adding a remote Macintosh computer to the Backup Exec Servers list

You can add one or more remote Macintosh computers to the list of servers on the **Backup and Restore** tab. When you add remote Macintosh computers, you must establish a trust between the Backup Exec server and the remote Linux computers to ensure secure communication.

See [“About establishing trust for a remote Macintosh system in the Servers list”](#) on page 1123.

**To establish trust and add a remote Macintosh computer to the Backup Exec Servers list**

- 1 On the **Backup and Restore** tab, in the **Servers** group, click **Add**.
- 2 Click **Macintosh computer**.
- 3 Follow the on-screen prompts.

See [“Adding servers to the list of servers”](#) on page 158.

See [“Adding additional Backup Exec servers to which the Agent for Mac can publish information”](#) on page 1124.

## Adding additional Backup Exec servers to which the Agent for Mac can publish information

You can specify additional Backup Exec servers to which the Mac Agent (Mac Agent) can publish information.

Each Backup Exec server to which the Mac Agent publishes information appears in the **Backup and Restore** tab, under the **Servers** list.

**To add additional Backup Exec servers to which the Agent for Mac can publish information**

- 1 Use a text editor to open the following file:

```
/etc/VRTSralus/ralus.cfg
```

- 2 Add the following string:

```
Software\Symantec\Backup Exec For Windows\Backup  
Exec\Engine\Agents\Agent Directory List unique identifier number = IP  
address or DNS name of Backup Exec server
```

- 3 Save and close the file.
- 4 Move to the Backup Exec server to which the Mac Agent is publishing itself and add the Macintosh computer to the **Servers** list.

See [“Adding servers to the list of servers”](#) on page 158.

## About backing up data by using the Agent for Mac

When you use the Agent for Mac (Mac Agent) to back up data, only the following backup methods are supported for Macintosh systems:

- Full - Using modified time
- Differential - Using modified time
- Incremental - Using modified time

When you use the **Backup Wizard** to specify backup job settings for the Mac Agent, only full backups are supported. If you select any other backup method in the **Backup Wizard**, a full backup runs.

See [“Backing up data”](#) on page 163.

See [“About stages”](#) on page 183.

See [“Editing a stage”](#) on page 184.

## Editing the default backup options for Macintosh systems

You can use the existing defaults for all backup jobs for Macintosh systems, or you can edit the defaults.

### To edit default backup options for Macintosh computers

- 1 Click the Symantec Backup Exec button, select **Configuration and Settings**, and then select **Backup Job Defaults**.
- 2 Select a backup option.
- 3 On the left, click **Linux and Macintosh**.
- 4 Select the default backup options for the Agent for Mac (Mac Agent).
- 5 Set the appropriate options.  
See [“Default backup job options for Macintosh systems”](#) on page 1126.
- 6 Click **OK**.

## Default backup job options for Macintosh systems

When you back up a Macintosh system, you should consider the following options.

See [“Editing the default backup options for Macintosh systems”](#) on page 1125.

**Table P-3** Default backup job options for Macintosh systems

Item	Description
<b>Preserve file and directory timestamps during backups</b>	<p>Prevents the Agent for Mac (Mac Agent) from changing an object's attributes when a backup occurs. An object is a file or a directory.</p> <p>This option is not selected by default.</p> <p>During a backup, Backup Exec preserves an object's last access timestamp by resetting the last access timestamp to the value before the backup occurred. When Backup Exec modifies the object's last access timestamp, the operating system internally updates the object's ctime.</p> <p>An object's ctime is the time when an object's attributes, such as permissions and timestamps, have been modified. If the Mac Agent does not change the attributes after a backup, the object's ctime is not changed.</p> <p>This option does not affect the attributes of the object that are set during restore operations.</p>
<b>Follow local mount points</b>	<p>Lets Backup Exec follow local mount points to back up data.</p> <p>This option is enabled by default.</p> <p>For more information on local mount points, see your operating system's documentation.</p>

**Table P-3** Default backup job options for Macintosh systems (*continued*)

Item	Description
<b>Follow remote mount points</b>	<p>Lets Backup Exec follow remote mount points to back up data.</p> <p>This option is not selected by default.</p> <p>When you use this option, the following limitations apply:</p> <ul style="list-style-type: none"> <li>■ The data that is mounted must reside on a system that Backup Exec supports. You can find a list of supported operating systems, platforms, and applications at the following URL: <a href="http://entsupport.symantec.com/umi/v-269-1">http://entsupport.symantec.com/umi/v-269-1</a></li> <li>■ If the mount point leads to an operating system that Backup Exec does not support, contact the operating system's vendor to resolve any issues.</li> </ul> <p>For more information on remote mount points, see your operating system's documentation.</p>
<b>Lock remote files to prevent applications from modifying them during backups</b>	<p>Lets the Mac Agent have exclusive access to the files on the remote servers that are connected through Network File System (NFS). Locking remote files prevents other applications from modifying the data during the backup or restore job.</p>

## About excluding files and directories from backup jobs for Macintosh computers

You can exclude specific files and directories on Macintosh computers from all backup jobs. Edit the `ralus.cfg` file to specify the excluded files.

The following is an example of strings in the `ralus.cfg` file that excludes files and directories from all backup jobs.

**Figure P-2** Example of file and directory exclusions in the ralus.cfg format

```
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude1=Adev/*.*B
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude2=Aproc/*.*B
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude3=Amnt/nss/pools/C
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude4=Amnt/nss/.pools/C
```

A = Required string  
B = Required and unique identifier (the order or appearance is irrelevant)  
C = File or directory to be excluded

To exclude files and directories for specific backup jobs, specify the exclusions in the backup job properties.

See [“Editing configuration options for Macintosh computers”](#) on page 1116.

## About restoring Macintosh systems

You can specify restore job properties to restore Macintosh systems.

See [“Macintosh restore options”](#) on page 1128.

### Macintosh restore options

When you restore Macintosh systems, you can enable the option to **Lock remote files**. This option allows exclusive access to the files on the remote systems that are connected through the Network File System (NFS). This option is enabled by default.

See [“About restoring Macintosh systems”](#) on page 1128.

## Troubleshooting the Agent for Mac

If you experience problems with the Agent for Mac (Mac Agent), read the following questions and answers.

**Table P-4** Troubleshooting the Agent for Mac

Question	Answer
<p>The Mac Agent is installed on a Macintosh system in a NIS domain, but Backup Exec is unable to browse resources on the system. What do I do?</p>	<p>If the group line and the password line in the nsswitch.conf file are set to compatibility mode, additional configuration is necessary. Refer to the nsswitch.conf man pages for additional information on configuring nsswitch.conf to use compatibility mode.</p> <p>Alternately, change the password line and the group line to NIS files so that the Macintosh system validates the user through NIS. If the NIS server is unavailable or the user is not found, the local files are used for validation.</p>
<p>I cannot load the Mac Agent. When I attempt to load the Mac Agent in console mode, ".beremote --log-console" shows the following message:</p> <p><b>"ACE_SV_Semaphore_Complex: no space left on device."</b></p> <p>What should I do?</p>	<p>This issue occurs when the computer reaches its maximum limit on allowable semaphores. It can occur after an unexpected termination of the Mac Agent. When the Mac Agent unexpectedly terminates, it is unable to clean up some of the semaphore resources that it used. Other processes may have caused the use of semaphores to reach the limit. You must restart the computer to safely recover it from this condition.</p> <p>If other processes are running, it may not be feasible to restart the computer. Instead, you can use the commands that let you list and then remove all semaphores in use by the operating system. Be careful when you select semaphores to remove. Semaphores that are in use by the Mac Agent cannot be identified. If you remove semaphores of other programs that are in use, those programs can become unstable.</p>



# Symantec Backup Exec Remote Media Agent for Linux

This appendix includes the following topics:

- [About the Remote Media Agent for Linux](#)
- [How the Remote Media Agent for Linux works](#)
- [Requirements for the Remote Media Agent for Linux](#)
- [About open files and the Remote Media Agent for Linux](#)
- [About installing the Remote Media Agent for Linux](#)
- [Uninstalling the Remote Media Agent for Linux](#)
- [Starting the Remote Media Agent for Linux daemon](#)
- [Stopping the Remote Media Agent for Linux daemon](#)
- [About establishing trust for a Remote Media Agent for Linux computer in the Backup Exec list of servers](#)
- [Adding additional Backup Exec servers to which Remote Media Agent for Linux can publish](#)
- [Finding simulated tape library files](#)
- [About the Backup Exec operators group for the Remote Media Agent for Linux](#)
- [About adding a Linux server as a Remote Media Agent for Linux](#)

- [Changing the port for communications between the Backup Exec server and the Remote Media Agent for Linux](#)
- [About creating storage device pools for devices attached to the Remote Media Agent for Linux](#)
- [Editing properties for the Remote Media Agent for Linux](#)
- [Deleting a Remote Media Agent for Linux from the Backup Exec list of servers](#)
- [Sharing a Remote Media Agent for Linux between multiple Backup Exec servers](#)
- [About backing up data by using the Remote Media Agent for Linux](#)
- [About restoring data by using the Remote Media Agent for Linux](#)
- [About the Tape Library Simulator Utility](#)
- [Creating a simulated tape library](#)
- [Viewing simulated tape libraries properties](#)
- [Deleting a simulated tape library](#)
- [Managing simulated tape libraries from the command line](#)
- [Command line switches for the Tape Library Simulator Utility](#)
- [Troubleshooting the Remote Media Agent for Linux](#)

## About the Remote Media Agent for Linux

The Remote Media Agent for Linux (RMAL) lets you back up data from remote computers to the following devices:

- The storage devices that are directly attached to a Linux server.
- A simulated tape library on a Linux server.

You can add a Linux server to a Backup Exec server as a RMAL. You can then back up data from the Linux server or from supported remote computers to the devices that are attached to the Linux server. You can also create a virtual device on a server on which RMAL is installed. This virtual device emulates a SCSI tape library.

RMAL supports operations for the following agents:

- Agent for Windows
- Agent for Mac
- Agent for Oracle on Linux or Windows Servers

See “[How the Remote Media Agent for Linux works](#)” on page 1133.

See “[About the Tape Library Simulator Utility](#)” on page 1149.

## How the Remote Media Agent for Linux works

From the Backup Exec server, you can add a Linux server as a Remote Media Agent for Linux (RMAL). RMAL establishes a data connection to the remote computer on which a supported agent is installed. You can then create backup, restore, and utility jobs on the Backup Exec server that run on the Linux server's storage devices.

If you use Backup Exec Central Admin Server Option, you can share a RMAL computer between multiple Backup Exec servers. Sharing can be enabled when you add RMAL. You can select new Backup Exec servers to share RMAL or remove the sharing ability from the Backup Exec servers at any time.

See “[About sharing storage devices](#)” on page 418.

Job performance increases because data travels from the remote computers to the devices that are attached to the Linux server. This increase is especially apparent if the Backup Exec server is located at a different site than the RMAL computer and the remote computers.

RMAL does not have a user interface. You use the administration console on the Backup Exec server to manage the jobs and devices on RMAL. The Backup Exec server maintains job logs, catalogs, job histories, alerts, and notifications.

See “[Requirements for the Remote Media Agent for Linux](#)” on page 1133.

See “[About installing the Remote Media Agent for Linux](#)” on page 1134.

See “[About adding a Linux server as a Remote Media Agent for Linux](#)” on page 1143.

See “[About the Tape Library Simulator Utility](#)” on page 1149.

## Requirements for the Remote Media Agent for Linux

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

You can find a list of compatible devices at the following URL:

<http://entsupport.symantec.com/umi/V-269-2>

You must have superuser privileges on the Linux servers before you install RMAL.

---

**Note:** RMAL does not support the Backup Exec File System Archiving Option or the Exchange Mailbox Archiving Option.

---

Symantec recommends that you use the Secure Shell (SSH) protocol when you push-install RMAL to remote servers. You must enable SSH before you install RMAL.

---

**Note:** Some versions of Linux may require that you install the `libstdc++.so.5` package.

---

See [“About installing the Remote Media Agent for Linux”](#) on page 1134.

## About open files and the Remote Media Agent for Linux

The Remote Media Agent for Linux (RMAL) uses advanced open file and image technologies that are designed to alleviate issues that are sometimes encountered during backup operations, such as backing up open files.

After you make file and folder selections and the job is submitted for backup, RMAL automatically makes a snapshot of the volume or volumes. Making snapshot of a volume provides a point-in-time record of the data. When it creates a snapshot, RMAL uses snapshot technologies to momentarily suspend write activity to a volume so that a snapshot of the volume can be created. During the backup, files can be open and data can be changed.

RMAL supports Simple, Logical Volume Manager (LVM), and RAID volume configurations.

See [“Requirements for the Remote Media Agent for Linux”](#) on page 1133.

## About installing the Remote Media Agent for Linux

Use the Backup Exec installation media to do the following:

- Install Remote Media Agent for Linux (RMAL) on a local Linux server.
- Push-install RMAL to one or more remote Linux servers.  
If you push-install RMAL, the RSH (Remote Shell) is used by default. Symantec recommends that you use SSH (Secure Shell) instead. To use SSH, you must enable it before you install RMAL. Refer to your operating system documentation for more information about SSH.

When you install RMAL, Backup Exec creates the beoper group and adds root as a member. Any Linux user that you add to the beoper group gets the permissions necessary to back up and restore the Linux servers.

However, if Backup Exec detects an NIS server during the RMAL installation, then the beoper group is not created. You must create the beoper group manually on the Linux servers.

After the installation completes, you must add the Linux server as a Remote Media Agent on the Backup Exec server. Then, you can send jobs to the devices that are attached to the Linux server.

See [“Installing the Remote Media Agent for Linux”](#) on page 1135.

See [“Creating the Backup Exec operators group manually for the Remote Media Agent for Linux”](#) on page 1142.

See [“About adding a Linux server as a Remote Media Agent for Linux”](#) on page 1143.

See [“About the Backup Exec operators group for the Remote Media Agent for Linux”](#) on page 1142.

## Installing the Remote Media Agent for Linux

You can install Remote Media Agent for Linux (RMAL) on a local Linux server or push-install it to one or more remote Linux servers.

See [“About installing the Remote Media Agent for Linux”](#) on page 1134.

---

**Note:** You must unzip the RALUS\_RMALS\_RAMs\_<version number>.gz file on a Linux server. The installation does not run if it is unzipped on a computer that runs the Windows operating system.

---

### To install the Remote Media Agent for Linux

- 1 At a Linux server, place the Backup Exec installation media in the appropriate drive.
- 2 Log on as root on the server on which you want to install RMAL.
- 3 Navigate to the following path on the installation media:  
    <LinuxUnixMac>
- 4 Copy the RALUS\_RMALS\_RAMs\_<version number>.gz file in this directory to a directory on the local server.

**5** Unzip the file.

For example:

```
gunzip RALUS_RMALS_RAMs_<version number>.gz
```

**6** Untar the file.

For example:

```
tar -xf RALUS_RMALS_RAMs_<version number>.tar
```

**7** Start the **installrmal** script.

For example:

```
./installrmal
```

**8** Do one of the following:

To install on a local server

Press **Enter**.

To install to one remote server

Type the name, IP address, or fully qualified domain name of a Linux server.

To install to multiple remote servers

Type the names, IP addresses, or fully qualified domain names of the Linux servers. Leave a space between each identifier.

**9** After the installer checks for a valid Linux operating system during the initial system check, press **Enter**.

**10** Review the package installation summary, and then press **Enter**.

**11** After the system installation requirements check completes, press **Enter**.

**12** Start the prerequisites check by pressing **Enter**.

**13** Type the name, IP address, or fully qualified domain name of the Backup Exec server (directory host) that you want to use this Remote Media Agent.

**14** Type any additional names, IP addresses, or fully qualified domain names of Backup Exec servers that you want to use this Remote Media Agent.

**15** Do one of the following:

If the server name, IP address, or fully qualified domain name is correct

Press **Enter** to continue the installation.

If you want to change a server name, IP address, or fully qualified domain name

Type **N**, press **Enter**, and then change the information.

- 16 Start the NIS server scan by pressing **Enter**.
- 17 Examine the results of the NIS server scan, and then do one of the following:

If an NIS server is detected	The RMAL installer cannot create the beoper group. You must create it manually after RMAL installation is complete.  Continue with the next step.
If an NIS server is not detected	Use the installer to create the beoper group.  Do the following in the order listed: <ul style="list-style-type: none"><li>■ To let the installer create the beoper group, type <b>y</b>.</li><li>■ To select the next available Group ID, type <b>n</b>.</li><li>■ To add the root user account to the beoper group, type <b>y</b>.</li><li>■ Continue with the next step.</li></ul>
- 18 Start the installation by pressing **Enter**.
- 19 After installation completes, press **Enter** to start the post-installation configurations and installation of SymSnap drivers.
- 20 Press **Y** to automatically start the Beremote service; otherwise, press **N** to start the service later
- 21 After the configuration process completes, press **Enter** to save the installation log to the following file:  
*/var/tmp/vxif/installrmalsummary file number/installrml.log*
- 22 If the RMAL installer did not create a beoper group, you must create it.  
[See “Creating the Backup Exec operators group manually for the Remote Media Agent for Linux” on page 1142.](#)
- 23 Start the Agent for Linux daemon.  
[See “Starting the Agent for Linux daemon” on page 1103.](#)
- 24 Add the Linux server as a Remote Media Agent.  
[See “About adding a Linux server as a Remote Media Agent for Linux ” on page 1143.](#)

# Uninstalling the Remote Media Agent for Linux

Before you uninstall the Remote Media Agent for Linux (RMAL), you should note the location of the simulated tape library files. Then, you can delete all of the simulated tape library files after the uninstall operation completes. When you delete these files, you delete the backup data that you stored on the Linux server.

See [“Finding simulated tape library files”](#) on page 1141.

---

**Note:** You must have the Backup Exec installation media to uninstall RMAL.

---

## To uninstall the Remote Media Agent for Linux

- 1 On the Linux server, place the Backup Exec installation media in the appropriate device.
- 2 Log on as root to the server from which you want to uninstall RMAL.
- 3 Navigate to the following path on the installation media:

<LinuxUnixMac>

- 4 Start the **uninstallrmal** script.

For example:

```
./uninstallrmal
```

- 5 Do one of the following:

To uninstall RMAL from one server      Type the name, IP address, or fully qualified domain name of the Linux server.

To uninstall RMAL from multiple servers      Type the names, IP addresses, or the fully qualified domain names of the Linux servers. Leave a space between each identifier.

- 6 Press **Enter**.
- 7 After the RMAL package check completes successfully, press **Enter**
- 8 When you are prompted to uninstall the RMAL packages, press **Enter** to save the uninstall summary and log to the following location:

```
/var/tmp/vxif/uninstallrmalsummary file number.log
```

- 9 Manually delete the simulated tape library files.

# Starting the Remote Media Agent for Linux daemon

If necessary, you can start the Remote Media Agent for Linux (RMAL) daemon after the operating system starts.

See [“Stopping the Remote Media Agent for Linux daemon”](#) on page 1139.

## To start the Remote Media Agent for Linux daemon

- 1 Use a terminal session to connect to the Linux server as the root user.
- 2 Navigate to the following directory:

```
/etc/init.d/
```

For example:

```
cd /etc/init.d/
```

- 3 Start the RMAL daemon.

For example:

```
/etc/init.d/VRTSralus.init start
```

# Stopping the Remote Media Agent for Linux daemon

You can stop the Remote Media Agent for Linux (RMAL) daemon.

See [“Starting the Remote Media Agent for Linux daemon”](#) on page 1139.

## To stop the Remote Media Agent for Linux daemon

- 1 Use a terminal session to connect to the Linux server as the root user.
- 2 Navigate to the following directory:

```
/etc/init.d/
```

For example:

```
cd /etc/init.d/
```

- 3 Stop the RMAL daemon.

For example:

```
/etc/init.d/VRTSralus.init stop
```

- 4 Restart the RMAL daemon when necessary.

## About establishing trust for a Remote Media Agent for Linux computer in the Backup Exec list of servers

When you connect to a Remote Media Agent for Linux (RMAL) computer from the Backup Exec server, you must establish trust between the Backup Exec server and the RMAL computer. You must also establish trust if you want to configure a remote RMAL computer to perform client-side deduplication.

See [“About establishing a trust between the Backup Exec server and a remote computer”](#) on page 734.

See [“Establishing trust and adding a Remote Media Agent for Linux computer to the Backup Exec list of servers”](#) on page 1140.

### Establishing trust and adding a Remote Media Agent for Linux computer to the Backup Exec list of servers

You can add one or more Remote Media Agent for Linux (RMAL) computers to the Backup Exec list of servers. When you add RMAL, you must establish a trust between the Backup Exec server and the remote Linux computers to ensure secure communication.

**To establish trust and add a Remote Media Agent for Linux computer to the Backup Exec list of servers**

- 1 On the **Storage** tab, click **Configure Storage**, and then select **Network storage**.
- 2 Click **Next**.
- 3 Select **Backup Exec Remote Media Agent for Linux**, and then click **Next**.
- 4 Follow the on-screen prompts.

See [“About establishing trust for a Remote Media Agent for Linux computer in the Backup Exec list of servers”](#) on page 1140.

## Adding additional Backup Exec servers to which Remote Media Agent for Linux can publish

You can specify additional Backup Exec servers to which the Remote Media Agent for Linux (RMAL) can publish information.

Each Backup Exec server to which RMAL publishes information appears in the Backup Exec list of servers.

### To add additional Backup Exec servers to which the Remote Media Agent for Linux can publish information

- 1 Use a text editor to open the following file:  
`/etc/VRTSralus/ralus.cfg`
- 2 Add the following string:  
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List *unique identifier number* = IP address or DNS name of Backup Exec server
- 3 Save and close the file.
- 4 Move to the Backup Exec server to which the Remote Media Agent for Linux is publishing itself and add the RMAL server to the **Servers** list.

See [“Adding servers to the list of servers”](#) on page 158.

## Finding simulated tape library files

Before you uninstall RMAL, you should note the location of the simulated tape library files. Then, after you uninstall RMAL, you can delete all of the simulated tape library files. When you delete these files, you delete the backup data that you stored on the Linux server.

See [“Uninstalling the Remote Media Agent for Linux”](#) on page 1138.

See [“About the Tape Library Simulator Utility”](#) on page 1149.

### To find simulated tape library files

- 1 Log on as root to the server on which you want to find the simulated tape library files.
- 2 Navigate to the following directory that contains the Tape Library Simulator:  
`/opt/VRTSralus/bin`  
For example:  

```
cd /opt/VRTSRALUS/bin
```
- 3 Start the **mktls** utility to list the simulated tape library files and folders.  
For example:  

```
/opt/VRTSralus/bin/mktls -l
```
- 4 Write down the locations of the directories for the simulated tape library files.

## About the Backup Exec operators group for the Remote Media Agent for Linux

The Backup Exec operators (**beoper**) group contains the names of the users who have permission to back up and restore the Linux servers.

When you install the Remote Media Agent for Linux (RMAL), Backup Exec creates the **beoper** group and adds root as a member. Any Linux user that you add to the beoper group gets the necessary permission to back up and restore the Linux servers.

However, if an NIS server is detected during RMAL installation, Backup Exec cannot create the **beoper** group. You must create the **beoper** group manually on the Linux servers on which you want to install RMAL. You must create the **beoper** group before you start backup and restore operations. Otherwise, connections fail between the Linux servers and the Backup Exec server.

Before the members of the **beoper** group can perform backup or restore operations, they must have a Backup Exec logon account.

See [“Creating the Backup Exec operators group manually for the Remote Media Agent for Linux”](#) on page 1142.

See [“Creating a Backup Exec logon account”](#) on page 500.

## Creating the Backup Exec operators group manually for the Remote Media Agent for Linux

If the Remote Media Agent for Linux (RMAL) installation detects an NIS server during installation, you must create a beoper group on each Linux server on which you install RMAL.

See [“About the Backup Exec operators group for the Remote Media Agent for Linux”](#) on page 1142.

---

**Note:** Ensure that you understand how to set security for groups on Linux servers before you assign a Group ID for the beoper group.

---

**Table Q-1** How to manually create the beoper group

Step	Action	More Information
Step 1	Navigate to the Linux server on which you want to install RMAL.  If the Linux server is in a NIS domain, navigate to the NIS domain's group file.	See the NIS documentation for information on how to add a group to a NIS domain group file.
Step 2	Create a group with the following case-sensitive name:  <b>beoper</b>	See the operating system documentation for more information about how to create a group.
Step 3	In the beoper group, add the users that you want to have permission to back up and restore the Linux server.	See the operating system documentation for more information about how to add users to a group.
Step 4	Create a Backup Exec logon account for each user that you add to the beoper group.	See <a href="#">“Creating a Backup Exec logon account”</a> on page 500.

## About adding a Linux server as a Remote Media Agent for Linux

After you add the Linux server as a Remote Media Agent for Linux (RMAL), and if you purchased and installed the Central Admin Server Option, you can share the storage devices that are connected to the RMAL computer with other Backup Exec servers.

See [“Adding a Linux server as a Remote Media Agent for Linux”](#) on page 1143.

See [“About sharing storage devices”](#) on page 418.

See [“About the Central Admin Server Option”](#) on page 996.

See [“About the Configure Storage wizard”](#) on page 145.

### Adding a Linux server as a Remote Media Agent for Linux

Use the following steps to add a Linux server as a Remote Media Agent for Linux (RMAL).

See [“About adding a Linux server as a Remote Media Agent for Linux”](#) on page 1143.

### To add a Linux server as a Remote Media Agent for Linux

- 1 On the **Storage** tab, click **Configure Storage**.
  - 2 Select **Network storage**, and then click **Next**.
  - 3 Select **Backup Exec Remote Media Agent for Linux**, and then click **Next**.
  - 4 Follow the on-screen prompts to trust the RMAL and to restart the services.
- See [“About sharing storage devices”](#) on page 418.
- See [“About the Configure Storage wizard”](#) on page 145.

## Remote Media Agent for Linux options

You must provide information when you add a Linux server as a Remote Media Agent for Linux (RMAL) to a Backup Exec server.

See [“About adding a Linux server as a Remote Media Agent for Linux”](#) on page 1143.

**Table Q-2** Add Remote Media Agent for Linux options

Item	Description
<b>Server name</b>	Specifies the name of the Linux server that you want to add as a Remote Media Agent for Linux.  If the Backup Exec Central Admin Server Option is installed in your environment, use the host name or fully qualified domain name of the Linux server. That is, use the name of the Linux computer that appears when you browse for backup selections. If you use the IP address, Backup Exec cannot distinguish which device path to use for jobs.

**Table Q-2** Add Remote Media Agent for Linux options (*continued*)

Item	Description
<b>Port number</b>	<p>Lists the port to use for communications between the Backup Exec server and RMAL. If you change the port number, you must edit the services file in the /etc directory on the Linux server, and update the NDMP entry.</p> <p>See <a href="#">“Changing the port for communications between the Backup Exec server and the Remote Media Agent for Linux”</a> on page 1146.</p> <p>Ensure that this port is open in any firewalls that exist between RMAL and the Backup Exec server. Use a port number that is not in use by another application or service.</p> <p>The default port is 10000.</p>
<b>Description</b>	Displays a description that you choose.
<b>Logon Account</b>	<p>Indicates the logon account for RMAL.</p> <p>The default logon account is the system logon account for the Backup Exec server.</p>
<b>Have Backup Exec use ICMP ping operations to detect the server</b>	<p>Lets the Backup Exec server use ICMP ping operations to locate the Linux server. You can turn off this option in environments where ping requests are blocked.</p> <p>This option is enabled by default.</p>
<b>Logon account</b>	<p>Indicates the Backup Exec logon account that you want to use to log on this server.</p> <p>See <a href="#">“About logon accounts”</a> on page 498.</p>

See [“About creating storage device pools for devices attached to the Remote Media Agent for Linux ”](#) on page 1146.

See [“About backing up data by using the Remote Media Agent for Linux”](#) on page 1149.

# Changing the port for communications between the Backup Exec server and the Remote Media Agent for Linux

You can change the port that Backup Exec uses to communicate with the Remote Media Agent for Linux (RMAL).

## To change the port for communications between the Backup Exec server and the Remote Media Agent for Linux

- 1 On the computer on which RMAL is installed, use a text editor to open the services file in the `/etc` directory.

For example:

```
vi /etc/services
```

- 2 Search the file for an entry that is similar to the following:  
**ndmp 10000/tcp**
- 3 Do one of the following:

If this entry exists

Change the port number to the port number that you want to use.

If this entry does not exist

Do the following in the order listed:

- At the end of the file, type `ndmp`, and then press **Tab**.
- Type the port number that you want NDMP to use, and then type `/tcp`.
- Press **Enter**.

- 4 Save the file, and then exit the editor.
- 5 Restart the Agent for Linux daemon.

See [“Starting the Remote Media Agent for Linux daemon”](#) on page 1139.

## About creating storage device pools for devices attached to the Remote Media Agent for Linux

Remote Media Agents may reside in different physical locations. To reduce network traffic and increase job performance, you can create separate storage device pools for Remote Media Agents that are located at different sites.

See [“About storage device pools”](#) on page 403.

See [“About the Tape Library Simulator Utility”](#) on page 1149.

## Editing properties for the Remote Media Agent for Linux

You can edit the properties for a Remote Media Agent for Linux (RMAL).

To edit properties for the Remote Media Agent for Linux

- 1 On the **Storage** tab, right-click a RMAL server.
- 2 Click **Details**.

See [“Remote Media Agent for Linux properties”](#) on page 1147.

## Remote Media Agent for Linux properties

You can view properties for a Remote Media Agent for Linux server (RMAL).

See [“Editing properties for the Remote Media Agent for Linux ”](#) on page 1147.

The following table lists Remote Meida Agent for Linux server properties:

**Table Q-3** Remote Media Agent for Linux properties

Item	Description
<b>Name</b>	Displays the name, IP address, or fully qualified domain name of RMAL.
<b>Port</b>	Displays the port that is used for communications between the Backup Exec server and RMAL.
<b>Backup Exec server status</b>	Displays the status of the Backup Exec server. Backup Exec server status includes Online, Pause, Unavailable, and Offline.
<b>Description</b>	Displays a description of RMAL. You can edit this description.
<b>Enable ICMP ping operations for Backup Exec to detect the Remote Media Agent</b>	Lets Backup Exec communicate with RMAL. You can turn off this option in environments where ping requests are blocked.  This option is enabled by default.

**Table Q-3** Remote Media Agent for Linux properties (*continued*)

Item	Description
Host ID	Displays the identifier number that RMAL generates.
System version	Displays the version of the operating system that runs on RMAL.
Logon account	Indicates the logon account for RMAL. Click <b>Change</b> to select or create another logon account.

## Deleting a Remote Media Agent for Linux from the Backup Exec list of servers

Use the following to delete a Remote Media Agent for Linux (RMAL) from the Backup Exec list of servers.

To delete a Remote Media Agent for Linux from a Backup Exec

- 1 On the **Storage** tab, right-click a RMAL.
- 2 Click **Yes**.

See [“Establishing trust and adding a Remote Media Agent for Linux computer to the Backup Exec list of servers”](#) on page 1140.

## Sharing a Remote Media Agent for Linux between multiple Backup Exec servers

If the Central Admin Server Option is installed, you can select Backup Exec servers to share a Remote Media Agent for Linux (RMAL) server. When you add an RMAL server, the Backup Exec server that you used to add the device is automatically selected for sharing.

See [“About sharing storage devices”](#) on page 418.

To share a Remote Media Agent for Linux between multiple Backup Exec servers

- 1 On the **Storage** tab, under **All Storage**, right-click a RMAL server that you want the Backup Exec servers to access.
- 2 Select **Share**.
- 3 Under **Server**, select the Backup Exec servers that you want to use with RMAL.

- 4 Click **OK**.
- 5 Restart the Backup Exec services on the Backup Exec servers that you selected in step 3.

## About backing up data by using the Remote Media Agent for Linux

Create a backup job for Remote Media Agent for Linux (RMAL) from the Backup Exec server.

See [“Backing up data”](#) on page 163.

See [“Editing backups”](#) on page 170.

See [“About stages”](#) on page 183.

## About restoring data by using the Remote Media Agent for Linux

Create a restore job for RMAL from the Backup Exec server.

---

**Note:** Use devices that are attached to the Backup Exec server to restore data from the tapes that other applications created. RMAL supports only Microsoft Tape Format (MTF) media.

---

See [“About searching for and restoring data”](#) on page 229.

## About the Tape Library Simulator Utility

The Tape Library Simulator Utility lets you create a virtual device on a hard disk or on any mounted volume on a Linux server. This virtual device emulates a SCSI tape library. The Remote Media Agent for Linux (RMAL) must be installed on the server.

When you run the Tape Library Simulator Utility, you are prompted for the following information:

- The number of slots that you want to allocate to this library.
- The location or path for the library.

The Tape Library Simulator Utility then creates the media for the simulated tape library. To ensure that each media has a unique name, the Tape Library Simulator

Utility creates a bar code label for each media. You cannot rename these bar code labels. However, you can add a unique media description.

The simulated tape library emulates an Advanced Intelligent Tape (AIT) media type. This media type is seldom used, so it helps you distinguish between a physical robotic library and a simulated tape library. The simulated media also has an AIT media type label.

The format of the files that are written to the simulated tape library is similar to the file format of backup-to-disk files. However, you cannot copy or move files between simulated tape libraries and backup-to-disk folders.

You can add the simulated tape library to Backup Exec device pools.

See [“About storage device pools”](#) on page 403.

To use the Tape Library Simulator Utility, you must have a minimum of 500 MB of available space on the Linux server. The available space includes hard disk space, flash drives, and USB drives. If there is not enough space, the jobs fail with an end-of-media error. You must either create available disk space or you must direct the jobs to another volume, and then start the jobs again.

A simulated tape library does not support all of the tasks that are available for physical robotic libraries.

See [“Storage operations for virtual tape libraries and simulated tape libraries”](#) on page 412.

See [“Creating a simulated tape library”](#) on page 1150.

## Creating a simulated tape library

Create a simulated tape library on a server on which RMAI is installed. You must create the simulated tape library on a hard disk or on a mounted volume.

See [“About the Tape Library Simulator Utility”](#) on page 1149.

### To create a simulated tape library

- 1 At the RMAI computer, stop the Agent for Linux daemon.  
See [“Stopping the Agent for Linux daemon”](#) on page 1103.
- 2 Navigate to the following path that contains the Tape Library Simulator Utility:

```
</opt/VRTSralus/bin>
```

For example:

```
cd /opt/VRTSralus/bin
```

- 3 Start the **mktls** utility.  
For example:  

```
./mktls
```
- 4 Select **Create a new simulated tape library**, and then press **Enter**.
- 5 Enter the appropriate information.  
See [“Simulated Tape Library options”](#) on page 1151.
- 6 Exit the utility.
- 7 Restart the Agent for Linux daemon.  
See [“Starting the Agent for Linux daemon”](#) on page 1103.
- 8 On the Backup Exec server, restart the Backup Exec services.  
See [“Starting and stopping Backup Exec services”](#) on page 511.

## Simulated Tape Library options

When you create a simulated tape library, you must provide a directory path and the number of slots for the library.

See [“Creating a simulated tape library”](#) on page 1150.

**Table Q-4** Simulated Tape Library options

Item	Description
<b>Directory Path</b>	Type the path of the directory for the simulated tape library. You can enter up to 512 characters. If the path does not exist, the Tape Library Simulator Utility creates it.
<b>Number of Slots</b>	Select the number of slots for this simulated tape library. The number of slots can range from 1 to 50. The default number of slots is 20.

See [“Viewing simulated tape libraries properties”](#) on page 1151.

## Viewing simulated tape libraries properties

You can use the Symantec Tape Library Simulator Utility to view information about a simulated tape library and its contents.

**To view simulated tape library properties**

- 1 On the RMAI computer, stop the Agent for Linux daemon.  
See “[Stopping the Agent for Linux daemon](#)” on page 1103.
- 2 Navigate to the following directory that contains the Tape Library Simulator Utility:  

```
/opt/VRTSralus/bin
```

For example:

```
cd /opt/VRTSralus/bin
```
- 3 Start the **mktls** utility.  
For example:  

```
./mktls
```
- 4 Select **View an existing simulated tape library**.
- 5 Move your cursor to the simulated tape library that you want to view, and then press **Enter**.
- 6 Press **Enter** again to view the simulated tape library properties.  
See “[Simulated tape library properties](#)” on page 1152.
- 7 Type **Q** to exit the utility.
- 8 Restart the Agent for Linux daemon.  
See “[Starting the Agent for Linux daemon](#)” on page 1103.

## Simulated tape library properties

You can view the properties of a simulated tape library.

See “[Viewing simulated tape libraries properties](#)” on page 1151.

**Table Q-5** Simulated tape library properties

Item	Description
<b>Number of drives</b>	Displays the number of drives for this simulated tape library.  A simulated tape library can have only drive. This drive is not configurable.

**Table Q-5** Simulated tape library properties (*continued*)

Item	Description
<b>Number of slots</b>	Displays the number of slots for this simulated tape library. The number of slots can range from 1 to 50. The default number of slots is 20.
<b>Tape capacity</b>	Displays the tape capacity. The default capacity is 100 gigabytes.
<b>Directory path</b>	Displays the directory path where the simulated tape library exists.

## Deleting a simulated tape library

You can use the Tape Library Simulator Utility to delete a simulated tape library. You must then manually delete the content of the simulated tape library files, and then delete the directories that contain these files.

### To delete a simulated tape library

- 1 At the RMA computer stop the Agent for Linux daemon.  
See [“Stopping the Agent for Linux daemon”](#) on page 1103.
- 2 Navigate to the following directory that contains the Tape Library Simulator:  
`/opt/VRTSralus/bin/`  
For example:  

```
cd /opt/VRTSralus/bin/
```
- 3 Start the **mktls** utility:  
For example:  

```
./mktls
```
- 4 Select **View an existing simulated tape library**.
- 5 Select the simulated tape library that you want to delete.
- 6 When you are prompted, delete the simulated tape library.
- 7 Exit the utility.
- 8 Restart the Agent for Linux daemon.  
See [“Starting the Agent for Linux daemon”](#) on page 1103.

- 9 Find the simulated tape library files, and then manually delete them.  
See [“About the Tape Library Simulator Utility”](#) on page 1149.
- 10 On the Backup Exec server, restart the Backup Exec services when it is convenient.  
See [“Starting and stopping Backup Exec services”](#) on page 511.

## Managing simulated tape libraries from the command line

You can use the command line to create a simulated tape library. Create a simulated tape library on a hard disk or on any mounted volume on the RMAL computer. From the command line, you can also view and delete simulated tape libraries.

### To manage simulated tape libraries from the command line

- 1 At the RMAL computer stop the Agent for Linux daemon.  
See [“Stopping the Agent for Linux daemon”](#) on page 1103.
- 2 Navigate to the following directory that contains the Tape Library Simulator Utility:  

```
/opt/VRTSralus/bin
```

For example:

```
cd /opt/VRTSralus/bin
```
- 3 Start the **mktls** utility with the appropriate parameter switches.  
See [“Command line switches for the Tape Library Simulator Utility”](#) on page 1154.
- 4 Start the Agent for Linux daemon.  
See [“Starting the Agent for Linux daemon”](#) on page 1103.

## Command line switches for the Tape Library Simulator Utility

You can use command line switches to manage simulated tape libraries. For example, the following command line creates a simulated tape library with 10 slots that is located at /TLS2/Testing.

```
./mktls -s10 -p/TLS2/Testing
```

See [“Managing simulated tape libraries from the command line”](#) on page 1154.

**Table Q-6** Command line switches for the Tape Library Simulator Utility

Switch	Description
-p<path>	Specifies the path to the directory for the simulated tape library. If the path does not exist, the utility creates it. The maximum path size is 512 characters.
-s<number of slots>	Specifies the number of slots for this simulated tape library. The number of slots can range from one to 50. The default number is 20.
-r	Prevents the information from displaying.
-l	Lists the simulated tape libraries that exist for RMAL.
-d -p<path>	Specifies the path of the simulated tape library that you want to delete.
-h	Displays the online Help.

## Troubleshooting the Remote Media Agent for Linux

If there are issues with Remote Media Agent for Linux (RMAL), review the following questions and answers.

**Table Q-7** Troubleshooting the RMAL

Question	Answer
RMAL does not detect my attached device. What should I do?	<p>First, ensure that Backup Exec and RMAL support the device.</p> <p>You can find a list of compatible devices at the following URL:</p> <p><a href="http://entsupport.symantec.com/umi/V-269-2">http://entsupport.symantec.com/umi/V-269-2</a></p> <p>If the device is listed on the hardware compatibility list, ensure the following:</p> <ul style="list-style-type: none"> <li>■ The operating system detects the device</li> <li>■ The device is listed in <code>/proc/scsi/scsi</code></li> </ul> <p>If the operating system can detect the device, ensure that the device is listed in <code>/etc/VRTSralus/TILDBG.TXT</code>.</p>

**Table Q-7** Troubleshooting the RMAL (*continued*)

Question	Answer
<p>My Backup Exec server does not display the devices that are attached to my Remote Media Agent. What should I do?</p>	<p>Try the following procedures:</p> <ul style="list-style-type: none"> <li>■ Ensure that the Agent for Linux daemon is running. If it is not running, start the daemon, and check that power for the server is enabled, and that all cables are properly attached.</li> <li>■ Ensure that RMAL properties are set to the correct port, and that ICMP ping operations are enabled.</li> <li>■ Ensure that the Backup Exec services are restarted after a Remote Media Agent is added to the Backup Exec server. The available devices should be displayed under RMAL node.</li> </ul> <p>See <a href="#">“Editing properties for the Remote Media Agent for Linux”</a> on page 1147.</p> <p>See <a href="#">“Starting the Agent for Linux daemon”</a> on page 1103.</p>
<p>Why don't my remote devices appear in any of the storage device pools that are created by Backup Exec?</p>	<p>By default, Backup Exec does not include remote devices in the storage device pools it creates. Symantec recommends that you create a separate storage device pool for the devices that are attached to each Remote Media Agent.</p> <p>See <a href="#">“About creating storage device pools for devices attached to the Remote Media Agent for Linux”</a> on page 1146.</p>

**Table Q-7** Troubleshooting the RMAL (*continued*)

Question	Answer
<p>RMAL won't run on the remote computer. What should I do?</p>	<p>Ensure that RMAL is installed on a supported version of Linux.</p> <p>You can find a list of compatible operating systems, platforms, and applications at the following URL:</p> <p><a href="http://entsupport.symantec.com/umi/V-269-1">http://entsupport.symantec.com/umi/V-269-1</a></p> <p>If you install RMAL to an unsupported version of Linux, RMAL is unavailable for use. You cannot create the jobs that run on the devices that are attached to the Linux server. However, you can back up the Linux server by using the Agent for Linux component. This component is installed with RMAL.</p> <p>To use the Agent for Linux component to back up the Linux server, do the following:</p> <ul style="list-style-type: none"> <li>■ Edit the <code>ralus.cfg</code> file.</li> <li>■ In the string <code>Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RMAL\DisableRMAL=0</code>, change 0 to 1. See “<a href="#">Editing configuration options for Linux computers</a>” on page 1083.</li> <li>See “<a href="#">Running the begather utility to troubleshoot Backup Exec components on Linux servers</a>” on page 670.</li> </ul>
<p>I cannot load RMAL. When I attempt to load RMAL in console mode, <code>/beremote --log-console</code> shows the following message:</p> <p><b>Error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory.</b></p> <p>What should I do?</p>	<p>This error indicates that the <b>libstdc++.so.5</b> library is not in the <code>/usr/lib</code> directory. This library is necessary to let RMAL start and function. To resolve this issue, install the <b>libstdc++.so.5</b> package. You can install this package from the media on which your copy of Linux was provided. Or, you can run the following command from a computer that has Internet access:</p> <pre>apt-get install libstdc++5</pre> <p>For SUSE Linux Enterprise Server 11, run the following command:</p> <pre>zypper install libstdc++5</pre>



# Symantec Backup Exec Storage Provisioning Option

This appendix includes the following topics:

- [About the Storage Provisioning Option](#)
- [Requirements for the Storage Provisioning Option](#)
- [Requirements for the Storage Provisioning Option in a CASO environment](#)
- [About installing the Storage Provisioning Option](#)
- [Viewing storage array components in Backup Exec](#)
- [About using the Configure Storage Wizard with the Storage Provisioning Option](#)
- [Configuring a storage array by using the Configure Storage Wizard](#)
- [Viewing properties for a storage array and its physical disks](#)
- [About the Any Virtual Disk Storage device pool in the Storage Provisioning Option](#)
- [About virtual disks in the Storage Provisioning Option](#)
- [About hot spares in the Storage Provisioning Option](#)
- [Detecting a new storage array](#)
- [Renaming a virtual disk or storage array](#)
- [About identifying the physical disks of a virtual disk](#)
- [Troubleshooting the Storage Provisioning Option](#)

## About the Storage Provisioning Option

The Storage Provisioning Option (SPO) lets you configure, manage, and monitor storage arrays that are attached to the Backup Exec server.

---

**Note:** If you use a Dell DL Appliance, do not use this appendix. See the *Dell™ PowerVault™ DL Backup to Disk Appliance and the Symantec Backup Exec Storage Provisioning Option* documentation that Dell provides with the appliance.

---

**Table R-1** Features of the Storage Provisioning Option

Feature	Description
Discovery of new storage arrays, physical disks, and virtual disks	Backup Exec can discover new storage arrays, physical disks, and the virtual disks that you add to a storage array. If you create virtual disks by using storage array vendor tools or the Microsoft Storage Manager for SANs utility, Backup Exec also detects those virtual disks.
A wizard to help you configure a storage array for use with Backup Exec	Backup Exec provides the <b>Configure Storage Wizard</b> to help you configure virtual disks on a storage array. The virtual disks are added to the <b>Any virtual disk storage</b> device pool. Backup Exec then uses the virtual disks in the device pool as destination devices for jobs.
Trend analysis of disk space usage	Backup Exec collects statistical information to predict the amount of disk space that is required on the storage arrays. Alerts are sent if the available disk space does not meet the predicted amount of disk space that is needed.  See <a href="#">“About storage trending for disk storage and virtual disks”</a> on page 306.
Alerts for low disk space	Backup Exec sends an alert when available disk space reaches each of three thresholds that you set for a virtual disk.

See [“Requirements for the Storage Provisioning Option”](#) on page 1161.

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

# Requirements for the Storage Provisioning Option

Do the following before you install the Backup Exec Storage Provisioning Option (SPO):

- Attach any storage arrays to the Backup Exec server.
- Install the storage array vendor's VDS hardware provider on the Backup Exec server.

See [“How to choose the location for CASO storage and media data ”](#) on page 999.

See [“Requirements for the Storage Provisioning Option in a CASO environment”](#) on page 1161.

See [“About installing the Storage Provisioning Option”](#) on page 1161.

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

## Requirements for the Storage Provisioning Option in a CASO environment

The following are required to run the Storage Provisioning Option (SPO) in a Central Admin Server Option (CASO) environment:

- SPO must be installed on the Backup Exec server to which the storage array is attached.  
If the storage array is attached to a managed Backup Exec server, install SPO on that managed Backup Exec server. You do not need to install SPO on the central administration server if the storage array is not attached to it.
- The Central Admin Server Option must use a centralized database.  
See [“About CASO catalog locations”](#) on page 1016.

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

See [“About installing the Storage Provisioning Option”](#) on page 1161.

## About installing the Storage Provisioning Option

Install SPO on a local Backup Exec server as a separate add-on component of Backup Exec.

You can install SPO when you upgrade from a previous version of Backup Exec.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

See [“Requirements for the Storage Provisioning Option in a CASO environment”](#) on page 1161.

## Viewing storage array components in Backup Exec

After you install the Storage Provisioning Option (SPO), storage arrays appear in the **All Storage** view. After you use the **Configure Storage Wizard** to configure the storage array, virtual disks appear under the storage array to which they belong.

You can also view the properties of the physical disks that comprise a storage array's configured virtual disk or disks by viewing the details of the storage array itself.

### To view storage array components in Backup Exec

- 1 On the **Storage** tab, under **All Storage**, expand a storage array.
- 2 View the storage array components.

See [“Properties for a storage array and its physical disks”](#) on page 1165.

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

See [“Configuring a storage array by using the Configure Storage Wizard”](#) on page 1163.

## About using the Configure Storage Wizard with the Storage Provisioning Option

The Storage Provisioning Option (SPO) uses the Backup Exec **Configure Storage Wizard** to help you configure virtual disks in a storage array.

With the **Configure Storage Wizard**, you can:

- Specify a virtual disk size, and then let the storage array automatically choose the physical disks for the virtual disk's disk group.

With this option, the storage array attempts to spread the required disk space for the virtual disk equally across each physical disk it selects.

When you specify a virtual disk size, the **Configure Storage Wizard** presents you with the total amount of disk space available to create a virtual disk. The total available disk space is derived from the physical disks that are present. You can use the entire space to create one virtual disk, or you can specify

smaller amounts of space and create multiple virtual disks. Each virtual disk you create is based on the amount of disk space you enter. To create multiple virtual disks, run the wizard multiple times, until you have the virtual disks you want, or until you exhaust the disk space.

- Create a disk group by manually selecting the physical disks, from which you can then choose the number of virtual disks to create.

With this option, the **Configure Storage Wizard** lets you customize the entire virtual disk creation process on the storage array.

- Configure hot spares.

You can also use this wizard to add or change hot spares for the disk groups that are already configured.

In addition, you can also use the **Configure Storage Wizard** to configure a virtual disk as a deduplication storage folder. Deduplication reduces the disk storage and the network bandwidth that is used for backups by storing and sending only unique data.

---

**Note:** Deduplication may not be available for the storage array if a deduplication storage folder presently exists on the Backup Exec server. Only one deduplication storage folder per Backup Exec server is supported. You can delete the existing deduplication storage folder and then rerun the **Configure Storage Wizard** to enable deduplication on the storage array.

---

When the wizard completes, it runs a utility job named Configure Storage Array. This utility job creates the virtual disks that you specified. Then, Backup Exec adds the virtual disks to a device pool named **Any virtual disk storage**. You can submit jobs to the **Any virtual disk storage** device pool, to the storage array, or to a specific virtual disk.

See [“Configuring a storage array by using the Configure Storage Wizard”](#) on page 1163.

See [“Requirements for the Deduplication Option”](#) on page 755.

See [“Configuring a storage array by using the Configure Storage Wizard”](#) on page 1163.

## Configuring a storage array by using the Configure Storage Wizard

Use the **Configure Storage Wizard** to configure a storage array for use with the Backup Exec Storage Provisioning Option (SPO).

Backup Exec then submits a Configure Storage Array job to create the virtual disks.

---

**Note:** In a Central Admin Server Option (CASO) environment, run the **Configure Storage Wizard** from the central administration server. You can run the **Configure Storage Wizard** for any managed Backup Exec server that has SPO installed. Managed Backup Exec servers can share a single storage array but cannot share a virtual disk on a storage array.

---

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

See [“Viewing storage array components in Backup Exec”](#) on page 1162.

**To configure a storage array by using the Configure Storage Wizard**

- 1 On the **Storage** tab, click **Configure Storage**.
- 2 Do one of the following:

In a non-CASO environment

Do the following in the order listed.

- Click **Disk-based Storage**, and then click **Next**.
- Click **Storage array**.
- Follow the on-screen directions.

In a CASO environment

Do the following in the order listed:

- Select a Backup Exec server for which you want to configure storage.
- Click **Disk-based Storage**, and then click **Next**.
- Click **Storage array**.
- Follow the on-screen directions.

## Viewing properties for a storage array and its physical disks

Properties provide detailed information for the storage array and its physical disks.

**To view properties for storage arrays**

1 On the **Storage** tab, select a storage array.

2 Right-click the storage array, and then click **Details**.

See “[Properties for a storage array and its physical disks](#)” on page 1165.

## Properties for a storage array and its physical disks

Properties provide detailed information for the storage array and its physical disks.

See “[Viewing properties for a storage array and its physical disks](#)” on page 1164.

**Table R-2** Properties for storage arrays

Item	Description
<b>Name</b>	Displays the default name that Backup Exec assigns to the storage array. The default name is Storage array x, where x is a number that increments each time that you add a storage array.  You can change the default name of the storage array.  See “ <a href="#">Renaming a virtual disk or storage array</a> ” on page 1193.
<b>Description</b>	Displays a description that you use to describe a storage array.

**Table R-2** Properties for storage arrays (*continued*)

Item	Description
<b>State</b>	<p>Indicates the current state of the storage array.</p> <p>States are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Pause</b> The storage array is temporarily stopped. You can pause a storage array to perform maintenance activities. Active jobs are not affected if they start before the storage array is paused.</li> <li>■ <b>Enable</b> The storage array is available for use with Backup Exec. If the storage array is not enabled, it is available for use with other applications.</li> <li>■ <b>Online</b> The storage array is available for use.</li> <li>■ <b>Offline</b> Backup Exec cannot access the storage array. You can click this check box to try to bring the storage array online.</li> <li>■ <b>Failed</b> Backup Exec cannot access the storage array.</li> </ul>
<b>Identification</b>	<p>Displays the information that the vendor provides to assist you with identification of the attached storage array hardware. Refer to the vendor documentation that is supplied with the storage array for information.</p>
<b>Hardware name</b>	<p>Displays the name that the storage array hardware or the vendor hardware provider assigns.</p>
<b>Hot spare disk is configured</b>	<p>Indicates whether or not a hot spare disk has been configured for the storage array.</p>

**Table R-2** Properties for storage arrays (*continued*)

Item	Description
<b>Total backup storage</b>	<p>Displays the expected amount of total raw capacity of all of the physical disks in the storage array.</p> <p>If a storage array can read the total capacity, then it appears in this field. Otherwise, Backup Exec estimates the total capacity.</p>
<b>Used capacity</b>	<p>Displays the amount of backup storage capacity presently being used.</p>
<b>Connection type</b>	<p>Shows the location of the storage array in use with the Backup Exec server. <b>Local</b> appears when the storage array is physically connected to the Backup Exec server.</p>
<b>Backup Exec service restarted needed</b>	<p>Indicates if the Backup Exec services must be restarted to apply any changes that are made to this device.</p>
<b>Hardware status</b>	<p>Indicates the hardware status.</p> <p>The values for hardware status are as follows:</p> <ul style="list-style-type: none"><li>■ <b>OK</b> The storage array is online.</li><li>■ <b>Offline</b> The storage array and the virtual disks on the storage array are offline. Backup Exec cannot access them.</li><li>■ <b>Unknown</b> The status of the storage array cannot be determined.</li></ul> <p>Refer to the vendor documentation and management software that are supplied with the storage array. After the storage array is brought online, the virtual disks are automatically brought online.</p>

**Table R-2** Properties for storage arrays (*continued*)

Item	Description
<b>Hardware health</b>	<p>Indicates the hardware health.</p> <p>Values for hardware health are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>OK</b> The storage array is online.</li> <li>■ <b>Warning</b> The storage array may fail or produce errors, but it is currently operational. The storage array and the virtual disks on the storage array are offline. Backup Exec cannot access them.</li> <li>■ <b>Critical</b> The storage array has failed. The storage array and the virtual disks on the storage array are offline. Backup Exec cannot access them.</li> </ul> <p><b>Unknown</b> The health of the storage array cannot be determined.</p> <p>Refer to the vendor documentation and management software that are supplied with the storage array. After the storage array is brought online, the virtual disks are automatically brought online.</p>
<b>Total capacity</b>	<p>Displays the expected amount of total raw capacity of all the of the physical disks in the storage array.</p> <p>If a storage array can read the total capacity, then it appears in this field. Otherwise, Backup Exec estimates the total capacity.</p>
<b>Unconfigured capacity</b>	<p>Displays the expected amount of total raw capacity of all of the unconfigured physical disks in the storage array.</p>
<b>Unused configured capacity</b>	<p>Displays the amount of total raw capacity of all of the configured physical disks in the storage array.</p>
<b>Enclosure</b>	<p>Identifies the enclosure that the physical disk is in.</p>

**Table R-2** Properties for storage arrays (*continued*)

Item	Description
<b>Slot</b>	Identifies the slot that the physical disk occupies.
<b>Capacity</b>	Displays the total amount of available disk space on the physical disk in this slot.
<b>State</b>	<p>Displays the hardware status of a physical disk.</p> <p>Values for hardware status are as follows:</p> <ul style="list-style-type: none"><li>■ <b>OK</b> The physical disk is online.</li><li>■ <b>Offline</b> The physical disk is offline. The virtual disks that use this physical disk may also be offline. Backup Exec cannot access them.</li><li>■ <b>Failed</b> The physical disk has failed. The virtual disks that use this physical disk may also fail. Backup Exec cannot access the virtual disks. If hot spares are configured, the virtual disk is automatically rebuilt. If your storage array does not support an automatic rebuild capability, you must use vendor tools to perform a manual rebuild of the virtual disks. Refer to your vendor documentation for the storage array for more information.</li><li>■ <b>Not configured</b> The drive is not configured as a virtual disk.</li></ul> <p>To troubleshoot issues, refer to the vendor documentation and management software that are supplied with the storage array.</p>

**Table R-2** Properties for storage arrays (*continued*)

Item	Description
<b>Status</b>	<p>Displays the status of a physical disk within an enclosure.</p> <ul style="list-style-type: none"> <li>■ <b>OK</b> The physical disk is online.</li> <li>■ <b>Offline</b> The physical disk is offline. The virtual disks that use this physical disk may also be offline. Backup Exec cannot access them.</li> <li>■ <b>Failed</b> The physical disk has failed. The virtual disks that use this physical disk may also fail. Backup Exec cannot access the virtual disks.</li> <li>■ <b>Unknown</b> The status of the physical disk cannot be determined.</li> </ul>
<b>Health</b>	<p>Displays the hardware health of a physical disk.</p> <p>Values for hardware health are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>OK</b> The physical disk is online.</li> <li>■ <b>Warning</b> The physical disk may fail or produce errors, but it is currently operational.</li> <li>■ <b>Critical</b> The physical disk may fail. You should replace the physical disk.</li> <li>■ <b>Unknown</b> The health of the physical disk cannot be determined.</li> </ul> <p>To troubleshoot issues, refer to the vendor documentation and management software that are supplied with the storage array.</p>

# About the Any Virtual Disk Storage device pool in the Storage Provisioning Option

After you install the Storage Provisioning Option (SPO), Backup Exec adds the **Any virtual disk storage** device pool to the list of storage device pools. The **Any virtual disk storage** device pool contains all virtual disks from all storage arrays on all computers in the Backup Exec environment.

See [“About the Configure Storage wizard”](#) on page 145.

See [“About storage device pools”](#) on page 403.

## About virtual disks in the Storage Provisioning Option

A virtual disk is a logical disk that you create on a storage array to provide virtual storage to the Backup Exec server.

You can use any of the following to create a virtual disk:

- The Configure Storage Wizard
- The management tools that the vendor of the storage array provides
- The Microsoft Storage Manager for SANs management tool

If you create a virtual disk with a tool other than the **Configure Storage Wizard**, you must configure the virtual disk for use with Backup Exec. After you configure a virtual disk, Backup Exec uses it as a destination device for jobs. Backup Exec automatically adds configured virtual disks to the **Any virtual disk storage** device pool.

See [“Configuring a virtual disk on a storage array”](#) on page 1173.

In the **Configure Storage Wizard**, you specify the number of virtual disks to create from the physical disks that are in the storage array. The Backup Exec server cannot access the physical disks. The Backup Exec server can access only the virtual disks that you create.

Backup Exec uses a configured virtual disk in the same manner in which it uses a disk storage device.

Backup Exec does not assign a drive letter to the virtual disk. You cannot browse for a virtual disk or access it from a command prompt. Since you cannot browse to the virtual disk, you cannot back it up with Backup Exec. Symantec recommends that you create a duplicate backup data job to move the data from the virtual disk to another device. For example, you can move the data to a tape device or to another virtual disk on a separate storage array.

Backup Exec provides three low disk space thresholds for the virtual disks. As available disk space reaches each threshold, Backup Exec sends an alert. When the available disk space on the virtual disk reaches the third threshold, the alert warns you to create more disk space immediately.

See [“Editing default options for a virtual disk on a storage array”](#) on page 1173.

---

**Note:** You cannot share a virtual disk between two computers.

---

Virtual disks can have the following states:

**Table R-3** States for virtual disks

States for virtual disks	Icon	Description
<b>Configured</b>		The virtual disk is in use as a device or as a hot spare.
<b>Online</b>		The virtual disk is online.
<b>Not configurable</b>		The virtual disk cannot be configured because it is in a bad state, or it has failed.
<b>Not configured</b>		The virtual disk is available for configuration but has not yet been configured.
<b>Offline</b>		The virtual disk is offline. Backup Exec cannot access it.

**Table R-3** States for virtual disks (*continued*)

States for virtual disks	Icon	Description
<b>Disabled</b>		The virtual disk is disabled. Backup Exec cannot access it.
<b>Paused</b>		The virtual disk is paused.

See [“Viewing storage array components in Backup Exec”](#) on page 1162.

See [“Editing default options for a virtual disk on a storage array”](#) on page 1173.

See [“Viewing properties for unconfigured virtual disks on a storage array”](#) on page 1174.

See [“About the Any Virtual Disk Storage device pool in the Storage Provisioning Option”](#) on page 1171.

## Editing default options for a virtual disk on a storage array

You can set the default options that apply to individual virtual disks.

See [“Editing properties of virtual disks on storage arrays”](#) on page 1180.

### To edit default options for a virtual disk on a storage array

- 1 On the **Storage** tab, select a storage array.
- 2 Expand the storage array, and then double-click the virtual disk that you want to view.
- 3 Change the information as appropriate.

See [“Properties for virtual disks on storage arrays”](#) on page 1180.

## Configuring a virtual disk on a storage array

If you create a virtual disk with a tool other than Backup Exec, then you must configure the virtual disk to use it with Backup Exec. Backup Exec can only use configured virtual disks as destination devices for jobs. When you configure the virtual disk, Backup Exec submits a job named **Configure Disk Storage**. When the

job completes successfully, the virtual disk is configured and added to the **Any virtual disk storage** device pool.

---

**Note:** Be careful when you select an unconfigured virtual disk. An unconfigured virtual disk may be in use as a Microsoft SQL Server database, an Exchange database, or a boot disk.

---

#### To configure a virtual disk on a storage array

- 1 On the **Storage** tab, select a storage array.
- 2 Expand the storage array, and then select the unconfigured virtual disk.
- 3 On the **Storage Array Operations** group, click **Configure Virtual Disk**.
- 4 Follow the on-screen instructions.

See [“Editing properties of virtual disks on storage arrays”](#) on page 1180.

## Viewing properties for unconfigured virtual disks on a storage array

You can view the properties of an unconfigured virtual disk on a storage array.

---

**Note:** You must configure a virtual disk before Backup Exec can use it as a destination device for jobs.

---

See [“Configuring a virtual disk on a storage array”](#) on page 1173.

#### To view properties for unconfigured virtual disks on a storage array

- 1 On the **Storage** tab, select a storage array.
- 2 Expand a storage array, and then select an unconfigured virtual disk.
- 3 Right-click the unconfigured virtual disk, and then click **Details**.

See [“Properties for unconfigured virtual disks on storage arrays”](#) on page 1174.

## Properties for unconfigured virtual disks on storage arrays

Properties for unconfigured virtual disks provide information on the name, status, and health of the disks.

See [“Viewing properties for unconfigured virtual disks on a storage array”](#) on page 1174.

**Table R-4** Properties for unconfigured virtual disks on storage arrays

Item	Description
<b>Name</b>	<p>Displays the default name that Backup Exec assigns to the unconfigured virtual disk.</p> <p>The default name is Virtual disk x, where x is a number that increments each time that you create a virtual disk.</p> <p>You can change the default name of the virtual disk.</p> <p>See <a href="#">“Renaming a virtual disk or storage array”</a> on page 1193.</p>
<b>Description</b>	<p>Displays a description of the virtual disk.</p> <p>You can edit this field.</p>
<b>State</b>	<p>Indicates the current state of the virtual disk.</p> <p>States are as follows:</p> <ul style="list-style-type: none"><li>■ <b>Pause</b> The virtual disk is temporarily stopped. You can pause a virtual disk to perform maintenance activities. Active jobs are not affected if they start before the virtual disk is paused.</li><li>■ <b>Enable</b> The virtual disk is available for use with Backup Exec. If the virtual disk is not enabled, it is available for use with other applications.</li><li>■ <b>Online</b> The virtual disk is available for use.</li><li>■ <b>Offline</b> Backup Exec cannot access the virtual disk. You can click this check box to try to bring the virtual disk online.</li><li>■ <b>Failed</b> Backup Exec cannot access the virtual disk.</li><li>■ <b>Not configured</b> The virtual disk has not been configured. You can configure the virtual disk by clicking <b>Configure Virtual Disk</b> in the <b>Storage Array Operations</b> group.</li></ul>

**Table R-4** Properties for unconfigured virtual disks on storage arrays  
*(continued)*

Item	Description
<b>Hardware name</b>	Displays the name that you assign to a virtual disk if you use a vendor-specific tool to create the virtual disk.
<b>Hardware status</b>	<p>Displays the hardware status.</p> <p>Values for the hardware status are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>OK</b> The unconfigured virtual disk is online.</li> <li>■ <b>Offline</b> The unconfigured virtual disk is offline.</li> <li>■ <b>Failed</b> The unconfigured virtual disk has failed.</li> <li>■ <b>Unknown</b> The status of the hardware cannot be determined.</li> </ul> <p>See your vendor's documentation for more information.</p>
<b>Hardware health</b>	<p>Displays the hardware health.</p> <p>Values for the hardware health are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>OK</b> The unconfigured virtual disk is online.</li> <li>■ <b>Warning</b> The unconfigured virtual disk may fail or produce errors, but it is currently operational.</li> <li>■ <b>Critical</b> The unconfigured virtual disk has failed.</li> <li>■ <b>Unknown</b> The status of the hardware cannot be determined.</li> </ul> <p>See your vendor's documentation for more information.</p>

**Table R-4** Properties for unconfigured virtual disks on storage arrays  
*(continued)*

<b>Item</b>	<b>Description</b>
<b>Disk classification</b>	

**Table R-4** Properties for unconfigured virtual disks on storage arrays  
*(continued)*

Item	Description
	<p>Displays the type of disk group that the unconfigured virtual disk is on.</p> <p>Disk classifications are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Simple (RAID 0)</b> A single physical disk, no striping, or parity. No redundancy.</li> <li>■ <b>Span</b> A set of multiple physical disks that are concatenated together. No striping or parity. No redundancy.</li> <li>■ <b>Stripe</b> A set of multiple physical disk extents with data striped across the physical disks. No redundancy.</li> <li>■ <b>Mirror (RAID 1)</b> A pair or multiple pairs of physical disks with the same data written to each physical disk of the pair. Provides for data redundancy.</li> <li>■ <b>Stripe with parity (RAID 5 or RAID 6)</b> Three or more physical disks with data striped across the physical disks, with one disk's worth of space that is used for parity. Provides for data redundancy.</li> <li>■ <b>Unknown</b></li> </ul> <p>Backup Exec creates only physical disk groups with a disk classification of Stripe with parity (RAID 5/RAID 6). If another disk classification appears, the disk group was created with a vendor-supplied tool other than the Storage Provisioning Option (SPO).</p> <p>Additional disk classifications may appear, including the following:</p> <ul style="list-style-type: none"> <li>■ <b>RAID-10</b> Implements striping over mirroring technology.</li> <li>■ <b>RAID-50</b> Implements a striped (RAID 0) array that is striped across a RAID 5 array.</li> </ul>

**Table R-4** Properties for unconfigured virtual disks on storage arrays  
(continued)

Item	Description
	<ul style="list-style-type: none"><li>■ <b>RAID-60</b> Implements a combination of multiple RAID 6 sets with RAID 0 (striping)</li></ul> See your vendor documentation for more information about RAID technologies.
<b>Total capacity</b>	Displays the total amount of storage space that is available on the virtual disk.  If the virtual disk is not configured, the value shown in this field is 0.
<b>Total backup storage</b>	Displays the expected amount of total raw capacity of all of the physical disks in the storage array.  If a storage array can read the total capacity, then it appears in this field. Otherwise, Backup Exec estimates the total capacity.  If the virtual disk is not configured, this field is empty.
<b>Used capacity</b>	Displays the amount of raw capacity of all of the physical disks that are used in the storage array. Backup Exec calculates used capacity by subtracting available capacity from total capacity.  If the virtual disk is not configured, this field is empty.
<b>Amount of data written</b>	Displays the amount of data that has been written to the disk. The amount of data written may differ from the used capacity due to the effects of data compression. Data compression tends to increase the amount of data written when compared to used capacity.  If the virtual disk is not configured, this field is empty.

**Table R-4** Properties for unconfigured virtual disks on storage arrays  
*(continued)*

Item	Description
<b>Available capacity</b>	<p>Displays the amount of expected raw capacity on the disk that remains unused. Available capacity is calculated by subtracting the amount of reserved disk space on the drive from the drive's total amount of space.</p> <p>If the virtual disk is not configured, the value shown in this field is 0.</p>
<b>Compression ratio</b>	<p>Displays the ratio of bytes written to used capacity. Compression ratio will show the overall effect that data compression and media flaws are having on the amount of data that is being stored on the virtual disk.</p> <p>If the virtual disk is not configured, this field is empty.</p>

## Editing properties of virtual disks on storage arrays

You can edit properties for a virtual disk on a storage array.

### To edit properties of virtual disks on storage arrays

- 1 On the **Storage** tab, select a storage array.
- 2 Expand the storage array, and then select the virtual disk on which you want to edit properties.
- 3 Right-click the virtual disk, and then click **Details**.
- 4 Edit the properties as appropriate.

See [“Properties for virtual disks on storage arrays”](#) on page 1180.

## Properties for virtual disks on storage arrays

Properties provide information about virtual disks on storage arrays.

See [“Editing properties of virtual disks on storage arrays”](#) on page 1180.

**Table R-5** Properties for virtual disks on storage arrays

Item	Description
<b>Name</b>	<p>Displays the default name that Backup Exec assigns to the virtual disk.</p> <p>The default name is Virtual disk x, where x is a number that increments each time that you create a virtual disk.</p> <p>You can change the default name of the virtual disk.</p> <p>See <a href="#">“Renaming a virtual disk or storage array”</a> on page 1193.</p>
<b>Description</b>	Displays a description of the virtual disk.
<b>State</b>	<p>Displays the current status of the virtual disk.</p> <p>Statuses for a virtual disk are as follows:</p> <ul style="list-style-type: none"><li>■ <b>Pause</b> The virtual disk is temporarily stopped.</li><li>■ <b>Enable</b> The virtual disk is available for use with Backup Exec. If the virtual disk is disabled, it is available for use with other applications. Backup Exec does not monitor the low disk space thresholds for a disabled virtual disk.</li><li>■ <b>Online</b> The virtual disk is available for use.</li><li>■ <b>Offline</b> Backup Exec cannot access the virtual disk. You can check <b>Offline</b> to try to bring the storage array online.</li></ul>
<b>Hardware name</b>	Displays the name that the storage array hardware or the vendor hardware provider assigns.

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Hardware status</b>	<p>Displays the hardware status.</p> <p>Values for the hardware status are as follows:</p> <ul style="list-style-type: none"><li>■ <b>OK</b> The virtual disk is online.</li><li>■ <b>Offline</b> The virtual disk is offline. Backup Exec cannot access it. To bring the virtual disk online, refer to the vendor documentation and management software that are supplied with the storage array.</li><li>■ <b>Failed</b> The virtual disk has failed. Backup Exec cannot access it. To troubleshoot the issue, refer to the vendor documentation and management software that are supplied with the storage array. After the issue is resolved, the virtual disk is automatically brought online.</li></ul> <p><b>Unknown</b> The status of the hardware cannot be determined.</p> <p>See your vendor's documentation for more information.</p>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Hardware health</b>	<p>Displays the hardware health.</p> <p>Values for the hardware health are as follows:</p> <ul style="list-style-type: none"><li>■ <b>OK</b> The virtual disk is online.</li><li>■ <b>Warning</b> The virtual disk may fail or produce errors, but it is currently operational.</li><li>■ <b>Critical</b> The virtual disk has failed. Backup Exec cannot access it. To troubleshoot the issue, refer to the vendor documentation and management software that are supplied with the storage array.</li><li>■ <b>Unknown</b> The status of the hardware health cannot be determined.</li></ul> <p>See your vendor's documentation for more information.</p>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Disk classification</b>	

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
	<p>Displays the type of disk group that the virtual disk is on.</p> <p>Disk classifications are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Simple (RAID 0)</b> A single physical disk, no striping, or parity. No redundancy.</li> <li>■ <b>Span</b> A set of multiple physical disks that are concatenated together. No striping or parity. No redundancy.</li> <li>■ <b>Stripe</b> A set of multiple physical disk extents with data striped across the physical disks. No redundancy.</li> <li>■ <b>Mirror (RAID 1)</b> A pair or multiple pairs of physical disks with the same data written to each physical disk of the pair. Provides for data redundancy.</li> <li>■ <b>Stripe with parity (RAID 5 or RAID 6)</b> Three or more physical disks with data striped across the physical disks, with one disk's worth of space that is used for parity. Provides for data redundancy.</li> <li>■ <b>Unknown</b></li> </ul> <p>Backup Exec creates only physical disk groups with a disk classification of Stripe with parity (RAID 5/RAID 6). If another disk classification appears, the disk group was created with a vendor-supplied tool other than SPO.</p> <p>Additional disk classifications may appear, including the following:</p> <ul style="list-style-type: none"> <li>■ <b>RAID-10</b> Implements striping over mirroring technology.</li> <li>■ <b>RAID-50</b> Implements a striped (RAID 0) array that is striped across a RAID 5 array.</li> <li>■ <b>RAID-60</b></li> </ul>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
	<ul style="list-style-type: none"> <li>■ Implements a combination of multiple RAID 6 sets with RAID 0 (striping)</li> </ul> <p>See your vendor documentation for more information about RAID technologies.</p>
<b>Limit Backup Exec to read-only operations</b>	<p>Indicates whether or not you want Backup Exec to reclaim disk space from this virtual disk. If you reattach a storage device to Backup Exec after a specified number of days, and if any data has expired, then Backup Exec may attempt to reclaim the disk space. To prevent this situation, limit Backup Exec to read-only operations so that you can restore data from this storage without having the existing data overwritten.</p> <p>If you enable this option, you can specify the number of days that the storage must be detached from Backup Exec before this option takes effect.</p>
<b>Maximum file size</b>	<p>Lets you set a maximum file size for the disk-based file that Backup Exec creates during a backup job.</p> <p>When this option is enabled, you can set a file size limit for a file that is created during a backup job. If Backup Exec reaches the maximum file size limit during a job, it creates an additional backup file and job spanning occurs. The additional backup file size conforms to the maximum file size limit that you set in this option.</p>

Table R-5 Properties for virtual disks on storage arrays (continued)

Item	Description
<b>Preallocate disk space incrementally up to the maximum file size</b>	<p>Creates the file when the job starts by preallocating space incrementally, according to the size of the increment that you set in Preallocation increment. As the job uses the disk space, more disk space is preallocated up to the maximum file size. When the job completes, the file size is then reduced to the amount of disk space that the job actually used.</p> <p>For example, if you enable preallocation and set the preallocation increment to 4 GB, then 4 GB of disk space is preallocated when the job starts. After the job uses 4 GB, then Backup Exec allocates another 4 GB. Disk space continues to be preallocated by 4 GB until the job completes. If the job only uses 13 GB of the 16 GB that was allocated, then the file size is reduced to 13 GB.</p> <p>Choices are <b>Enabled</b> or <b>Disabled</b>.</p> <p><b>Note:</b> This option works with the option <b>Maximum file size</b>.</p>
<b>Preallocation increment</b>	<p>Displays the amount of disk space by which to increase the file size. The file size is increased by this increment as the job requires disk space, up to the maximum file size. The default is 1 GB.</p> <p><b>Note:</b> This option appears when you enable the option <b>Preallocate disk space incrementally up to the maximum file size</b>.</p>
<b>Auto detect block and buffer size</b>	<p>Indicates if Backup Exec automatically detects the preferred settings for block size, and for the read and write buffers for the virtual disk. The default value is Enabled.</p> <p>When you disable this option, you can manually set the virtual block size and buffers size options as desired.</p> <p>Choices are Enabled or Disabled.</p>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<p><b>Low disk space - Critical</b></p>	<p>Displays the critically low disk space threshold at which you want Backup Exec to send an alert. Backup Exec sends alerts when the amount of free disk space drops below the low disk space threshold, and again if it drops below the warning threshold. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the warning threshold.</p> <p>The default is 5%.</p>
<p><b>Low disk space - Warning</b></p>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of free disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes. This threshold must be less than the low disk space threshold.</p> <p>The default is 15%.</p>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Low disk space</b>	<p>Displays the low disk space threshold at which you want Backup Exec to send an alert. If free disk space drops below this threshold to the amount specified in the warning threshold, another alert is sent. If free disk space drops below the warning threshold to the critical threshold, another alert is sent. The amount of disk space does not include the disk space that is reserved for non-Backup Exec operations.</p> <p>You can change the value of the threshold, and you can change the amount of disk space to megabytes or gigabytes.</p> <p>The default is 25%.</p>
<b>Total capacity</b>	Displays the size of the volume on the virtual disk.
<b>Total backup storage</b>	<p>Displays the expected amount of total raw capacity of all of the physical disks in the storage array.</p> <p>If a storage array can read the total capacity, then it appears in this field. Otherwise, Backup Exec estimates the total capacity.</p>
<b>Used capacity</b>	Displays the amount of raw capacity of all of the physical disks that are used in the storage array. Backup Exec calculates used capacity by subtracting available capacity from total capacity.
<b>Amount of data written</b>	Displays the amount of data that has been written to the disk. The amount of data written may differ from the used capacity due to the effects of data compression. Data compression tends to increase the amount of data written when compared to used capacity.

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Available capacity</b>	Displays the amount of expected raw capacity on the disk that remains unused. Available capacity is calculated by subtracting the amount of reserved disk space on the drive from the drive's total amount of space.
<b>Compression ratio</b>	Displays the ratio of the uncompressed size of a file over its compressed size.
<b>Path</b>	Displays the physical location of the virtual disk on the storage array on the Backup Exec server.
<b>Connection type</b>	Indicates if the virtual disk is located on disk that is local to the Backup Exec server or if it is on a remote disk.
<b>Backup Exec service restart needed</b>	Indicates if the Backup Exec services must be restarted to apply any changes that are made to the Backup Exec server.
<b>Auto detect settings</b>	Indicates if Backup Exec automatically detects the preferred settings for read and write buffers for the virtual disk.
<b>Buffered read</b>	<p>Indicates the following when the setting is enabled:</p> <ul style="list-style-type: none"> <li>■ You do not want Backup Exec to automatically detect settings for this virtual disk.</li> <li>■ You want this virtual disk to allow buffered reads, which is the reading of large blocks of data.</li> </ul> <p>Enabling buffered reads may provide increased performance.</p>

**Table R-5** Properties for virtual disks on storage arrays (*continued*)

Item	Description
<b>Buffered write</b>	Indicates the following when the setting is enabled: <ul style="list-style-type: none"><li data-bbox="829 401 1237 482">■ You do not want Backup Exec to automatically detect settings for this virtual disk.</li></ul> You want this virtual disk to allow buffered writes, which is the writing of large blocks of data.
<b>Concurrent write operations</b>	Displays the number of concurrent write operations that you want to allow to this virtual disk.

## About hot spares in the Storage Provisioning Option

If a storage array that has automatic rebuild capability loses virtual disk redundancy, it uses a physical disk as a hot spare to regain redundancy. If your storage array does not support an automatic rebuild capability, you must use vendor tools to manually rebuild the virtual disks. Refer to your storage vendor documentation for more information.

Use the **Configure Storage Wizard** to specify the physical disks that you want to use as hot spares.

Before you specify a hot spare, refer to the following best practices:

- Specify at least one hot spare for each enclosure. Although you can specify only one hot spare for all of the enclosures, consider the risk if more than one physical disk fails.
- Specify the physical disks that are in slot 0 in the enclosures as hot spares. Then, you can quickly identify which disk is a hot spare.
- Specify a hot spare that is at least the same size as the physical disk that it replaces. If the hot spare is smaller than the physical disk, the storage array cannot rebuild the virtual disk.

For more recommendations, refer to your storage array vendor's documentation.

See [“Changing a hot spare by using the Configure Storage Wizard”](#) on page 1192.

See [“About using the Configure Storage Wizard with the Storage Provisioning Option”](#) on page 1162.

See [“Configuring a storage array by using the Configure Storage Wizard”](#) on page 1163.

## Adding a hot spare by using the Configure Storage Wizard

You can use the **Configure Storage Wizard** to add a hot spare in a storage array. When you complete this wizard, it submits a utility job named **Configure Storage Array**. When the job completes successfully, the hot spare has been added.

See [“About hot spares in the Storage Provisioning Option”](#) on page 1191.

### To add a hot spare by using the Configure Storage Wizard

- 1 On the **Storage** tab, click **Configure Storage Wizard**.
- 2 Click **Disk-based Storage**, and then click **Next**.
- 3 Select **Storage array**, and then click **Next**.
- 4 Select a storage array on which to configure a hot spare drive, and then click **Next**.
- 5 Select the option, **I only want to configure hot spares**, and then click **Next**.
- 6 Follow the on-screen instructions.

## Changing a hot spare by using the Configure Storage Wizard

You can use the **Configure Storage Wizard** to select a different physical disk to use as a hot spare in a storage array. When you complete this wizard, it submits a utility job named **Configure Storage Array**. When the job completes successfully, the hot spare has been changed.

See [“About hot spares in the Storage Provisioning Option”](#) on page 1191.

### To change a hot spare by using the Configure Storage Wizard

- 1 On the **Storage** tab, click **Configure Storage Wizard**.
- 2 Click **Disk-based Storage**, and then click **Next**.
- 3 Select **Storage array**, and then click **Next**.
- 4 Select a storage array on which to change a hot spare drive, and then click **Next**.
- 5 Click **I only want to configure hot spares**, and then click **Next**.
- 6 Do one of the following:

- |  |  |
|--|--|
| To designate a hot spare as an available physical disk | Do the following in the order listed: <ul style="list-style-type: none"><li>■ In the <b>Hot Spares</b> list, select the hot spare that you want to return to the <b>Available Physical Disks</b> list.</li></ul> |
| To designate an available physical disk as a hot spare | Do the following in the order listed: <ul style="list-style-type: none"><li>■ In the <b>Available Physical Disks</b> list, select one or more physical disks that you want to use as hot spares.</li></ul>       |

7 Click **Next**.

8 Review the **Summary** panel, and then click **Finish**.

See [“Viewing storage array components in Backup Exec”](#) on page 1162.

## Detecting a new storage array

Backup Exec periodically searches for new storage arrays or new physical disks. If Backup Exec does not find a new storage array or physical disk that you added, then you should run a refresh operation. If a refresh operation does not discover the new devices, then restart the Backup Exec services.

After you restart the services, the new storage array appears on the **Storage** tab, under **All Storage**.

You must install the Storage Provisioning Option (SPO) before Backup Exec can detect a new storage array.

### To detect a new storage array

- 1 Click the **Storage** tab.
- 2 If you recently added a new storage array or a physical disk, and neither appears under **All Storage**, press F5 to refresh the view.
- 3 If the refresh does not discover the storage array, restart the Backup Exec services.

See [“Starting and stopping Backup Exec services”](#) on page 511.

See [“Troubleshooting the Storage Provisioning Option”](#) on page 1195.

## Renaming a virtual disk or storage array

You can rename a virtual disk or storage array. Names cannot exceed 128 characters. You cannot change the hardware name.

If you use a vendor-supplied tool to configure the storage array, the hardware name that you assign it in the vendor tool appears. To change the hardware name of the storage array, you must use the vendor-supplied tool or the Microsoft Storage Manager for SANs utility.

#### To rename a virtual disk or storage array

- 1 On the **Storage** tab, under **All Storage**, do one of the following:

To rename a virtual disk

Do the following in the order listed.

- Expand a storage array whose virtual disk you want to rename.
- Right-click a virtual disk, then select **Details**.
- In the **Name** field, type a new name for the virtual disk.
- Continue with step 2.

To rename a storage array

Do the following in the order listed.

- Right-click a storage array, and then select **Details**.
- In the **Name** field, type a new name for the storage array.
- Continue with step 2.

- 2 Click **Apply**.

See [“About virtual disks in the Storage Provisioning Option”](#) on page 1171.

## About identifying the physical disks of a virtual disk

Many storage array enclosures incorporate a set of physical disks that use small status lights to indicate the operational status of physical disks. The Storage Provisioning Option (SPO) uses these lights with its **blink** feature to help you quickly identify the physical disks that comprise a virtual disk. When you select the **blink** feature for a virtual disk, the status lights on the physical disks blink.

---

**Note:** Storage array support for the blink features depends on storage array hardware support for the feature. Not all storage array hardware supports blinking. See your storage array hardware documentation for more information.

---

You can use the blink feature in different ways. You can use it to assist with:

- Moving virtual disks from one storage array to another.

You can use the blink feature when you want to move a virtual disk from one enclosure to another. If you have many enclosures, you can use the blink feature to identify the physical disks that comprise the virtual disk. Without it, determining the physical disks that comprise a virtual disk can be difficult.

- Identifying problematic physical disks.

When SPO generates an alert for a physical disk issue, you can use the blink feature to assist you in finding problematic physical disks.

When you use the blink feature, the following applies:

- The blink feature works on one virtual disk at a time.

You cannot use it to simultaneously identify the physical disks in multiple virtual disks.

See “[Identifying the physical disks of a virtual disk](#)” on page 1195.

## Identifying the physical disks of a virtual disk

Use the following steps to identify the physical disks of a virtual disk.

See “[About identifying the physical disks of a virtual disk](#)” on page 1194.

### To identify the physical disks of a virtual disk

- 1 On the **Storage** tab, select a storage array.
- 2 Expand the storage array, and then select a virtual disk.
- 3 Right-click the virtual disk, and then click **Blink**
- 4 To turn off the blink feature, right-click the storage array and then click **Unblink**.

## Troubleshooting the Storage Provisioning Option

If problems occur with the Storage Provisioning Option (SPO) or with storage array hardware, ensure the following:

- The vendor storage array and the vendor hardware provider are supported. You can find a list of compatible devices at the following URL: <http://entsupport.symantec.com/umi/v-269-2>
- The storage array has power and is turned on.
- All lights and indicators on the storage array appear normal.
- The storage array is properly zoned if it is on a SAN.
- The cables are plugged into the correct ports.

- The Microsoft DiskRAID command line tool or the Microsoft Storage Manager for SANs management tool can detect and exercise the storage array hardware.
- The Disk Manager can detect the unmasked virtual disks.
- The refresh operation has run to detect new virtual disks.

If you installed the trial version of SPO, ensure that the license is still within the trial period. When the trial period expires, the option functions in a very limited mode.

See [“About the Storage Provisioning Option”](#) on page 1160.

# Symantec Backup Exec Archiving Option

This appendix includes the following topics:

- [About the Archiving Option](#)
- [Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option](#)
- [Installing the Backup Exec Archiving Option](#)
- [How the Archiving Option works](#)
- [Best practices for the Archiving Option](#)
- [About creating an archive job](#)
- [Editing default settings for the Archiving Option](#)
- [About single instance storage of archived items](#)
- [About synchronizing archive permissions and settings](#)
- [About vault stores in the Archiving Option](#)
- [About vault store partitions in the Archiving Option](#)
- [About archives in the Archiving Option](#)
- [About Archiving Option operation entries in the audit log](#)
- [About Exchange mailbox groups in archive jobs](#)
- [About deleting archived data from its original location](#)
- [About archive settings in the Archiving Option](#)

- [About managing index locations in the Backup Exec Archiving Option](#)
- [About restoring items from the archives](#)
- [About searching for data in the archives](#)
- [About deleting data from the archives](#)
- [About backing up and restoring the Archiving Option components from a remote Backup Exec server](#)
- [Preventing the deletion of expired archived items from an archive](#)
- [About backing up Archiving Option components](#)
- [About restoring an Archiving Option component](#)
- [About moving Archiving Option components to a new location](#)
- [Troubleshooting archive jobs](#)
- [Reports for the Archiving Option](#)
- [About Backup Exec Virtual Vault](#)

## About the Archiving Option

The Archiving Option includes the following features that you can install separately or together:

- The File System Archiving Option, which archives the eligible Windows file system data.
- The Exchange Mailbox Archiving Option, which archives the eligible Exchange mail messages.

To find the data that is eligible for archiving, Backup Exec applies rules to the selected file system shares and folders and to the Exchange mailboxes. Data in the selections is eligible for archiving if it is backed up and meets the criteria that the rules specify. The archive job then sends the data to disk-based vault stores. The data is deleted from its original location on the source computer immediately after it is archived, or after you back up the Archiving Option components.

You can apply retention categories to the data that is archived that specify how long to keep data in the archives. Backup Exec automatically deletes the archived data that has expired retention dates.

By archiving data from the backup sets, Backup Exec eliminates additional querying and movement of data on the remote computers. After Backup Exec deletes the

archived data from its original location, you have more disk space, and Backup Exec requires less time for future backup jobs.

The Archiving Option uses Symantec Enterprise Vault technology to archive data. When you install the Archiving Option, some Enterprise Vault services are also installed.

When you install the Exchange Mailbox Archiving Option, the Virtual Vault feature is automatically installed. Virtual Vault lets end users view their email messages that are archived from Microsoft Outlook on their desktop and laptop computers. These desktop and laptop computers are known as Virtual Vault clients, and they connect to the Backup Exec server for synchronization by using a DNS alias. You must install the Backup Exec Outlook Ad-In on the end users' computers to enable Virtual Virtual.

You can set defaults for each archive job that you create. You can also set the defaults that apply to all archive jobs, and that let you manage other archive operations.

See [“About creating an archive job”](#) on page 1225.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

See [“About Enterprise Vault services for the Archiving Option”](#) on page 1221.

See [“Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option”](#) on page 1199.

See [“Installing the Backup Exec Archiving Option”](#) on page 1217.

See [“How the Archiving Option works”](#) on page 1222.

See [“Best practices for the Archiving Option”](#) on page 1224.

See [“About Backup Exec Virtual Vault ”](#) on page 1273.

## Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option

Some requirements apply to both the Exchange Mailbox Archive Option and to the File System Archive Option. You should also review the requirements that apply to each specific option.

See [“Requirements for the Exchange Mailbox Archiving Option”](#) on page 1201.

See [“Requirements for the File System Archiving Option”](#) on page 1204.

Following are the requirements that apply to both of the Archiving Options:

- The Backup Exec server must be part of a domain. You cannot install the Archiving Option on a server in a workgroup.

- Only common encryption keys can be used to decrypt a backup set during an archive job. If a restricted key is used, then eligible items in the backup set are not archived.
- The Backup Exec server must have enough space to store the Archiving Options index files. When you install the Archiving Options, you are prompted to provide a path where the index files are stored. The path must be on a local NTFS volume. Paths on FAT and FAT32 partitions are not supported.

---

**Note:** Symantec recommends that you have more RAM available in addition to Backup Exec's base requirements.

---

See “[System requirements](#)” on page 65.

You can find a list of compatible operating systems, platforms, and applications at the following URL:

<http://entsupport.symantec.com/umi/V-269-1>

The Archiving Option does not support the following:

- The Backup Exec Central Admin Server Option.

---

**Note:** You can install the Archiving Option on a central administration server. However, distributed job management for archive jobs is not supported.

---

- Archiving from backup sets from the Backup Exec Remote Media Agent for Linux.
- Installation on clustered servers. Additionally, you cannot install Backup Exec on a cluster if you have also selected the Archiving Option for installation.
- Installation of the Exchange Mailbox Archiving Option on a computer on which Microsoft Exchange Server is installed.
- Server groups or multiple servers that are selected for backup.

See “[How to calculate disk space requirements for the Exchange Mailbox Archiving Option](#)” on page 1211.

See “[How to calculate disk space requirements for the File System Archiving Option](#)” on page 1214.

See “[About Enterprise Vault services for the Archiving Option](#)” on page 1221.

## Requirements for the Exchange Mailbox Archiving Option

Requirements that apply to both of the Archiving Options are listed separately. Review those requirements in addition to the requirements that apply only to the Exchange Mailbox Archive Option.

See [“Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option”](#) on page 1199.

If appropriate, you should also review Exchange Mailbox Archiving Option support for Exchange Server 2010.

See [“Requirements for Exchange Mailbox Archiving Option support for Exchange Server 2010”](#) on page 1203.

Following are the requirements that apply to the Exchange Mailbox Archive Option:

- You must enter an Exchange Agent license on the Backup Exec server for each Exchange Server that you want to archive.
- You must install one of the following versions of Microsoft Outlook on the Backup Exec server before you install the Exchange Mailbox Archiving Option:
  - Outlook 2007 Service Pack 2 with hotfix kb968858 or later
  - Outlook 2003 Service Pack 3
- Microsoft Outlook must be the default mail client on the Backup Exec server.
- You must create a profile when you install Outlook on the Backup Exec server, and then connect to an Exchange Server mailbox. Outlook may display an error message about a conflicting program. If Outlook offers to fix the problem, choose to do so, and then follow the instructions that are given.
- The Exchange Server backups must have the Granular Recovery Technology (GRT) option enabled.  
See [“Microsoft Exchange backup options”](#) on page 854.
- The Exchange Server backups must be on one of the following types of storage:
  - Non-removable disk storage.
  - Deduplication disk storage.
  - A storage array in a Storage Provisioning Option environment.
- The Exchange Server backups must have a valid path configured on an NTFS volume that is local to the Backup Exec server for temporary storage of data. The default path is set to use C:\temp.  
See [“Setting default Granular Recovery Technology \(GRT\) options”](#) on page 482.

- A mailbox must be configured for exclusive use by Backup Exec on each Exchange Server on which you want to select mailboxes to archive. Whenever you create an archive job for the Archive Option for Exchange you are prompted to enter the name of the system mailbox. The system mailbox is the mailbox that you configure for use by Backup Exec. It does not need to be named 'system' mailbox.
- The following are restrictions for this mailbox:
  - The mailbox must not be used for any other purpose. The Exchange Mailbox Archiving Option requires exclusive access.
  - The mailbox must not be hidden from address lists.
  - The mailbox account must not be disabled.
- The Backup Exec server domain, and the Exchange Server domains must trust the domain that the Backup Exec service account belongs to.
- You must grant permissions to the Backup Exec service account to the Exchange servers.  
 See “[About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option](#)” on page 1205.
- The Backup Exec service account must be a member of the Active Directory domain. Symantec recommends that you use a Backup Exec service account that has domain and local administrator rights on the Exchange Server. The Backup Exec service account does not need to be a domain administrator.

The components that are listed in the following table are required to install or upgrade the Exchange Mailbox Archiving Option.

**Table S-1** Installed or required components for the Exchange Mailbox Archiving Option

Operating system	Installed or required components
Windows Server 2008	Backup Exec automatically installes IIS 7.0 and some IIS 7.0 role services on Windows Server 2008.  See “ <a href="#">About the Internet Information Services (IIS) 7.0 role services installed by Backup Exec</a> ” on page 1218.

**Table S-1** Installed or required components for the Exchange Mailbox Archiving Option *(continued)*

Operating system	Installed or required components
Windows Server 2003	<p>Backup Exec automatically installs ASP.NET 2.0.</p> <p>On Windows 2003 x64, Backup Exec installs and configures ASP.NET 2.0 in 32-bit mode.</p> <p>You must install the following components manually:</p> <ul style="list-style-type: none"> <li>■ Internet Information Services (IIS) 6.0</li> <li>■ World Wide Web Publishing Service</li> </ul> <p>See your Microsoft documentation for information about installing these components.</p>

## Requirements for Exchange Mailbox Archiving Option support for Exchange Server 2010

You should also review all other requirements that may apply to the Exchange Mailbox Archiving Option.

See [“Requirements for the Exchange Mailbox Archiving Option”](#) on page 1201.

The following are requirements for Exchange Mailbox Archiving Option support for Exchange Server 2010:

- You must install Microsoft Outlook 2007 Service Pack 2 with hotfix kb968858 on the Backup Exec server.
- You must install the Exchange Management Tools for Exchange Server 2010 on the Backup Exec server.  
The management tools on the Backup Exec server must be the same version or later as the management tools that are on the Exchange Server 2010. You can install the management tools when you perform a custom installation of Exchange Server 2010.

---

**Note:** If you install the management tools and Backup Exec together on a Backup Exec server, install the tools first. If you install Backup Exec before you install the management tools, you must restart the Backup Exec server when the tools installation is complete.

---

- If you select mailbox databases in a Microsoft Exchange Database Availability Group (DAG), then you must configure a system mailbox for each member server in the DAG.
- You must grant the Backup Exec service account Send As permissions on a system mailbox
- You must grant permissions for Exchange Server 2007/2010 for the Archiving Option.

See [“Granting the Backup Exec service account Send As permissions on a system mailbox for Exchange Server 2010”](#) on page 1206.

See [“Granting permissions for Exchange Server 2007/2010 for the Archiving Option”](#) on page 1208.

## Requirements for the File System Archiving Option

Some requirements that apply to both of the Archiving Options and to the File System Archiving Option are listed separately. Review those requirements in addition to the requirements that apply only to the File System Archiving Option.

See [“Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option”](#) on page 1199.

The following are requirements for the File System Archiving Option:

- The Backup Exec server must be in the same time zone as the file servers from which eligible data is archived.
- The Backup Exec server domain, the file server domains, and the Exchange Server domains must trust the domain that the Backup Exec service account belongs to.
- The Backup Exec server domain must trust the domains that contain the accounts of users that access the file server shares.
- The Backup Exec service account must have local administrative rights on the file server.
- The Backup Exec service account must have Full Control share permissions on the share that is selected for archiving.
- The Backup Exec service account must be granted the following NTFS rights on the folders in the share that is selected for archiving:
  - **Modify**
  - **List Folder Contents**
  - **Read**

- **Write**

- You must install one of the following Outlook versions on the Backup Exec server to provide full indexing of .msg files:
  - Outlook 2003 Service Pack 3
  - Outlook 2007 Service Pack 2 with hotfix kb968858 or later

## About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option

The Backup Exec service account must access mailboxes on the Exchange Servers that you want to archive. To gain this access, the Backup Exec service account must have permission to access the Exchange Servers.

You can use either of the following methods to grant the permissions that the Backup Exec service account needs to access the mailboxes on Exchange Servers:

- Grant permissions at the organization level or at the Administrative Group level.

Permissions are then propagated automatically to any new Exchange Servers that you add under the level at which the permissions are assigned.

---

**Note:** You must have Exchange administrative permissions to grant permissions to other accounts.

---

- Grant permissions explicitly on each Exchange Server.  
If you grant permissions explicitly and then add another Exchange Server, you must grant permissions explicitly on the added server as well.

The Backup Exec service account must also have the Send As permission on the mailbox that you create for Backup Exec's exclusive use. This mailbox, called the system mailbox, must be created on each Exchange Server on which you want to select mailboxes to archive.

See [“Granting permissions at the Organization level for Exchange Server 2007 for the Archiving Option”](#) on page 1208.

See [“Granting permissions explicitly on each Exchange Server 2007 for the Archiving Option”](#) on page 1209.

See [“Granting permissions at the Organization level for Exchange Server 2003 for the Archiving Option”](#) on page 1210.

See [“Granting permissions at the server level for Exchange Server 2003 for the Archiving Option”](#) on page 1211.

See [“Granting the Backup Exec service account Send As permissions on a system mailbox for Exchange Server 2010”](#) on page 1206.

See [“Granting permissions for Exchange Server 2007/2010 for the Archiving Option”](#) on page 1208.

## Granting the Backup Exec service account Send As permissions on a system mailbox for Exchange Server 2010

The Backup Exec service account requires Send As permissions on the system mailbox on each Exchange server. You can set this permission manually on each account, or use the following procedure.

See [“Requirements for Exchange Mailbox Archiving Option support for Exchange Server 2010”](#) on page 1203.

**To grant the Backup Exec service account Send As permissions on a system mailbox**

- 1 Log on to the Exchange Server using an account with the management role of Active Directory Permissions.

By default, members of the Organization Management role group are assigned this role.

- 2 On the Exchange Server, click **Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
- 3 Type the following command:

```
Add-ADPermission -Identity '<system mailbox name>' -User '<Domain Name\Backup Exec service account>' -AccessRights ExtendedRight -ExtendedRights "send as"
```

See [“Microsoft Exchange permissions granted to the Backup Exec service account”](#) on page 1206.

## Microsoft Exchange permissions granted to the Backup Exec service account

The following table lists the permissions that the script SetEVExchangePermissions.ps1 grants to the Backup Exec service account.

See [“Granting the Backup Exec service account Send As permissions on a system mailbox for Exchange Server 2010”](#) on page 1206.

**Table S-2** Permissions granted to the Backup Exec service account

Path	Object	Permissions
<b>CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Administrative Groups, CN=AdminGroup</b>	<p>Permissions are granted to the CN=Database and descendant objects if Exchange Server 2010 exists in the environment.</p> <p>Permissions are granted to the CN=Servers and descendant objects if Exchange Server 2007 or previous exists in the environment.</p>	<p>The following permissions are granted:</p> <ul style="list-style-type: none"> <li>■ Read</li> <li>■ Administer Information Store</li> <li>■ Open mail send queue</li> <li>■ Receive as</li> <li>■ Send as</li> <li>■ View Information Store status</li> </ul>
<b>CN=Configuration, CN=Services, CN=Microsoft Exchange</b>	Permissions are granted to the following object: <b>CN=Organization</b>	Read
<b>CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization</b>	<p>Permissions are granted to the following objects:</p> <ul style="list-style-type: none"> <li>■ <b>CN=ELC Folders Container</b> and descendant objects</li> <li>■ <b>CN=Global Settings</b> and descendant objects</li> <li>■ <b>CN=Transport Settings</b></li> </ul>	Read
<b>CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Transport Settings</b>	Permissions are granted to the following object: <b>CN=Rules</b>	Read
<b>CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Transport Settings, CN=Rules</b>	<p>Permissions are granted to the following objects:</p> <ul style="list-style-type: none"> <li>■ <b>CN=Journaling</b> and descendant objects</li> <li>■ <b>CN=JournalingVersioned</b> and descendant objects</li> </ul>	Read

## Granting permissions for Exchange Server 2007/2010 for the Archiving Option

You can use a PowerShell script to assign the necessary permissions to the Backup Exec service account for Exchange Server 2007/2010 support.

You must run this script on Exchange Server 2010 or Exchange Server 2007. Note that the script assigns the permissions that all the Exchange Server versions in your environment require, including Exchange Server 2003.

### To grant permissions for Exchange Server 2007/2010 for the Archiving Option

- 1 Log on to the Exchange Server using an account with the following management roles:
  - Active Directory Permissions
  - Exchange Servers
  - Organization Configuration

By default, members of the "Organization Management" role group are assigned these roles.
- 2 Copy the script SetEVEExchangePermissions.ps1 to the Exchange Server.  
The script SetEVEExchangePermissions.ps1 is located on the Backup Exec installation path at \enterprise vault\powershellscripts.
- 3 On the Exchange Server, open the Exchange Management Shell.
- 4 Type the following command:

```
SetEVEExchangePermissions.ps1 -User "<Domain Name\Backup Exec service account>"
```
- 5 To force these changes to take effect immediately, restart the Exchange Information Store service on each Exchange mailbox server.

See ["Microsoft Exchange permissions granted to the Backup Exec service account"](#) on page 1206.

## Granting permissions at the Organization level for Exchange Server 2007 for the Archiving Option

You can grant the **Full Control** permission for the Backup Exec service account at the Organization level.

See ["About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option"](#) on page 1205.

**Note:** You must have Exchange administrative permissions to grant permissions to other accounts.

---

### To grant permissions at the Organization level for the Backup Exec service account in the Archiving Option

**1** On the Exchange Server, click **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Shell**.

**2** Type the following command:

```
Get-OrganizationConfig | Add-ADPermission -User '<Domain Name\Backup Exec service account>' -AccessRights GenericAll -InheritanceType All
```

**3** Type the following command:

```
Add-ADPermission -Identity '<system mailbox name>' -User '<Domain Name\Backup Exec service account>' -ExtendedRights 'Send-as'
```

**4** To grant **Send As** permission on the mailboxes that you created for Backup Exec's exclusive use, repeat the previous step on the appropriate Exchange Servers.

### Granting permissions explicitly on each Exchange Server 2007 for the Archiving Option

You can grant the **Full Control** permission for the Backup Exec service account on each Exchange Server. Perform this procedure on each Exchange Server that you want to archive.

See [“About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option ”](#) on page 1205.

---

**Note:** You must have Exchange administrative permissions to grant permissions to other accounts.

---

### To grant permissions explicitly on each Exchange Server 2007 for the Archiving Option

- 1 On the Exchange Server, click **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Shell**.

- 2 Type the following command:

```
Get-MailboxServer -Identity "<mailbox server name>" > |  
Add-ADPermission -User "<Domain name>\Backup Exe service account"&br/>-AccessRights GenericAll -InheritanceType All
```

- 3 Type the following command:

```
Add-ADPermission -Identity '<system mailbox name>' -User '<Domain  
Name>\Backup Exec service account' -ExtendedRights 'Send-as'
```

### Granting permissions at the Organization level for Exchange Server 2003 for the Archiving Option

You can grant the **Full Control** permission for the Backup Exec service account at the Organization level.

See [“About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option”](#) on page 1205.

Refer to the Microsoft knowledge base for more information on this procedure.

### To grant permissions at the Organization level for Exchange Server 2003 for the Archiving Option

- 1 Configure the **ShowSecurityPage** registry setting to enable the display of the **Security** page.
- 2 In the left pane of Microsoft Exchange System Manager, right-click the **Exchange Organization**, and then click **Properties**.
- 3 On the **Security** tab, click **Add**.
- 4 Select the Backup Exec service account to add it to the list.
- 5 Click **OK**.
- 6 In the **Name** list, select the Backup Exec service account.
- 7 In the **Permissions** list, ensure that all of the check boxes in the **Allow** column are selected.
- 8 Select any check boxes that are not selected.
- 9 Click **OK**.

## Granting permissions at the server level for Exchange Server 2003 for the Archiving Option

You can grant permissions for the Backup Exec service account at the server level for Exchange Server 2003. Perform this procedure on each Exchange Server that you want to archive.

See [“About granting permissions on the Exchange Server for the Backup Exec service account in the Archiving Option”](#) on page 1205.

### To grant permissions at the server level for Exchange Server 2003 for the Archiving Option

- 1 In the left pane of the **Microsoft Exchange System Manager**, expand the **Servers** container.
- 2 Right-click the Exchange Server, and then click **Properties**.
- 3 On the **Security** tab, click **Add**.
- 4 Select the Backup Exec service account to add it to the list.
- 5 Click **OK**.
- 6 In the **Name** list, click the Backup Exec service account.
- 7 In the **Permissions** list, ensure that all of the check boxes in the **Allow** column are selected.
- 8 Select any check boxes that are not selected.
- 9 Click **OK**.

## How to calculate disk space requirements for the Exchange Mailbox Archiving Option

Backup Exec requires permanent disk space for the following components in the Exchange Mailbox Archiving Option:

- The vault store partitions.
- The index locations.
- The SQL Server database, which contains the Directory, vault store, and fingerprint databases.

You should also consider the size of the temporary cache that is required for the Virtual Vault feature. The default maximum size of the temporary cache is 10 GB, but it can be increased.

See [“About the temporary cache location on the Backup Exec server”](#) on page 1284.

[Table S-3](#) describes the formulas that you can use to estimate the disk space requirements for these components for the Exchange Mailbox Archiving Option.

The following values and variables are used in the formulas:

- $N$  is the number of emails.
- $m$  is the average number of identical copies of attachments across user mailboxes.
- The compression factor for attachments is estimated as 60%.  
If the attachments are mostly Office 2007 files, the compression factor to use is 90%.
- The average number of emails that have attachments is estimated at 20%.
- The average size of an email attachment is estimated at 250 KB.

**Table S-3** Calculations for disk space requirements for the Exchange Mailbox Archiving Option

Component	Requirements
Vault store partitions	<p>The size of a vault store partition depends on the following items:</p> <ul style="list-style-type: none"> <li>■ The size of the emails.</li> <li>■ The type of attachments.</li> <li>■ The number and size of the attachments.</li> <li>■ The number of emails with attachments.</li> </ul> <p><b>Note:</b> If single instance storage is enabled, items are shared within and across vault stores and vault store partitions. Shareable parts of a message that exceed the single-instance threshold of 20 KB are shared. These parts include attachments and message bodies. User information and shareable parts under the single instance threshold are not shared.</p> <p>See “<a href="#">About single instance storage of archived items</a>” on page 1233.</p> <p>You can use the following calculations to approximate the disk space requirements of a vault store partition:</p> <ul style="list-style-type: none"> <li>■ Approximate vault store partition size for which single instance storage is not enabled:  <math>(N \times 16) + (N \times 0.2 \times 0.6 \times 250)</math> kilobytes</li> <li>■ Approximate vault store partition size for which single instance storage is enabled:  <math>(N \times 16) + ((1/m) \times (N \times 0.2 \times 0.6 \times 250))</math> kilobytes</li> </ul> <p>For example, you want to know the disk space requirements for a vault store partition for 100,000 emails. You estimate that each email attachment is shared across three people on average.</p> <p>If single instance storage of archived items is not enabled, the calculation for the disk space requirements is as follows:</p> $(100000 \times 16) + (100000 \times 0.2 \times 0.6 \times 250) \text{ kilobytes} = 4.6 \text{ GB approximately}$ <p>If single instance storage is enabled, the calculation for the disk space requirements is as follows:</p> $(100000 \times 16) + ((1/3) \times 100000 \times 0.2 \times 0.6 \times 250) \text{ kilobytes} = 2.6 \text{ GB approximately}$

**Table S-3** Calculations for disk space requirements for the Exchange Mailbox Archiving Option (*continued*)

Component	Requirements
Indexes	<p>The size of an index is approximately 8% of the total size of the items that are archived. The percentage may be less if there is less content to index. For example, there is less content to index when there are large attachments such as MP3 or .jpeg files.</p> <p>For example, you have 100,000 emails that each have a body size of 8 KB. About 20% of the emails have attachments, each with an average total size of 250 KB. The index size is approximately 450 MB.</p>
Directory database	<p>The Directory database only grows when a new mailbox or share is archived for the first time.</p> <p>The recommended disk space is 500 MB.</p>
Vault store database	<p>The size of a vault store database is approximately <math>N \times 500</math> bytes. The vault store database grows with every item that is archived. Temporary space is used to hold information on the items that have not been backed up or indexed.</p>
Fingerprint database	<p>The fingerprint database is created only if you enable single instance storage of archived items. Backup Exec initially allocates 212 MB for the fingerprint database. The fingerprint database grows with every item that is archived.</p> <p>If the database grows to more than 212 MB, use the following calculation to estimate the disk space that it requires:</p> $1/m \times N \times 0.2 \times 500 \text{ bytes}$ <p>See “<a href="#">About single instance storage of archived items</a>” on page 1233.</p>

## How to calculate disk space requirements for the File System Archiving Option

Backup Exec requires permanent disk space for the following File System Archiving Option components:

- Vault store partitions.
- Indexes.
- SQL Server database.

[Table S-4](#) describes the formulas that you can use to estimate the disk space requirements for these components for the File System Archiving Option.

## Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option

The following values and variables are used in the formulas:

- $N$  is the number of files.
- $m$  is the average number of identical copies per file.  
If  $m$  is unknown, use the estimate of 1.2.
- The compression factor for files is estimated as 50%.  
This estimate applies to a mix of files that contain mostly Office 2003 documents. Office 2007 documents do not compress but when mixed with non-Office files, the compression average is 80% of the original size. Pure image files are not compressed.

**Table S-4** Calculating disk space requirements for the File System Archiving Option components

Component	Disk space requirements
Vault store partition	<p>You can use the following calculations to approximate the disk space requirements of a vault store partition:</p> <ul style="list-style-type: none"> <li>■ Approximate vault store partition size for which single instance storage of archived items is not enabled: <math>(N \times 4) + (N \times \text{average file size in kilobytes} \times 0.5)</math> kilobytes</li> <li>■ Approximate vault store partition size for which single instance storage is enabled: <math>(N \times 4) + ((1/m) \times N \times \text{average file size} \times 0.5)</math> kilobytes</li> </ul> <p>For example, you want to know the disk space requirement for a vault store partition for 10,000 files. The average size of each file is 250 KB, and the average number of identical copies per file is 1.2.</p> <p>If single instance storage of archived items is not enabled, then the calculation for the disk space requirement is as follows:</p> $(10000 \times 4) + (100000 \times 250 \times 0.5) \text{ kilobytes} = 1.3 \text{ GB approximately}$ <p>If single instance storage is enabled, then the calculation for the disk space requirement is as follows:</p> $(10000 \times 4) + ((1/1.2) \times 10000 \times 250 \times 0.5) \text{ kilobytes} = 1.08 \text{ GB approximately}$

**Table S-4** Calculating disk space requirements for the File System Archiving Option components (*continued*)

Component	Disk space requirements
Indexes	<p>You can estimate that the index files require approximately 2% of the total size of the files that are archived. The percentage may be less if there is less content to index. If the files are all compressed image file, indexing is less than if the files are mostly small text messages. Numerous small text messages require disk space requirements similar to those of the Archive Option for Exchange for indexing.</p> <p>For example, to archive 10 GB of data, at least 200 MB of available disk space is required to store the index files.</p>
Directory database	<p>The Directory database only grows when a new mailbox or share is archived for the first time.</p> <p>The recommended disk space is 1 GB.</p>
Vault store database	<p>The vault store database grows with every item that is archived. Temporary space is used to hold information on the items that have not been backed up or indexed.</p> <p>The size of a vault store database is approximately <math>N \times 3000</math> bytes.</p>
Fingerprint database	<p>The fingerprint database is created only if you enable single instance storage of archived items. The fingerprint database holds the shareable parts of archived items. Shareable parts of an item that exceed the single-instance threshold of 20 KB are shared. For the File System Archiving Option, it is expected that all files are larger than the 20-KB threshold.</p> <p>Backup Exec initially allocates 212 MB for the fingerprint database. The fingerprint database grows with every item that is archived.</p> <p>If the database grows to more than 212 MB, use the following calculation to estimate the disk space that it requires:</p> <p><math>1/m \times N \times 500</math> bytes</p> <p>See <a href="#">“About single instance storage of archived items”</a> on page 1233.</p>

# Installing the Backup Exec Archiving Option

You can install one or both of the following options locally as a separate, add-on component of Backup Exec:

- Exchange Mailbox Archiving Option
- File System Archiving Option

When you install or upgrade the Backup Exec Exchange Mailbox Archiving Option, the Virtual Vault feature is automatically installed and enabled on the Backup Exec server.

During installation of the Exchange Mailbox Archiving Option, the installation wizard prompts you to specify the following information:

- A path to a location on the Backup Exec server where archived emails are temporarily cached for synchronization with Virtual Vault clients. The default is C:\Program Files\Symantec\Backup Exec\AOCache.
- The maximum size of the temporary cache on the Backup Exec server. The default is 10 GB.
- A fully qualified domain name to create a DNS alias for the Backup Exec Exchange Mailbox Archiving Option. An example of a fully qualified domain name is serveralias.domain.com. The use of a DNS alias simplifies operations if you must move the Backup Exec Archiving Option to another computer. The DNS alias is also used for the connection to the Backup Exec server for virtual vault synchronization.

Command line switches are also available for silent mode installation of these options.

See [“About using the command line to install the Backup Exec Exchange Mailbox Archiving Option”](#) on page 1218.

Before you attempt to install the Archiving Option, verify that all requirements are met.

See [“Installing additional Backup Exec options to the local Backup Exec server”](#) on page 75.

See [“Repairing the Backup Exec Archiving Option”](#) on page 1222.

See [“Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option”](#) on page 1199.

See [“About Enterprise Vault services for the Archiving Option”](#) on page 1221.

See [“About installing Enterprise Vault on a Backup Exec server on which the Archiving Option is installed”](#) on page 1221.

See [“About Backup Exec Virtual Vault ”](#) on page 1273.

See [“About the Internet Information Services \(IIS\) 7.0 role services installed by Backup Exec”](#) on page 1218.

See [“About Vault Cache synchronization”](#) on page 1282.

## About using the command line to install the Backup Exec Exchange Mailbox Archiving Option

If you use the command line to install or upgrade Backup Exec, an additional switch is required to install the Exchange Mailbox Archiving Option. Use this switch to specify a fully-qualified DNS alias.

Use the following command line switch as part of the silent mode installation:

*/BEAODNSALIAS: <fully qualified DNS alias >*

See [“Command line switches for silent mode installation of Backup Exec”](#) on page 105.

See [“Requirements for the Exchange Mailbox Archiving Option”](#) on page 1201.

## About the Internet Information Services (IIS) 7.0 role services installed by Backup Exec

On Windows Server 2008, Backup Exec automatically installs Internet Information Services (IIS) 7.0 and some IIS role services. These role services are described in the following table.

**Table S-5** Installed IIS 7.0 role services

IIS 7.0 features	IIS 7.0 role services
Common HTTP Features	The following role services are installed on the Backup Exec server: <ul style="list-style-type: none"><li>■ Static Content</li><li>■ Default Document</li><li>■ Directory Browsing</li><li>■ HTTP Errors</li><li>■ HTTP Redirection</li></ul>

**Table S-5** Installed IIS 7.0 role services (*continued*)

IIS 7.0 features	IIS 7.0 role services
Application Development Features	<p>The following role services are installed on the Backup Exec server:</p> <ul style="list-style-type: none"> <li>■ ASP.NET</li> <li>■ .NET Extensibility</li> <li>■ Active Server Pages (ASP)</li> <li>■ Internet Server Application Programming Interface (ISAPI) Extensions</li> <li>■ ISAPI Filters</li> </ul>
Health and Diagnostics Features	<p>The following role services are installed on the Backup Exec server:</p> <ul style="list-style-type: none"> <li>■ HTTP Logging</li> <li>■ Logging Tools</li> <li>■ Request Monitor</li> <li>■ Tracing</li> </ul>
Security Features	<p>The following role services are installed on the Backup Exec server:</p> <ul style="list-style-type: none"> <li>■ Basic Authentication</li> <li>■ Windows Authentication</li> <li>■ Request Filtering</li> <li>■ IP and Domain Restrictions</li> </ul>
Performance Features	<p>The Static Content Compression role service is installed on the Backup Exec server.</p>
Management Tools	<p>The following role services are installed on the Backup Exec server:</p> <ul style="list-style-type: none"> <li>■ IIS Management Console</li> <li>■ IIS Management Scripts and Tools</li> <li>■ Management Service</li> <li>■ IIS 6.0 Management Compatibility</li> <li>■ IIS Metabase Compatibility</li> <li>■ IIS 6 WMI Compatibility</li> <li>■ IIS 6 Scripting Tools</li> <li>■ IIS 6 Management Console</li> </ul>

See [“Requirements for the Exchange Mailbox Archiving Option”](#) on page 1201.

## About uninstalling or reinstalling the Archiving Option

If you uninstall both the Exchange Mailbox Archiving Option and the File System Archiving Option, the Enterprise Vault files and the Enterprise Vault services that are included in the Archiving Option are removed. All archive-related jobs display a status of **Disabled**. You cannot run, edit, or save a disabled job. You can delete a disabled job.

If you uninstall only one option, then no changes occur for the existing archive jobs. You can continue to edit and run the archive jobs as usual.

If you reinstall one or both options, all previously archived data is available if you specify the same Backup Exec installation folder path that you used in the initial installation. You can rerun any disabled jobs if no changes were made to the Backup Exec Database. Otherwise, if you try to run the jobs again, the jobs fail.

If you want to reinstall the Archiving Option and use new databases, you must reinstall both options. However, all previously archived data becomes unavailable. Archiving selections, rules, and archiving configurations are also unavailable.

You must remove the following items before you can reinstall the Archiving Option with new databases:

- The Enterprise Vault databases that are included in the Archiving Option. If SQL Express is used, these databases are located by default at \Program Files\Symantec\Backup Exec\Data. If the full version of SQL Server is used, the archive databases are in the path that the administrator defined.
- The BEAODatabase.xml file, which is located at \Program Files\Symantec\Backup Exec.
- The index files, which are located by default at \Program Files\Symantec\Backup Exec\ArchiveIndex.
- The temporary cache, which by default is located at \Program Files\Symantec\Backup Exec\AOCache.

If you reinstall one or both options and you use a different Backup Exec service account than you used for the initial installation, then you must use the Backup Exec Services Manager to update the service account after the reinstallation is complete.

See [“Uninstalling Backup Exec options from the local Backup Exec server”](#) on page 129.

See [“About the temporary cache location on the Backup Exec server”](#) on page 1284.

## About installing Enterprise Vault on a Backup Exec server on which the Archiving Option is installed

If you install Enterprise Vault on a Backup Exec server on which the Archiving Option is installed, all archiving functionality is unavailable. Archive jobs that are active when Enterprise Vault is installed run to completion, but scheduled archive jobs do not run.

All archive-related jobs display a status of **Disabled**. You cannot run, edit, or save a disabled job. You can delete a disabled job.

If you subsequently uninstall Enterprise Vault, archiving functionality remains unavailable.

## About Enterprise Vault services for the Archiving Option

Symantec Enterprise Vault technology is the foundation for the Archiving Option. When you install the Archiving Option, some Enterprise Vault services are also installed. The Enterprise Vault services that run on the Backup Exec server use the same credentials as the Backup Exec service account.

The following Enterprise Vault services are installed on the Backup Exec server:

- Enterprise Vault Admin Service
- Enterprise Vault Directory Service
- Enterprise Vault Indexing Service
- Enterprise Vault Storage Service
- Enterprise Vault Task Controller Service

You must always use the Backup Exec Services Manager on the Backup Exec server to update your Backup Exec credentials. The Backup Exec Service Manager automatically updates the Enterprise Vault service credentials with the same credentials.

---

**Note:** Use of the Windows Services applet to edit the credentials of an Enterprise Vault service or a Backup Exec service is not supported. The use of this applet can leave the Archiving Option unsynchronized with the Backup Exec service account credentials. Errors can occur during the archiving operations.

---

See [“Changing service account information”](#) on page 513.

## Repairing the Backup Exec Archiving Option

If you have missing or corrupted Backup Exec Archiving Option files in an existing setup, or if there are specific installation failures during an upgrade, you can run the Repair option. The Repair option lets you provide service account credentials. If the Exchange Mailbox Archiving Option is configured, the Repair option lets you provide the DNS alias.

See [“Repairing Backup Exec”](#) on page 115.

## How the Archiving Option works

To process an archive job, Backup Exec performs the following actions:

- Reads the associated backup of the file system and Exchange server from which you make archive selections.
- Applies the archive rules that you specify to identify the files and mail messages that are eligible for archiving.
- Checks if eligible files already exist in the archives.  
If a file already exists in the archives, it is not archived again.
- Adds the data to the archives.  
All of the archived data content is indexed to enable fast searching and retrieval of archived items.
- Deletes the archived files and mail messages from their original location.  
Depending on an option that you specify, deletion occurs immediately after the archive job completes or after the vault store is backed up.

The Archiving Option operations that you can perform are described in the following table:

**Table S-6** Operations that you can run

Operation	More information
Create an archive job to archive file system data and Exchange mail messages to vault stores.	See <a href="#">“About creating an archive job”</a> on page 1225.
Create disk-based vault stores to use as storage for the archived data.	See <a href="#">“About vault stores in the Archiving Option”</a> on page 1235.
Restore individual items from the archives.	See <a href="#">“About restoring items from the archives”</a> on page 1259.

**Table S-6** Operations that you can run (*continued*)

Operation	More information
Delete individual items from the archives.	See <a href="#">“About deleting data from the archives”</a> on page 1260.
Delete expired archive data from an archive automatically to free disk space, or ensure that archive data is never deleted from an archive.	See <a href="#">“Preventing the deletion of expired archived items from an archive”</a> on page 1262.
Back up the Archiving Option components. These components include vault stores, vault store partitions, archives, databases, and index locations.	See <a href="#">“About backing up Archiving Option components”</a> on page 1262.
Restore the Archiving Option components. These components include vault stores, vault store partitions, archives, databases, and index locations.	See <a href="#">“About restoring an Archiving Option component”</a> on page 1265.
Synchronize the archive permissions with mailbox permissions, and share and folder permissions.	See <a href="#">“About synchronizing archive permissions and settings”</a> on page 1234.

See [“Best practices for the Archiving Option”](#) on page 1224.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

## Types of data not included in archive jobs

The Archiving Option does not include some types of data in archive jobs.

**Table S-7** The types of data that are not included in archive jobs

Archive Option	Types of data
File System Archiving Option	<p>The following types of data are not included in a file system archive job:</p> <ul style="list-style-type: none"> <li>■ Hard links</li> <li>■ Files with alternate streams</li> <li>■ Reparse points</li> <li>■ Sparse files</li> <li>■ Files in Microsoft Distributed File System Replication (DFSR) shares, system folders, or recycle bins</li> <li>■ Files that have an encrypted, hidden, or system attribute</li> <li>■ Files that are in mount point directories You can share the root of the mount point target, and then select it for archiving.</li> </ul>
Exchange Mailbox Archiving Option	<p>The following types of data are not included in an Exchange mailbox archive job:</p> <ul style="list-style-type: none"> <li>■ Mail messages that have pending reminders.</li> <li>■ Any Exchange items other than mail messages, such as address book entries and calendar items.</li> <li>■ Mail messages in Exchange managed folders, journal mailboxes, or in public folders.</li> </ul>

## Best practices for the Archiving Option

Following are best practices when you use the Archiving Option:

- Use the default full recovery model for the SQL Server instance that hosts the Backup Exec Database and the Archiving Option databases. All Archiving Option databases that are created on the SQL Server are then also created with the full recovery model.
- Do not use different Backup Exec servers to archive files or mailboxes from the same file server or Exchange server.
- Consider archiving a smaller amount of data at first, such as a mailbox or a folder. All backup data may be eligible when you run the first archive job. Over

a period of time, the amount of eligible archive data lessens, and it becomes a predictable amount.

- Ensure that an item is included in only one archive job. Unlike backup jobs, archive jobs cannot share the same items.
- Ensure that all subdirectories are included in only one archive job.
- Do not archive the system drive. The Archiving Option does not archive system files.
- If you redirect the restore of Archiving Option components to a new server because of hardware failure, redirect the restore of the Directory database first. After the redirected restore of the Directory database is complete, you must run some additional tasks in a separate program called Backup Exec Utility. The tasks in the Backup Exec Utility update the Directory database with the new locations of the components. You should run the Backup Exec Utility tasks before you redirect the restore of any other Archiving Option components.

## About creating an archive job

You create an archive job by adding an archive stage to a backup job. You can add the archive stage when you create the backup job, or you can edit an existing backup job and add an archive stage. When you add the archive stage, you choose the file system shares and folders and Exchange mailboxes that you want to archive. You can set other archive job options when you create the archive stage.

You can also edit the default settings that apply to all archive jobs.

---

**Note:** Archive is not available for server groups or when you select multiple servers for backup.

---

See [“Setting archive job options”](#) on page 1226.

See [“Viewing the servers that have archiving jobs”](#) on page 1225.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

See [“About the Archiving Option”](#) on page 1198.

## Viewing the servers that have archiving jobs

You can view a list of all of the servers for which you have created archiving jobs.

See [“About creating an archive job”](#) on page 1225.

### To view the servers that have archiving jobs

- ◆ Do either of the following:

To view archiving jobs for servers from the **Backup and Restore** tab

Do the following in the order listed:

- On the **Backup and Restore** tab, multi-select any number of servers.
- Right-click the servers, and then click **Details**.
- In the **Views** group, click **List**, and then click **Sort and Filter**.
- Click **Filter**, and then select **Job Type**.
- Click **Enable this filter**, and then click **Archive**, and then click **OK**.

To view archiving jobs for servers from the **Storage** tab

Do the following in the order listed:

- On the **Storage** tab, double click a vault store.
- On the left, click **Archives**.
- View the list of servers in the **Server** column.

## Setting archive job options

You can choose the file system shares and folders and Exchange mailboxes that you want to archive, and set other options for the archive job.

See [“About creating an archive job”](#) on page 1225.

### Setting archive job options

- 1 Create a backup with an archive stage, or edit a stage that is part of a backup job.  
See [“Backing up data”](#) on page 163.  
See [“Editing a stage”](#) on page 184.
- 2 On the Archive box in the backup definition, click **Edit**.

**3** On the **Archive Options** dialog box, do any of the following:

- |  |  |
|--|--|
| To set a time and frequency for when to run the archive job                            | Click <b>Schedule</b> .<br>See <a href="#">“Schedule options”</a> on page 188.   |
| To configure Backup Exec to notify specified recipients when the archive job completes | Click <b>Notification</b> .<br>See <a href="#">“Notification options for jobs”</a> on page 299.                              |
| To configure file system shares and folders to archive                                 | Click <b>File System Selections</b> .<br>See <a href="#">“File System Selections options for archive jobs”</a> on page 1227. |
| To configure Exchange mailboxes to archive   | Click <b>Exchange Selections</b> .<br>See <a href="#">“Exchange Selections options for archive jobs”</a> on page 1228.       |
| To specify the storage that you want to use for the archive job.                       | Click <b>Storage and Settings</b> .<br>See <a href="#">“Storage and Settings options for archive jobs”</a> on page 1229.     |
- You can also specify the system mailbox to use if you archive Exchange mailboxes.

**4** Click **OK**.**File System Selections options for archive jobs**

You can select the folders or shares where you want Backup Exec to find data to archive. You can apply the same archive settings to all of the selections, or apply different archive settings to different selections.

See [“Setting archive job options”](#) on page 1226.

**Table S-8** File System Selections options for archive jobs

Item	Description
<b>Show administrative shares</b>	Displays the administrative shares from which you can select the files and folders where you want Backup Exec to find data to archive.
<b>Add to Include List</b>	Lets Backup Exec search the share selection or the folder selection for the eligible data to include in the archive stage.

**Table S-8** File System Selections options for archive jobs *(continued)*

Item	Description
<b>Add to Exclude List</b>	Lets Backup Exec search the share selection or the folder selection for the eligible data to exclude from the archive stage.
<b>Remove from List</b>	Lets you remove the share or folder from the selections list.
<b>Share or Folder Path</b>	Displays the location of the share selection or the folder selection.
<b>Include/Exclude</b>	Lets you specify if you want to include in or exclude the shares and folders from the archive stage.
<b>Archive Setting</b>	Lets you select the retention category and archive rules to apply to specific share and folder selections.
<b>New Archive Settings</b>	Lets you create a retention category and archive rules to apply to the selections.  See “ <a href="#">About archive settings in the Archiving Option</a> ” on page 1247.

## Exchange Selections options for archive jobs

You can select Exchange mailboxes to archive, and configure them into groups for the archive job.

See “[Setting archive job options](#)” on page 1226.

**Table S-9** Exchange Selections options for archive jobs

Item	Description
<b>Enable archiving for Exchange mailboxes</b>	Lets Backup Exec archive Exchange mailboxes.
<b>Mailbox group details</b>	Displays the details of the mailbox groups.
<b>New Mailbox Group</b>	Lets you create a new mailbox group to archive.  See “ <a href="#">Mailbox group options for mailbox group details</a> ” on page 1245.

**Table S-9** Exchange Selections options for archive jobs (*continued*)

Item	Description
<b>Mailbox Group</b>	Displays the names of the mailbox groups that you can select for archiving.  See “ <a href="#">About Exchange mailbox groups in archive jobs</a> ” on page 1242.
<b>Users</b>	Lists the names of the users whose mailboxes are included in a mailbox group for archiving.
<b>Virtual Vault</b>	Indicates if Virtual Vault is enabled for this mailbox group.
<b>Retention Category</b>	Indicates the retention category that is applied to the mailbox group. A retention category specifies the period of time for which you want to keep items in the archives.
<b>Retention Period</b>	Indicates the amount of time that the item stays in the archives.
<b>Items Older Than</b>	Indicates if the items that are older than a specified period are included or excluded from the archive job.
<b>File Size Greater Than</b>	Indicates if the items have a size that is greater than a specified amount are included or excluded from the archive job.
<b>Messages With Attachments</b>	Indicates if messages with attachments are included or excluded from the archive job.
<b>Unread Messages</b>	Indicates if the messages that have not been read are included or excluded from the archive job.

## Storage and Settings options for archive jobs

When you add an archive stage to a backup job, you must specify a vault store where Backup Exec stores the archived data. If you archive Exchange mailboxes, you must also specify a system mailbox.

See “[Setting archive job options](#)” on page 1226.

**Table S-10** Storage and Settings options for archive jobs

Item	Description
<b>Server</b>	Displays the name of the server that is selected for the archive job.
<b>Vault Store Name</b>	<p>Displays the vault store where Backup Exec stores the archived data.</p> <p>You must specify a vault store to the server if one is not already specified. If you change the specified vault store, the change only affects the mailboxes or shares that you archive after you reassign the vault store. The shares and mailboxes that already have an archive in the previously specified vault store continue to be archived to that same archive.</p> <p>If there is no vault store, you must create one.</p>
<b>System Mailbox</b>	<p>Displays the name of the system mailbox on the Exchange Server for Backup Exec to log on to. If a system mailbox is not assigned, you must assign one.</p> <p>This option only appears if you choose to archive Exchange mailboxes.</p> <p>See <a href="#">“Requirements for the Exchange Mailbox Archiving Option”</a> on page 1201.</p>
<b>New Vault Store</b>	<p>Lets you create a new vault store.</p> <p>See <a href="#">“About vault stores in the Archiving Option”</a> on page 1235.</p>

## Editing default settings for the Archiving Option

You can edit the default settings for the Archiving Option.

See [“About the Archiving Option”](#) on page 1198.

### To edit default settings for the Archiving Option

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.

- 3 Select the appropriate options.  
See [“Default settings for the Archiving Option”](#) on page 1231.
- 4 Click **OK**.

## Default settings for the Archiving Option

You can use the default settings that Backup Exec creates during installation for the Archiving Option. Or you can choose your own default settings.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

**Table S-11** Default settings for the Archiving Option

Item	Description
<b>Synchronize archive permissions and mailbox group members every day at</b>	Indicates the time at which Backup Exec synchronizes the correct archive settings and archive permissions to each mailbox in all of the mailbox groups.  The default time is 3:00 A.M.  See <a href="#">“About synchronizing archive permissions and settings”</a> on page 1234.
<b>To run synchronization now, click Run Now</b>	Starts the synchronization task immediately.
<b>Delete archived items that have expired retention periods every day at</b>	Indicates the time at which Backup Exec searches the vault store partitions to delete the archived items that have expired retention periods.  The default time is 4:00 A.M.  For individual archives, you can prevent Backup Exec from automatically deleting the expired archived items.  See <a href="#">“Preventing the deletion of expired archived items from an archive”</a> on page 1262.

**Table S-11** Default settings for the Archiving Option *(continued)*

Item	Description
<p><b>Enable single instance storage of archived items</b></p>	<p>Lets Backup Exec identify the shareable parts of an item, such as a message attachment or the contents of a document. Backup Exec then stores the parts separately, and only once. When Backup Exec identifies a shareable part that is already stored in a vault store, it references the stored shareable part instead of archiving it again.</p> <p>Enabling this option can provide a significant reduction in the storage space that is required for archived items.</p> <p>See <a href="#">“About single instance storage of archived items”</a> on page 1233.</p> <p>If you enable this option, you should back up the fingerprint databases. Single instance storage-related information is contained in the fingerprint databases for all of the vault stores.</p>
<p><b>Default retention category</b></p>	<p>Displays the retention category that applies to the Backup Exec archive jobs by default. A retention category specifies the period of time for which you want to keep items in the archives.</p> <p>You can edit a retention category to change the retention period.</p> <p>The default retention category specifies a retention period of infinite.</p> <p>See <a href="#">“About retention categories for archived items”</a> on page 1250.</p>
<p><b>Temporary cache location for synchronization of archived emails with Virtual Vault clients</b></p>	<p>Displays the location where copies of new items that are added to the archive on the network are held.</p> <p>See <a href="#">“About the temporary cache location on the Backup Exec server”</a> on page 1284.</p>

**Table S-11** Default settings for the Archiving Option (*continued*)

Item	Description
<b>Maximum cache size</b>	Displays the maximum size of the temporary cache location. The default is 10 GB.  See <a href="#">“About the temporary cache location on the Backup Exec server”</a> on page 1284.
<b>Retention categories</b>	Lets you manage retention categories.  See <a href="#">“About retention categories for archived items”</a> on page 1250.
<b>Archive Settings</b>	Lets you manage archive settings.  See <a href="#">“About archive settings in the Archiving Option”</a> on page 1247.
<b>Mailbox Groups</b>	Lets you manage mailbox groups.  See <a href="#">“About Exchange mailbox groups in archive jobs”</a> on page 1242.
<b>Index Locations</b>	Lets you manage index locations.  See <a href="#">“About managing index locations in the Backup Exec Archiving Option”</a> on page 1254.

## About single instance storage of archived items

Single instance storage of the archived items lets Backup Exec identify the shareable parts of an item. An example of a shareable part is a message attachment or the contents of a document. Backup Exec then stores the parts separately, and only once. When Backup Exec identifies a shareable part that is already stored in a vault store, it references the stored shareable part instead of archiving it again.

If single instance storage is enabled, items are shared within and across vault stores and vault store partitions. The vault store partitions may be on different storage. Shareable parts of a message that exceed the single-instance threshold of 20 KB are shared. These parts include attachments and message bodies. The user information and the shareable parts that are under the single instance storage threshold are not shared.

Enabling this option can provide a significant reduction in the storage space that is required for archived items. If you enable single instance storage, you should back up the fingerprint databases. Single instance storage-related information is contained in the fingerprint databases for all of the vault stores.

See [“Enabling single instance storage of archived items”](#) on page 1234.

## Enabling single instance storage of archived items

You can enable single instance storage of archived items.

See [“About single instance storage of archived items”](#) on page 1233.

### To enable single instance storage of archived items

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Archive**.
- 3 Ensure that **Enable single instance storage of archived items** is selected.

See [“Default settings for the Archiving Option ”](#) on page 1231.

## About synchronizing archive permissions and settings

Backup Exec runs a daily synchronization task for the Archiving Option.

Synchronization associates the correct archive settings to each mailbox in all of the mailbox groups. This task also ensures that archive permissions are synchronized with the mailbox permissions for each mailbox that is archived. For the File Systems Archiving Option, archive permissions are synchronized with share and folder permissions for each file that is archived.

For Exchange 2010 support, the synchronization task synchronizes Exchange server membership of any Database Availability Groups (DAG) that you select for archiving. The synchronization task detects if Exchange servers are added to a selected DAG. If so, then the vault store and the system mailbox that are associated with an existing DAG member server are automatically associated to the added server. If necessary, you can modify the system mailbox association by editing the archive stage for which this DAG is selected for backup.

The job log for the synchronization task displays the following information:

- All of the archives and folders for which permissions are synchronized.
- Any Exchange servers that are added to a DAG.
- The vault stores and system mailboxes that are automatically associated with any new Exchange servers that are added to a DAG.
- Any Exchange servers that are removed from a DAG.

You can specify the time of day to run this operation. Symantec recommends that you schedule the archive jobs to run at a different time than the synchronization operation.

An alert is sent to the administration console when the synchronization operation completes. The alert displays the summary statistics of the operation, and contains a link to the operation's job log.

---

**Note:** The Exchange servers and file system servers must be online and accessible by the Backup Exec server for synchronization to occur.

---

See [“Editing default settings for the Archiving Option”](#) on page 1230.

## About vault stores in the Archiving Option

A vault store is a disk-based container for the archived data that Backup Exec archives from one server. When you add an archive stage to a backup job, you select a vault store as the storage device to which you want to send the archived data. A vault store contains at least one vault store partition that is the physical location where the archived items are stored. You can create additional vault store partitions for a vault store when it requires more disk space.

See [“About vault store partitions in the Archiving Option”](#) on page 1238.

Each vault store has an associated database. The database holds information about the archives in the vault store and all the items that are stored in each archive. For example, when an item is archived, the vault store's database is updated with this information. Single instance storage-related information is contained in the fingerprint databases for all of the vault stores.

The following vault store properties let you manage the deletion of archived items:

- Delete an item from its original location on the server immediately after it is archived, or after the vault store is backed up.  
See [“About deleting archived data from its original location”](#) on page 1247.
- Delete the archived items that have expired retention periods from specific archives in vault stores.  
See [“Preventing the deletion of expired archived items from an archive”](#) on page 1262.

You can back up vault stores and their associated databases, along with other Archiving Option components.

You must use the Configure Storage wizard to create a vault store.

See [“About the Configure Storage wizard”](#) on page 145.

See [“Editing or viewing vault store properties”](#) on page 1236.

See [“About deleting an Archiving Option vault store”](#) on page 1237.

## Editing or viewing vault store properties

You can edit or view vault store properties.

See [“About vault stores in the Archiving Option”](#) on page 1235.

### To edit or view vault store properties

- 1 On the **Storage** tab, double-click the vault store for which you want to view properties.
- 2 On the left, click **Properties**.
- 3 Edit the information as appropriate.

See [“Vault store properties”](#) on page 1236.

## Vault store properties

You can edit the vault store properties.

See [“Editing or viewing vault store properties”](#) on page 1236.

**Table S-12** Vault store properties

Item	Description
<b>Name</b>	Displays the name of the vault store where Backup Exec stores archived data. You can edit this field to change the name.  <b>Note:</b> Do not name a vault store with the same name that is already in use by an Archiving Option component, such as <b>Fingerprint Databases</b> or <b>All Partitions</b> . A vault store that has the same name as another Archiving Option component can cause errors when you make backup selections. Backup job or restore job failures can also occur.
<b>Description</b>	Displays a description of the vault store. You can edit this field to change the description.

Table S-12 Vault store properties (*continued*)

Item	Description
<b>State</b>	<p>Displays the following states:</p> <ul style="list-style-type: none"> <li>■ <b>Available</b> Archive jobs can send data to this vault store.</li> <li>■ <b>Being deleted</b> The vault store is in the process of being deleted. Archive jobs cannot send data to this vault store.</li> <li>■ <b>In backup mode</b> A backup or restore job is running for the vault store.</li> </ul>
<b>Database name</b>	Displays the name of the database that is associated with this vault store.
<b>Archive count</b>	Displays the number of archives that the vault store contains.
<b>Total size</b>	Displays the total size of all of the items that are archived in the vault.
<b>Item deletion method</b>	<p>Designates when to delete archived items from their original locations.</p> <p>You can choose to delete the item immediately after it is archived or delete it after the vault store is backed up. If you delete an item immediately after it is archived, the item is deleted from its original location after the archive job has successfully completed.</p> <p>See <a href="#">“About deleting archived data from its original location”</a> on page 1247.</p>

## About deleting an Archiving Option vault store

You can delete a vault store if one of the following conditions apply:

- It is not assigned to any servers on which you have made archive selections.
- It is the only vault store and you have deleted all of the archive stages that send archive data to it.

When you delete a vault store, you cannot cancel or undo the operation.

When you delete a vault store, all partitions, archives, and archived items in that vault store are also deleted. You must reassign another vault store to all of the servers that were assigned to the vault store that you want to delete.

See [“Deleting a vault store”](#) on page 1238.

## Deleting a vault store

You can delete a vault store from Backup Exec.

See [“About deleting an Archiving Option vault store”](#) on page 1237.

### To delete a vault store

- 1 On the **Storage** tab, right-click the vault store that you want to delete.
- 2 Click **Delete**.
- 3 If no other vault stores exist, you must do one of the following:
  - Delete all of the existing archive stages before you can delete this vault store.  
See [“Deleting scheduled jobs”](#) on page 259.
  - Create a new vault store, assign it to all of the affected archived servers, and then delete the selected vault store.  
See [“About the Configure Storage wizard”](#) on page 145.

## About vault store partitions in the Archiving Option

A vault store partition represents the physical location where the archived items are stored. A vault store can contain one or more vault store partitions. Backup Exec creates one vault store partition in each vault store by default.

As the data in a vault store grows, you can create more vault store partitions to provide additional capacity. You can specify a local drive or a network share as a location for a vault store partition. You cannot specify a path that is a subdirectory in the path for another vault store partition. You must use the Configure Storage wizard to create a vault store partition.

See [“About the Configure Storage wizard”](#) on page 145.

A vault store can contain many vault store partitions, but only one partition is open at a time. As data is archived, it is stored in the open partition. You can specify a vault store partition as open or closed by editing the partition properties.

You can restore archived items from closed partitions, as well as delete the archived items that are in closed partitions.

Backup Exec searches the vault store partitions daily to delete the archived items that have expired retention periods. You can specify the time at which this daily operation runs.

See [“Preventing the deletion of expired archived items from an archive”](#) on page 1262.

See [“Editing vault store partition properties”](#) on page 1239.

## Editing vault store partition properties

You can change the state of a vault store partition to open or closed. You can also edit the name and description of a vault store partition.

See [“About vault store partitions in the Archiving Option”](#) on page 1238.

### To edit vault store partition properties

- 1 On the **Storage** tab, expand the vault store that contains the vault store partition that you want to edit.
- 2 Right-click the vault store partition, and then click **Details**.
- 3 Edit the appropriate information.

See [“Vault store properties”](#) on page 1236.

## Vault store partition properties

A vault store partition represents the physical location where the archived items are stored. You can create a new vault store partition or change the state of an existing vault store partition.

See [“Editing or viewing vault store properties”](#) on page 1236.

**Table S-13** Vault store partition properties

Item	Description
<b>Name</b>	Displays the name of the vault store partition.
<b>Description</b>	Displays a description of the vault store partition.

**Table S-13** Vault store partition properties (*continued*)

Item	Description
<b>Location</b>	<p>Displays the path name where the vault store partition is located.</p> <p>The path can be on a local drive or on a network share. You cannot specify a path that is a subdirectory in the path for another vault store partition.</p> <p>For example, you can create a vault store partition on C:\vault store 1. However, you cannot create another vault store partition on C:\vault store 1\vault store 2.</p> <p>Ensure that the Backup Exec service account has full permissions for the path.</p> <p>See <a href="#">“About the Backup Exec service account”</a> on page 512.</p>
<b>State</b>	<p>Displays one of the following states:</p> <ul style="list-style-type: none"> <li>■ <b>Open</b> New archived data is stored in this vault store partition.</li> <li>■ <b>Closed</b> New archived data cannot be stored in this vault store partition.</li> </ul>

## About archives in the Archiving Option

An archive is a logical group of archived items. Items in an archive are stored in different vault store partitions depending on which partition is open at the time that the item is archived. Each archived file system share has its own archive, and each archived Exchange mailbox has its own archive. Backup Exec creates the archives when it runs an archive stage.

You cannot back up archives. You can only back up the vault store partitions.

See [“Editing archive properties”](#) on page 1240.

See [“Deleting an archive”](#) on page 1241.

### Editing archive properties

You can edit archive properties.

See [“About archives in the Archiving Option”](#) on page 1240.

#### To edit archive properties

- 1 On the **Storage** tab, expand the vault store that contains the archive for which you want to edit properties.
- 2 Double-click the archive.
- 3 In the left pane, click **Properties**.

See [“Archive properties”](#) on page 1241.

## Deleting an archive

You can delete an archive. However, if you delete an archive from Backup Exec, all of the archived data in the archive is also deleted.

See [“About archives in the Archiving Option”](#) on page 1240.

#### To delete an archive

- 1 On the **Storage** tab, double-click the vault store that contains the archive that you want to delete.
- 2 Right-click the archive, and then click **Delete**.
- 3 When you are prompted if you want to delete the archive, click **Yes**.

## Archive properties

You can view archive properties. You can also edit the setting to let Backup Exec automatically delete the archived items that have expired retention periods.

See [“Editing archive properties”](#) on page 1240.

**Table S-14** Archive properties

Item	Description
Resource name	Displays the name of the file share or Exchange mailbox that is archived.
Resource type	Displays one of the following types of archive: <ul style="list-style-type: none"><li>■ File share</li><li>■ Exchange mailbox</li></ul>

**Table S-14** Archive properties (*continued*)

Item	Description
<b>Status</b>	Displays one of the following statuses as appropriate: <ul style="list-style-type: none"><li>■ Available</li><li>■ Being created</li><li>■ Being deleted</li></ul>
<b>Server</b>	Displays the name of the server on which the archive is stored.
<b>Automatically delete archived items that have expired retention periods</b>	Lets Backup Exec delete the archived items that have expired retention periods from the archives.  You can set a time at which Backup Exec deletes these items daily.  Disable this option if you do not want archived items to be automatically deleted from this archive.  This option is enabled by default.

## About Archiving Option operation entries in the audit log

Audit logs provide information about the operations that have been performed in Backup Exec.

You can view information about archiving operations for the following:

- Vault stores
- Vault store partitions
- Archive settings
- Retention categories

See [“About audit logs”](#) on page 516.

## About Exchange mailbox groups in archive jobs

A mailbox group contains the selections on the Exchange Server that you want to archive. A mailbox group consists of user mailboxes to which you want to assign

the same archive settings. For example, you can add a single user to a mailbox group, or you can add the entire Exchange organizational unit to a mailbox group.

Backup Exec applies the archive settings sequentially to each mailbox group in the list. The archive settings of the first mailbox group that a mailbox is found in are applied to that mailbox.

The order of the mailbox groups is important. You should arrange the mailbox groups that have specific selections of users, groups, and distribution lists at the top of the list. Arrange the mailbox groups that contain the least specific selections at the bottom of the list. For example, a mailbox group that contains specific users should be listed before a mailbox group that contains a user group. In turn, a mailbox group that contains a user group should be listed before a mailbox group that contains the whole Exchange organizational unit. For example, you want to ensure that the correct archive settings are applied to the users that are in multiple groups.

You would arrange the following example mailbox groups in the order listed:

- The Managers group contains individual user accounts and requires all messages to be archived.
- The Some Users group contains some users in an organizational unit and requires messages to be archived from the last two months.
- The All Users group contains the entire Exchange organizational unit and requires messages to be archived from the last six months.

You can select the following items to archive in a mailbox group:

- Distribution lists
- User groups
- Users

You can create mailbox groups when you create an archive stage for Exchange Server mailboxes, or at any time from the global defaults.

See [“Managing Exchange mailbox groups”](#) on page 1243.

## Managing Exchange mailbox groups

You can configure and manage mailbox groups for archive jobs for the Exchange Mailbox Archiving Option.

See [“About Exchange mailbox groups in archive jobs”](#) on page 1242.

### To manage Exchange mailbox groups

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Archive**.
- 3 Click **Manage Mailbox Groups**.
- 4 Enter the necessary information as appropriate.  
See [“Manage mailbox groups options”](#) on page 1244.

## Manage mailbox groups options

You can configure or edit the mailbox groups that contain the selections for an archive job.

See [“Managing Exchange mailbox groups”](#) on page 1243.

**Table S-15** Manage mailbox group options

Item	Description
<b>Domain</b>	Displays the domains that you can select.
<b>Mailbox Group</b>	Displays the names of the mailbox groups in the selected domain that this stage archives.  If there are no mailbox groups, you must create one before you can run an archive job.
<b>Retention Category</b>	Displays the retention category that the mailbox group is assigned to.
<b>Virtual Vault Status</b>	Indicates if Virtual Vault is enabled for this mailbox group.  See <a href="#">“About enabling and disabling Virtual Vault”</a> on page 1286.
<b>Add</b>	Lets you create a mailbox group to add to an archive job.  See <a href="#">“Mailbox group options for mailbox group details”</a> on page 1245.
<b>Edit</b>	Lets you edit the selected mailbox group.  See <a href="#">“Mailbox group options for mailbox group details”</a> on page 1245.

**Table S-15** Manage mailbox group options (*continued*)

Item	Description
<b>Delete</b>	Deletes the selected mailbox group from the list of mailbox groups to archive.
<b>Move Up</b>	<p>Moves the selected mailbox group up in the list.</p> <p>The retention category and the archive rules apply to the mailbox groups in the order in which the mailbox groups are listed. A mailbox that belongs to multiple groups is archived according to the archive settings of the highest-level group that it is in.</p> <p>See <a href="#">“About Exchange mailbox groups in archive jobs”</a> on page 1242.</p>
<b>Move Down</b>	Moves the selected mailbox group lower in the list.

## Mailbox group options for mailbox group details

For an archive job, create a mailbox group that contains the selections on the Exchange servers that you want to archive. You can also specify the retention category and archive rules for each group.

See [“Managing Exchange mailbox groups”](#) on page 1243.

**Table S-16** Mailbox group options for mailbox group details

Item	Description
<b>Name</b>	Designates the name of the mailbox group.
<b>Users</b>	Lets you specify the users that you want to include in this mailbox group.
<b>Enable Virtual Vault for this mailbox group</b>	<b>Note:</b> If you make changes to Virtual Vault, you must notify your end users that they must restart Outlook before changes can take effect.

**Table S-16** Mailbox group options for mailbox group details (*continued*)

Item	Description
<b>Retention category</b>	<p>Lets you specify the retention category for the mailbox group.</p> <p>The default setting is the default retention category, which has a retention period of infinite.</p> <p>See “<a href="#">About retention categories for archived items</a>” on page 1250.</p>
<b>New Retention Category</b>	<p>Lets you create a new retention category.</p> <p>See “<a href="#">Retention category properties</a>” on page 1252.</p>
<b>Retention period</b>	<p>Indicates how long to retain the items in the archives.</p>
<b>Description</b>	<p>Displays a description of the retention category.</p>
<b>Archive items that are older than</b>	<p>Indicates that the items that are older than the specified time are archived.</p> <p>The default setting is six months.</p>
<b>If the items are larger than</b>	<p>Indicates that if the items that are larger than the specified size and are older than the specified time are archived, then archive those items after a specified number of weeks..</p> <p>You should archive larger mail messages more often than other messages. Specify a lesser amount of time in this option than in the previous <b>Are older than</b> option.</p> <p>The default setting is 10 MB and two weeks.</p>
<b>Archive only messages with attachments</b>	<p>Indicates that the messages with attachments are archived.</p> <p>The option is enabled by default.</p>
<b>Archive unread messages</b>	<p>Indicates that the messages that have not been read are archived.</p>

## About deleting archived data from its original location

When you create a vault store, you can specify when to delete the archived data from its original location.

You can let Backup Exec do one of the following:

- Delete the item from its original location immediately after it is archived. If the data is lost before the vault store is backed up, the only version of the data is on the backup set.
- Delete it after the vault store is backed up and the next archive job runs.

If Backup Exec deletes an item immediately after it is archived, the item is deleted from its original location after the archive job has successfully completed. If the item is modified after it is archived but before it is backed up, then it is not deleted from its original location.

See [“Editing or viewing vault store properties”](#) on page 1236.

## About archive settings in the Archiving Option

Archive settings let you apply the following criteria:

- The retention category that specifies how long to keep the data in the archives.
- The rules that determine if data is eligible for archiving.

For example, you can specify that only the mail messages that are older than six months are archived for a mailbox selection.

You can create archive settings for the following selections:

- File system shares
- File system folders within the shares

---

**Note:** You can name each group of archive settings that you create.

---

See [“Editing default settings for the Archiving Option”](#) on page 1230.

## Manage Archive Settings options

You can add an archive setting or edit an archive setting to apply a different retention category and different rules to the archived data. Changes that you make here affect all of the selections to which the archive setting applies.

See [“About archive settings in the Archiving Option”](#) on page 1247.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

**Table S-17** Manage Archive Settings options

Item	Description
<b>Archive Settings</b>	Displays the name of the archive settings to apply to the Exchange mailbox selection or file system selections.
<b>Retention Category</b>	Displays the name of the retention category.
<b>Retention Period</b>	Displays how long the items are retained in the archives for this retention category.
<b>Description</b>	Displays a description of the retention category.
<b>Add</b>	Lets you create an archive setting. See <a href="#">“Archive Settings Details”</a> on page 1248.
<b>Edit</b>	Lets you edit an existing archive setting. See <a href="#">“Archive Settings Details”</a> on page 1248.
<b>Delete</b>	Lets you delete an existing archive setting.
<b>Default Folder Archive Settings</b>	Displays the current settings for the default archive settings. See <a href="#">“Archive Settings Details”</a> on page 1248.

## Archive Settings Details

You can specify a retention category and archive rules to apply to data.

See [“Manage Archive Settings options”](#) on page 1247.

**Table S-18** Archive settings options

Item	Description
<b>Archive settings</b>	Specifies the name of the archive settings to apply to Exchange mailbox selections or file system selections.  You can apply these same archive settings to other selections.
<b>Name</b>	Specifies the name of the retention category to apply to the selections.

**Table S-18** Archive settings options (*continued*)

Item	Description
<b>New Retention Category</b>	Lets you create a new retention category. See " <a href="#">About retention categories for archived items</a> " on page 1250.
<b>Retention period</b>	Displays how long the items are retained in the archives for this retention category.
<b>Description</b>	Displays any description that was entered for this retention category.
<b>Name</b>	Displays the name for this archive rule.
<b>Action</b>	Indicates if the filter for this archive rule is set to include or exclude files when archiving.
<b>File Type</b>	Indicates the type of file that this archive rule applies to.
<b>Not accessed in</b>	Indicates if the files that have not been accessed in a specified number of days are included or excluded from the archive stage. The default is to include the files that have not been accessed in 30 days in the archive job.
<b>Not modified in</b>	Indicates if the files that have not been modified in a specified number of days are included or excluded from the archive stage .
<b>Not created in</b>	Indicates if the files that have not been created in a specified number of days are included or excluded from the archive stage.
<b>File size</b>	Indicates if the files that are greater than or equal to or less than or equal to a specified size are included or excluded from the archive stage. The default is to include the files that are greater than or equal to 10 MB in the archive job.

**Table S-18** Archive settings options (*continued*)

Item	Description
<b>Add</b>	Lets you add a rule to the list of rules in the archive settings. This rule applies when you run the archive job for the file system selections.  See <a href="#">“Archive Rule options”</a> on page 1253.
<b>Edit</b>	Lets you edit an existing rule in the archive settings.
<b>Delete</b>	Deletes a rule from the list of rules in the archive settings.
<b>Move Up</b>	Moves a rule up in the list of rules. An item is archived according to the first rule for which it meets the criteria. The top rule in the list is the first rule that applies.
<b>Move Down</b>	Moves a rule down in the list of rules.

## About retention categories for archived items

Use retention categories to specify the period of time for which you want to keep items in the archives. You can give the retention categories meaningful names, such as Business or Personal. Retention categories make it easier for you to retrieve items because you can search for them by their category name. Each retention category has a retention period, which indicates how long you want to retain the items that are archived with this retention category.

For example, you can create a retention category named Finance Data Retention and set it to retain archived data for seven years.

The retention period starts on the date that the item is archived. Backup Exec runs a daily operation that deletes all items that have expired retention periods. You can prevent this operation from running on specific archives.

See [“Preventing the deletion of expired archived items from an archive”](#) on page 1262.

You cannot delete retention categories. You can edit retention categories, including the retention periods.

Changes that you make to a retention category apply to the following:

- All items to which the retention category is already applied.

- Any new items to which you apply the retention category.  
See [“Adding or editing a retention category”](#) on page 1251.

You can create retention categories as needed when you create an archive job. You can also specify a retention category to use as the default setting for all archive jobs. If you do not specify a retention category, then a default retention category with a retention period of infinite is applied to an archive job.

See [“About creating an archive job”](#) on page 1225.

See [“Adding or editing a retention category”](#) on page 1251.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

## Adding or editing a retention category

You can add a retention category or edit an existing retention category. Changes apply to existing archived items as well as to new items to which you apply the retention category.

See [“About retention categories for archived items”](#) on page 1250.

### To add or edit a retention category

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 In the left pane, click **Archive**.
- 3 Click **Retention Categories**.
- 4 Do one of the following:

To add a retention category

Click **Add**, edit the appropriate information, and then click **OK**.

See [“Retention category properties”](#) on page 1252.

To edit a retention category

Do the following in the order listed:

- Select the retention category that you want to edit, and then click **Edit**.
- Edit the appropriate information, and then click **OK**.

See [“Retention category properties”](#) on page 1252.

- 5 Click **OK** on the Manage Retention Category dialog box, and click **OK** on the Archive Settings dialog box.

## Manage Retention Category options

You can add a retention category or edit a retention category to change the period of time for which you want to keep items in the archive. Changes that you make here affect all of the selections to which the retention category applies.

See [“Adding or editing a retention category”](#) on page 1251.

**Table S-19**      Manage Retention Category options

Item	Description
<b>Retention Category</b>	Displays the name of the retention category.
<b>Retention Period</b>	Displays how long the items are retained in the archives for this retention category.
<b>Description</b>	Displays a description of the retention category.
<b>Add</b>	Lets you create a retention category. See <a href="#">“Retention category properties”</a> on page 1252.
<b>Edit</b>	Lets you edit an retention category. See <a href="#">“Retention category properties”</a> on page 1252.

## Retention category properties

You can specify the period of time for which you want to keep items in the archives.

See [“Adding or editing a retention category”](#) on page 1251.

**Table S-20**      Retention category properties

Item	Description
<b>Retention category</b>	Displays the name of the retention category.
<b>Infinite</b>	Retains the item in the archives for an infinite amount of time. The retention period starts from the date that the item is archived.
<b>For a period of</b>	Retains the item in the archives for a specified period of time. The retention period starts from the date that the item is archived.

**Table S-20** Retention category properties (*continued*)

Item	Description
<b>Description</b>	Displays a description of the retention category.

## Adding or editing archive rules

See [“About retention categories for archived items”](#) on page 1250.

You can add or edit archive rules in the archive settings that apply to the archive jobs.

### To add or edit archive rules

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Archive Settings**.
- 4 Select an archive setting, and then click **Add** or **Edit**.
- 5 Under Archive Rules, do one of the following:

To add new archive rules	Click <b>Add</b> .
To edit archive rules	Select a rule, and then click <b>Edit</b> .
- 6 Edit the appropriate options.  
See [“Archive Rule options”](#) on page 1253.
- 7 Click **OK**.

## Archive Rule options

You can configure the rules that specify the characteristics of the data to include or exclude in the archive job.

See [“Adding or editing archive rules”](#) on page 1253.

**Table S-21** Options for archive rules

Item	Description
<b>Name</b>	Displays the name of the archive rule.

**Table S-21** Options for archive rules (*continued*)

Item	Description
<b>Include when archiving</b>	Specifies that the files that meet the requirements that you select are included in the archive job. This option is enabled by default.
<b>Exclude from archiving</b>	Specifies that the files that meet the requirements that you select are excluded from the archive job.
<b>Type of files</b>	Specifies the types of file to include or exclude from the archive job. You can type your own rule or use a predefined rule.
<b>Files not accessed in</b>	Includes or excludes the files that have not been accessed in a specified number of days. The default is to include the files that have not been accessed in 6 months in the archive job.
<b>Files not modified in</b>	Includes or excludes the files that have not been modified in a specified number of days.
<b>Files not created in</b>	Includes or excludes the files that have not been created in a specified number of days.
<b>File size</b>	Includes or excludes the files that are greater than or equal to, or less than or equal to a specified size. The default is to include the files that are greater than or equal to 10 MB in the archive job.

## About managing index locations in the Backup Exec Archiving Option

Index locations store all of the archived data content that is indexed to enable fast searching and retrieval of archived items.

You can manage index locations by doing the following:

- Add new index locations.  
 Add index locations to another disk or to a remote computer that has more space rather than moving the indexes to a new location. If you want a particular

location to be used for indexing, close all of the other index locations and leave one location open.

- **Open and close index locations.**

Close an index location to prevent new indexes from being created at that location. You can re-open index locations when appropriate. When you close a location, new items for existing indexes continue to use the closed location. New indexes, such as those for new archives, are created in the open index location. They do not use the closed location.

- **Delete index locations.**

Delete empty index locations. An index location becomes empty when all of the archived items that had index information in this location have expired.

See [“Viewing index locations”](#) on page 1255.

See [“Adding a new index location”](#) on page 1255.

See [“Opening or closing an index location”](#) on page 1257.

See [“Deleting an index location”](#) on page 1256.

## Viewing index locations

You can view index locations.

See [“About managing index locations in the Backup Exec Archiving Option”](#) on page 1254.

### To view index locations

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Index Locations**.
- 4 View the existing index locations.  
See [“Manage Index Locations options”](#) on page 1257.
- 5 Click **Close**.

## Adding a new index location

You can add index locations. For the best performance, do not place the index location paths on the same disks as vault partition paths.

---

**Note:** The index location must be on an NTFS drive, or on a UNC path on an NTFS network share. Mapped drives are not supported. The Backup Exec service account must be granted the NTFS Read and Write permissions for the index location path. The index location cannot be at the root of a volume. You must specify a path that has at least one folder name.

---

See [“About managing index locations in the Backup Exec Archiving Option”](#) on page 1254.

#### To add a new index location

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Index Locations**.
- 4 In the **Index location path** field, enter a new location, and then click **Add**.
- 5 Click **Close**.

## Deleting an index location

An index location must be empty before you can delete it. To empty an index location, use the Backup Exec Utility to move all index files to a different index location.

See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.

You cannot delete an index location if it is the only index location.

See [“About managing index locations in the Backup Exec Archiving Option”](#) on page 1254.

#### To delete an index location

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Index Locations**.
- 4 Select the index location that you want to delete.  
See [“Manage Index Locations options”](#) on page 1257.
- 5 Click **Delete**.

- 6 When you are prompted to delete the index location, click **Yes**.
- 7 Click **Close**.

## Opening or closing an index location

You can close an index location to prevent new indexes from being created at that location. Items can still be added to closed indexes. You can still perform searches on the index locations that are closed.

---

**Note:** Ensure that at least one index location is open. Archive jobs must be able to store index information for archived items. Without an open index location, archive jobs fail.

---

See [“About managing index locations in the Backup Exec Archiving Option”](#) on page 1254.

### To open or close an index location

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Index Locations**.
- 4 Select the index location that you want to open or close.  
See [“Manage Index Locations options”](#) on page 1257.
- 5 Click **Set Open** or **Set Close**, as appropriate.
- 6 Click **Close**.

## Manage Index Locations options

You can manage the Archiving Option index locations.

See [“Adding a new index location”](#) on page 1255.

**Table S-22** Manage Index Locations options

Item	Description
<b>Index location path</b>	<p>Indicates the path where you want to store the archive index files.</p> <p><b>Note:</b> The index location must be on an NTFS drive, or on a UNC path on an NTFS network share. Mapped drives are not supported. The Backup Exec service account must be granted the NTFS Read and Write permissions for the index location path. The index location cannot be at the root of a volume. You must specify a path that has at least one folder name.</p>
<b>Browse</b>	<p>Lets you browse the network and select an NTFS folder where you want to store the index files.</p>
<b>Index Locations</b>	<p>Displays all of the index locations that have been created or configured.</p>
<b>Status</b>	<p>Displays the state of the index location.</p> <p>Possible values include the following:</p> <ul style="list-style-type: none"> <li>■ Open</li> <li>■ Closed</li> </ul>
<b>Backup Mode</b>	<p>Displays <b>Yes</b> if the index location is currently being backed up; otherwise, displays <b>No</b>.</p> <p>When an index location is in backup mode, no new index data is written to that location. You can continue to search index locations that are in backup mode.</p>
<b>Add</b>	<p>Lets you add new index locations.</p> <p><b>Note:</b> For best performance, do not add an index location to the same disk on which vault partitions are located.</p> <p>See <a href="#">“Adding a new index location”</a> on page 1255.</p>
<b>Delete</b>	<p>Lets you delete an index location.</p> <p>See <a href="#">“Deleting an index location”</a> on page 1256.</p>

**Table S-22** Manage Index Locations options (*continued*)

Item	Description
Set Open	Lets you open an index location. See <a href="#">“Opening or closing an index location”</a> on page 1257.
Set Close	Lets you close an index location. See <a href="#">“Opening or closing an index location”</a> on page 1257.

## About restoring items from the archives

You can perform the following restore operations for archived items:

- Restore files to their original locations or to another file server.

---

**Note:** In the Restore Wizard, if you redirect the restore to another Exchange server, you must add two backslash characters (\\) in front of the Exchange server name. For example, if the Exchange server name is 'ExchangeServer01', you must enter '\\ExchangeServer01'. Otherwise, you cannot continue to the next page in the Restore Wizard.

---

- Restore mail messages to the original mailbox or to another mailbox on the Exchange server.

---

**Note:** The mailbox must already exist on the server to which you want to restore the mail messages.

---

The archives can contain multiple versions of the same item. To restore a specific version of the item, you must select it individually. Otherwise, Backup Exec restores the latest version of an item. You can distinguish between versions of the same file by checking the modified time of an item.

---

**Note:** NTFS permissions for archived data are not restored.

---

See [“About searching for and restoring data”](#) on page 229.

## About searching for data in the archives

You can search the archives to find and select the data in the archives. The archives contain access control restrictions, but these restrictions are not applied when you search from the Backup Exec Administration Console. The search displays all archived versions of the data.

You can specify criteria such as content, retention categories, or retention periods. You can also restrict the search to one archive or to all archives that are associated with a server. You can use wildcard characters. Use a question mark (?) to represent any single character. Use an asterisk (\*) to represent any number of characters.

See [“About searching for and restoring data”](#) on page 229.

## About deleting data from the archives

You can delete archived files and mail messages from the archives. If you need to free some disk space, you can delete items from the archives before their retention periods expire.

The archives can contain multiple versions of the same item. To delete a specific version of the item, you must select it individually. Otherwise, Backup Exec deletes the latest version of an item. You can distinguish between versions of the same file by checking the modified time of an item.

You can delete only files and mail messages from the archives. To delete an entire archive, you must delete it from the **Storage** tab.

Additionally, Backup Exec searches the vault store partitions daily to delete the archived items that have expired retention periods. You can specify the time at which this daily operation runs.

See [“Editing default settings for the Archiving Option”](#) on page 1230.

See [“Deleting an archive”](#) on page 1241.

See [“Deleting data from the archives”](#) on page 1260.

## Deleting data from the archives

You can delete specific data from the archives.

See [“About deleting data from the archives”](#) on page 1260.

### To delete data from the archives

- 1 On the **Backup and Restore** tab, double-click the server that you archived.
- 2 In the **Archive** group, click **Delete from Archive**.

- 3 Edit the options as appropriate.  
See [“Delete from Archive options”](#) on page 1261.
- 4 Click **OK**.

## Delete from Archive options

You can select the data that you want to delete from the archives.  
See [“Deleting data from the archives”](#) on page 1260.

**Table S-23** Delete from Archives options

Item	Description
<b>Name</b>	Specifies the name of the server that the data was archived from.
<b>Select the data that you want to delete:</b>	Lets you check the archived data that you want to delete.
<b>Name</b>	Displays the name of the data that you select to delete from the archives.

# About backing up and restoring the Archiving Option components from a remote Backup Exec server

You can back up and restore the Archiving Option components from a remote Backup Exec server on which licenses are not installed. You can also edit the backup job default settings for the Archiving Option components.

The remote Backup Exec server that you use to back up the Archiving Option components does not require licenses for the following options:

- File System Archiving Option
- Exchange Mailbox Archiving Option

You must provide the credentials of the Backup Exec service account on the Backup Exec server on which the Archiving Option is installed.

See [“About backing up Archiving Option components”](#) on page 1262.

See [“About searching for and restoring data”](#) on page 229.

See [“Setting default backup job settings”](#) on page 456.

## Preventing the deletion of expired archived items from an archive

Backup Exec deletes the archived items that have expired retention periods from a specific archive. You can clear this option to prevent Backup Exec from deleting expired archived items.

See “[About archives in the Archiving Option](#)” on page 1240.

### To prevent the deletion of expired archived items from an archive

- 1 On the Storage tab, expand the vault store that contains the archive.
- 2 Double-click the archive.
- 3 On the left, click **Properties**.
- 4 Disable the option **Automatically delete archived items that have expired retention periods**.
- 5 Click **OK**.

## About backing up Archiving Option components

You can select any or all of the Archiving Option components for backup. If you select all of the components for backup in the same job, recovery time is faster. However, if you create multiple backup jobs for the components, the backup jobs run faster.

The Archiving Option components that you can back up are described in the following table, along with recommendations for backup:

**Table S-24** Backing up Archiving Option components

Component	Description
Archiving Option Components	Archiving Option Components contain all of the components that are associated with the Archiving Option. Symantec recommends that you select Archiving Option Components to back up all of the Archiving Option environment.

**Table S-24** Backing up Archiving Option components (*continued*)

Component	Description
Backup Exec Archiving Site	<p>The Backup Exec Archiving Site is a logical representation of an installation of the Archiving Option. A Backup Exec server can have only one Archiving Site. If you select this component for backup, the Directory database is also automatically backed up.</p>
Directory database	<p>The Directory database is a Microsoft SQL Server database that contains configuration data and information about the archives.</p> <p>After the database is populated, the amount of data in the Directory database changes very little over time.</p> <p>You should back up the Directory database after you add or remove any Archiving Option component. You should also back up the Directory database if you change the location of any component. Configuration changes can include creating vault stores, creating vault store partitions, and changing vault store partition statuses.</p> <p>See <a href="#">“About disabling backup mode for Archiving Option components”</a> on page 1265.</p>
Index location	<p>The index location stores all of the archived data content that is indexed to enable fast searching and retrieval of archived items. The indexing data is stored in index files in the location that is specified when the Archiving Option is installed.</p> <p>You should back up the index location on a regular basis.</p>
Vault store group	<p>The vault store group is a logical entity. If you select it for backup, all of the vault databases, vault store partitions, and the fingerprint databases are backed up. Because these components are closely related, you should consider selecting the vault store group to back up all of these components together.</p>

**Table S-24** Backing up Archiving Option components (*continued*)

Component	Description
Fingerprint databases	<p>The fingerprint databases contains the single instance storage-related information for all of the vault stores in the vault store group.</p> <p>If you enable single instance storage of archived items, you should back up the fingerprint databases on a regular basis.</p> <p>See <a href="#">“About single instance storage of archived items”</a> on page 1233.</p>
Vault store	<p>The vault store is a logical entity. If you select it for backup, all of the vault databases and the vault store partitions are backed up.</p>
All partitions	<p>A vault store partition represents the physical location where the archived items are stored. A vault store can contain one or more vault store partitions. If you select <b>All Partitions</b> for backup, then all of the vault store partitions in the vault store are selected for backup.</p> <p><b>Note:</b> When you back up an open partition, the vault store database is automatically backed up.</p> <p>You should back up the vault store partitions on a regular basis.</p> <p>See <a href="#">“About vault store partitions in the Archiving Option”</a> on page 1238.</p>
Vault store databases	<p>The vault store databases are the Microsoft SQL Server databases that contain configuration data and information about the archives. Each vault store has an associated database. Each vault store database contains an entry for each item that is archived in the associated vault store. If an item is deleted from the archive, then the references to it are deleted from the vault store database.</p> <p>You should back up the vault store databases on a regular basis.</p>

You can also back up and restore the Archiving Option components from a remote Backup Exec server on which licenses are not installed.

See [“About backing up and restoring the Archiving Option components from a remote Backup Exec server”](#) on page 1261.

See [“Backing up data”](#) on page 163.

See [“About consistency checks for Archiving Option databases”](#) on page 1265.

## About consistency checks for Archiving Option databases

Backup Exec automatically checks the physical consistency of an Archiving Option database before a backup job and after a restore job. Any consistency check failures are reported in the Backup Exec job log. Backup Exec uses Microsoft SQL Server's utility Physical Check Only for consistency checks of Archiving Option databases.

For more information about the Physical Check Only utility, see the Microsoft SQL Server documentation.

## About disabling backup mode for Archiving Option components

When you back up the Directory database, ensure that the Archiving Option components are not in backup mode.

See [“Editing or viewing vault store properties”](#) on page 1236.

If a component is in backup mode, you must take it out of backup mode by running the task **Disable Backup Mode on Archiving Option entities** in the Backup Exec Utility.

See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.

## About restoring an Archiving Option component

You can restore any of the following Archiving Option components:

- Directory database
- Vault store databases
- Fingerprint databases
- Vault store partition
- Index location

---

**Note:** The procedures for redirecting restore jobs include running tasks in Backup Exec Utility to update the new locations of the restored components.

---

See [“About running the Backup Exec Utility to complete redirected restores of Archiving Option components”](#) on page 1266.

Review the scenarios in the following table to find the best procedure to restore an Archiving Option component.

**Table S-25**      Methods for restoring an Archiving Option component

Method	More information
If a data loss occurs, and you want to restore an Archiving Option component to the same location	See <a href="#">“About searching for and restoring data”</a> on page 229.
If hardware fails and a data loss occurs, and you want to restore an Archiving Option component to a different location	See <a href="#">“About moving Archiving Option components to a new location”</a> on page 1270.
If you want to move components to new hardware, such as to a new SQL Server or a new disk	See <a href="#">“About moving Archiving Option components to a new location”</a> on page 1270.

See [“About searching for and restoring data”](#) on page 229.

See [“About consistency checks for Archiving Option databases”](#) on page 1265.

## About running the Backup Exec Utility to complete redirected restores of Archiving Option components

You can run a redirected restore job if you want to restore one or more Archiving Option components to a different location. After the redirected restore job completes, you must run additional tasks in Backup Exec Utility to update the new locations of the restored components.

The following table lists the possible scenarios and the associated redirected restore solutions for Archiving Option components.

**Table S-26**      Redirected restore solutions for Archiving Option components

Scenario	Solution
The SQL Server that hosts the databases fails and a data loss occurs.	Do the following in the order listed: <ul style="list-style-type: none"><li>■ Redirect the restore of the Archiving Option databases to a new SQL Server. See <a href="#">“About searching for and restoring data”</a> on page 229.</li><li>■ Run the <b>Change Database Location</b> task in the Backup Exec Utility.</li><li>■ Run the <b>Update SQL Server Name</b> task in the Backup Exec Utility.</li></ul> See <a href="#">“Running the Backup Exec Utility to complete a redirected restore of the Archiving Option databases”</a> on page 1268.
The local drive or network share that hosts the vault store partition fails and a data loss occurs.	Do the following in the order listed: <ul style="list-style-type: none"><li>■ Redirect the restore of a vault store partition to a different path in a local drive or network share. See <a href="#">“About searching for and restoring data”</a> on page 229.</li><li>■ Run the <b>Change Vault Partition Path</b> in the Backup Exec Utility.</li></ul> See <a href="#">“Running the Backup Exec Utility before redirecting the restore of an Archiving Option vault store partition”</a> on page 1268.
The disk that contains the index files fails and a data loss occurs.	Do the following in the order listed: <ul style="list-style-type: none"><li>■ Redirect the restore of the index files to a new location. See <a href="#">“About searching for and restoring data”</a> on page 229.</li><li>■ Run the <b>Change Index Location</b> task in the Backup Exec Utility. See <a href="#">“Running the Backup Exec Utility before redirecting the restore of Archiving Option index files”</a> on page 1269.</li></ul>

## Running the Backup Exec Utility to complete a redirected restore of the Archiving Option databases

After you redirect the restore of the Archiving Option databases to a new SQL Server, you must run the **Change Database Location** task in Backup Exec Utility.

See [“About running the Backup Exec Utility to complete redirected restores of Archiving Option components”](#) on page 1266.

**To run the Backup Exec Utility to complete a redirected restore of the Archiving Option databases**

- 1 When the redirected restore job is complete, start the **Backup Exec Utility**.  
See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.
- 2 In the **Backup Exec Utility** task pane, under **Archiving Option Tasks**, click **Change Database Location**.
- 3 In **Destination SQL server instance**, type the name of the new SQL Server.
- 4 Click **OK**.
- 5 In the **Backup Exec Utility** task pane, under **Archiving Option Tasks**, click **Update SQL Server Name**.
- 6 After the operation completes, exit the Backup Exec Utility.

## Running the Backup Exec Utility before redirecting the restore of an Archiving Option vault store partition

You can redirect the restore of a vault store partition to a different path in a local drive or network share.

If you restore a vault store partition that has an **Open** status, its vault store database is automatically restored.

See [“About running the Backup Exec Utility to complete redirected restores of Archiving Option components”](#) on page 1266.

If a vault store partition needs more disk space, you can create a new partition.

### To run the Backup Exec Utility before redirecting the restore of an Archiving Option vault store partition

- 1 Start the **Backup Exec Utility**.  
See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.
- 2 In the **Backup Exec Utility** task pane, under **Archiving Option Tasks**, click **Change Vault Partition Path**.
- 3 Select the name of the vault store partition.
- 4 In **New Vault Store Partition Path**, type the new path to which you want to restore the vault store partition.
- 5 Ensure that **Move Vault Store Partition Files** is not selected.
- 6 Click **OK**.
- 7 On the Backup Exec Administration Console, start the Restore Wizard to restore the vault store partition..  
See [“About searching for and restoring data”](#) on page 229.

## Running the Backup Exec Utility before redirecting the restore of Archiving Option index files

You can redirect the restore of the index files to a new location.

---

**Note:** You must locate the index files on a local NTFS drive.

---

See [“About restoring an Archiving Option component”](#) on page 1265.

### To run the Backup Exec Utility before redirecting the restore of Archiving Option index files

- 1 Start the **Backup Exec Utility**.  
See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.
- 2 In the **Backup Exec Utility** task pane, under **Archiving Option Tasks**, click **Change Index Location**.
- 3 In **New Index Location**, type the new path to which you want to restore the index files.
- 4 Ensure that **Move Index Files** is not selected.

- 5 Click **OK**
- 6 On the Backup Exec Administration Console, create a restore job to restore the index files.  
See [“About searching for and restoring data”](#) on page 229.

## Running the Backup Exec Utility to complete Archiving Option operations

You must run the Backup Exec Utility to complete some operations for an Archiving Option component.

See [“About running the Backup Exec Utility to complete redirected restores of Archiving Option components”](#) on page 1266.

### To run the Backup Exec Utility to complete Archiving Option operations

- 1 From the Backup Exec installation directory, double-click **BEUtility.exe**.
- 2 In the **Properties** pane, under **Archiving Option Tasks**, click the appropriate task.
- 3 Click **Help** for information about a task.

## About moving Archiving Option components to a new location

You can use the Backup Exec Utility to move Archiving Option components to a new location. Ensure that no other archive-related operations are running when you move a component.

If you must move a component because the hardware that hosts the component has failed, you should use a redirected restore job.

See [“About running the Backup Exec Utility to complete redirected restores of Archiving Option components”](#) on page 1266.

**Table S-27** Moving Archiving Option components to a new location

Component	More information
Index location	You can move an index location if the disk where the index files are stored runs out of space. Use the <b>Change Index Location</b> task in Backup Exec Utility.

**Table S-27** Moving Archiving Option components to a new location (*continued*)

Component	More information
Databases	<p>You can move databases to a different SQL Server. For example, you can move the databases if the current SQL Server becomes overloaded.</p> <p>Use the <b>Change Database Location</b> task in Backup Exec Utility.</p>
Vault store partitions	<p>You can move vault store partitions if you must remove the current drive or network share that contains the partition.</p> <p><b>Note:</b> If a vault store partition only requires more disk space, you can create a new partition and designate it as open.</p> <p>Use the <b>Change Vault Store Partition Path</b> task in Backup Exec Utility.</p>

See [“Running the Backup Exec Utility to complete Archiving Option operations”](#) on page 1270.

## Troubleshooting archive jobs

If there are issues with archive jobs, you can find information in the following sources:

- Backup Exec job logs.  
See [“Viewing the job log”](#) on page 264.
- Enterprise Vault event log that is located in the Windows Event Viewer.  
See [“Viewing the Enterprise Vault event log for Archiving Option events”](#) on page 1272.
- Backup Exec diagnostic utilities.  
See [“About the Backup Exec diagnostic application”](#) on page 665.

An Exchange Mailbox Archiving Option job may not find data to archive for the following reasons:

- Only back up sets for which the Granular Recovery Technology option was enabled and that exist on disk storage devices can be archived.
- The associated Exchange mail stores may not be backed up, or the mailbox or user may have been deleted in the last 14 days.

A File System Archiving Option job can only find data to archive if backup sets are on disk storage devices.

See [“Requirements for both the Exchange Mailbox Archiving Option and the File System Archiving Option”](#) on page 1199.

## Viewing the Enterprise Vault event log for Archiving Option events

You can view the Windows Event Viewer to review the Enterprise Vault event log for information about Archiving Option events. Enterprise Vault generates many log entries. You must take some action to make sure that the log files do not grow too large. For information on how to control the log file size, see the Windows Event Viewer help.

## Reports for the Archiving Option

The reports in the following table are available to help you monitor your Archiving Option environment.

See [“About reports in Backup Exec”](#) on page 556.

**Table S-28** Reports for the Archiving Option

Report	Description
<b>Vault Store Usage Summary</b>	Displays the archived items that are in each vault store and the total size of the vault store.
<b>Vault Store Usage Details</b>	Displays the archives that are in each store and the size of each archive.
<b>File System Archive Settings</b>	Displays the archive settings that are applied to archive selections for each server.
<b>Exchange Mailbox Group Archive Settings</b>	Displays the archive settings that are applied to mailbox groups in each domain.
<b>Archive Selections by Archive Rules and Retention Categories</b>	Displays the archive rules and retention categories that are applied to each archive selection.
<b>Archive Job Success Rate</b>	Displays the number of archive jobs that ran successfully.
<b>Failed Archive Jobs</b>	Displays a list of archive jobs that failed recently.

**Table S-28** Reports for the Archiving Option (*continued*)

Report	Description
<b>Overnight Archive Summary</b>	Displays a summary of archive jobs for the last 24 hours.

## About Backup Exec Virtual Vault

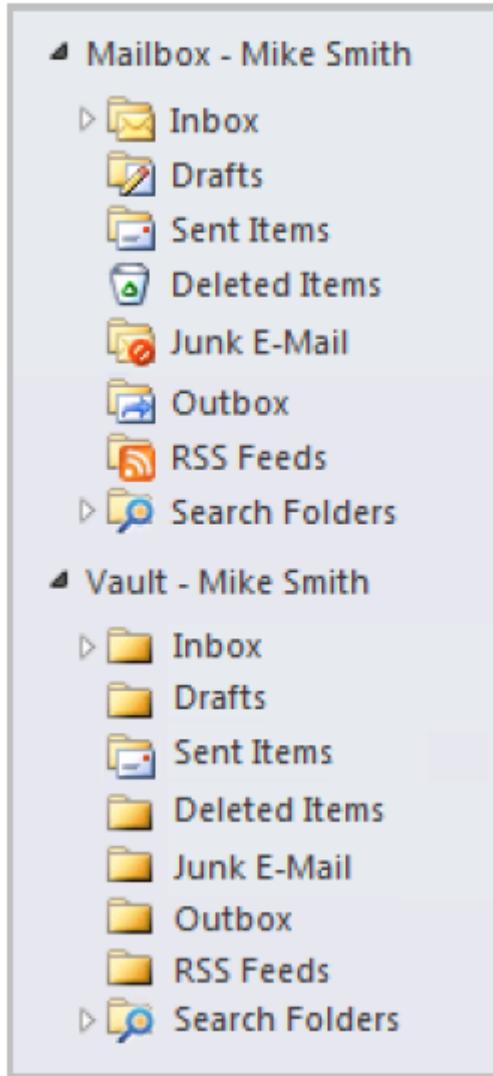
After an archive job runs on an end user's mailbox, the email messages are archived and stored in an archive on the network. Each archived Exchange mailbox has its own archive on the network. Typically, only the administrator can access the archives on the network. However, with Backup Exec's Virtual Vault feature, the end users can access their archived email messages from a vault on their Outlook Navigation Pane.

The Backup Exec administrator must make the Backup Exec Outlook Add-In (add-in) available to the end users to install on their computers. The add-in is a component of the Virtual Vault feature that runs on the end user's computer. The add-in maintains a cache that is called the Vault Cache on each end user's computer. The add-in regularly synchronizes the end user's Vault Cache with the mailbox archive on the network. The Vault Cache acts like a local copy of an end user's archived mailbox.

End users can view, search, read, forward, and reply to the email messages in their vaults. End users cannot move, delete, or rename a folder in their vaults. End users can also search the contents of their vaults by using Outlook Instant Search, Outlook Advanced Find, or Windows Desktop Search.

In the following example, the vault for the end user named Mark Smith appears as **Vault - Mark Smith**.

**Figure S-1** An example of an end user's vault on the Outlook Navigation Pane



Backup Exec's Virtual Vault feature is automatically installed and enabled on the Backup Exec server when you install or upgrade the Backup Exec Exchange Mailbox Archiving Option. Virtual Vault is enabled for all mailbox groups by default. The Backup Exec administrator can disable the use of Virtual Vault for all end users that belong to a mailbox group.

See [“About installing the Backup Exec Outlook Add-In to end users' computers”](#) on page 1276.

See [“Best practices for Virtual Vault”](#) on page 1281.

See [“About using the command line to install the Backup Exec Exchange Mailbox Archiving Option”](#) on page 1218.

See [“About configuring Outlook in cached Exchange mode”](#) on page 1281.

See [“About enabling and disabling Virtual Vault ”](#) on page 1286.

## About the Backup Exec Outlook Add-In

The Backup Exec Outlook Add-In is a component of Backup Exec's Virtual Vault. The add-in must be installed on the end users' computers.

The add-in maintains the end user's Vault Cache. The Vault Cache is a location that stores the archived email message headers and the email message contents that are downloaded from the Backup Exec server. These items are downloaded from the Backup Exec server when the Vault Cache synchronizes with the mailbox archives on the network. To synchronize the Vault Cache, the add-in connects to the Backup Exec server by using the DNS alias that you entered during the Archiving Option installation or upgrade.

End users can perform the following tasks by using the Backup Exec Outlook Add-In:

- Start synchronization between the Vault Cache and the Backup Exec server.
- Suspend or resume synchronization.
- Edit the size of the Vault Cache.
- Specify the amount of time that Backup Exec waits after Outlook starts before it starts synchronization.

The Backup Exec Outlook Add-In contains Help that the end users can access on their computers. The Help is located on the Outlook toolbar, in **Help > Backup Exec Help Topics**.

See [“About installing the Backup Exec Outlook Add-In to end users' computers”](#) on page 1276.

See [“About the Vault Cache”](#) on page 1281.

## About installing the Backup Exec Outlook Add-In to end users' computers

Several methods are available to install the Backup Exec Outlook Add-In to end users' computers.

**Table S-29** Installation methods for the Backup Exec Outlook Add-In

Installation method	Information
Copy the Backup Exec Outlook Add-In.msi file to a network share that end users can access. Then, send instructions to specific end users about how to install the add-in.	See <a href="#">“Installing the Backup Exec Outlook Add-In by copying it to a network share”</a> on page 1280.
Use the command line to install the Backup Exec Outlook Add-In.msi file to remote computers, one at a time.	See <a href="#">“Installing the Backup Exec Outlook Add-In by using the command line (Silent Mode)”</a> on page 1276.
Install the Backup Exec Outlook Add-In in an Active Directory network.	See <a href="#">“Installing the Backup Exec Outlook Add-In in an Active Directory network”</a> on page 1277.
Use Microsoft's System Center Configuration Manager to deploy the Backup Exec Outlook Add-In to end users' computers.	See your Microsoft documentation for instructions on how to use System Center Configuration Manager, or search the Symantec Knowledge Base for specific instructions.

### Installing the Backup Exec Outlook Add-In by using the command line (Silent Mode)

You can use the command line to install the Backup Exec Outlook Add-In to a single computer.

See [“About installing the Backup Exec Outlook Add-In to end users' computers”](#) on page 1276.

**To install the Backup Exec Outlook Add-In by using the command line (Silent Mode)**

- 1 Open a Windows command prompt.
- 2 Type the following command:

```
msiexec /i <path to the Backup Exec Outlook Add-In.msi package>
/qn+ ALLUSERS=1
```

- 3 Optionally, to add logging, type the following command:

```
msiexec /i <path to the Backup Exec Outlook Add-In.msi package>
/qn+ /lv* <Path to log file> ALLUSERS=1
```

**Installing the Backup Exec Outlook Add-In in an Active Directory network**

You can centrally manage the installation of the Backup Exec Outlook Add-In to computers in an Active Directory network. You configure the installation once, and then use a Group Policy Object to assign that installation to computers in an Organizational Unit. The add-in is installed automatically whenever a computer in the Organizational Unit is restarted.

See [“About installing the Backup Exec Outlook Add-In to end users' computers”](#) on page 1276.

---

**Note:** Review your organization's deployment plans before you implement a rollout of the Backup Exec Outlook Add-In to client computers. You should also review your Group Policy Desktop Management and Active Directory documentation.

---

**Table S-30** Installing the Backup Exec Outlook Add-In in an Active Directory network

Step	Action	Description
Step 1	Create a distribution point (share) that contains the source file that you want to install.	You must copy the Backup Exec Outlook Add-In package to the distribution point.  See <a href="#">“Creating a software distribution point to deploy the Backup Exec Outlook Add-In”</a> on page 1278.

**Table S-30** Installing the Backup Exec Outlook Add-In in an Active Directory network (*continued*)

Step	Action	Description
Step 2	Configure a Group Policy Object to assign the directory in the distribution point to computers in an Active Directory Organizational Unit.	<p>The software is installed automatically when the computers in the Organizational Unit are restarted.</p> <p><b>Note:</b> Computers in the Organizational Unit may need to be restarted twice if the Windows Fast Logon Optimization feature is enabled.</p> <p>See <a href="#">“Configuring a Group Policy Object for the Backup Exec Outlook Add-In”</a> on page 1279.</p>

## Creating a software distribution point to deploy the Backup Exec Outlook Add-In

To install the Backup Exec Outlook Add-In in an Active Directory network, you must create a software distribution point (share).

See [“Installing the Backup Exec Outlook Add-In in an Active Directory network”](#) on page 1277.

**Table S-31** Creating a software distribution point

Step	Description
Step 1	Create a shared folder, and then set read-only permissions for all of the client computers to which you want to deploy the package.
Step 2	Copy the Symantec Backup Exec Add-In.msi package to the shared folder.
Step 3	<p>Configure a Group Policy Object to deploy the source files.</p> <p>See <a href="#">“Configuring a Group Policy Object for the Backup Exec Outlook Add-In”</a> on page 1279.</p>

## Configuring a Group Policy Object for the Backup Exec Outlook Add-In

To install the Backup Exec Outlook Add-In in an Active Directory network, you must configure a Group Policy Object after you create a software distribution point.

See [“Creating a software distribution point to deploy the Backup Exec Outlook Add-In”](#) on page 1278.

Refer to your Microsoft Windows documentation for information on configuring a Group Policy Object.

---

**Note:** Symantec recommends that you create a new Group Policy Object and apply it only to the computers to which you want to deploy the Backup Exec Outlook Add-In.

---

### To configure a Group Policy Object for the Backup Exec Outlook Add-In

- 1 From the Active Directory snap-in that manages users and groups, right-click the domain name, and then click **Properties**.
- 2 Create a new Group Policy Object.
- 3 Under **Computer Configuration**, expand **Software Settings**.
- 4 Right-click **Software Installation**, click **New**, and then click **Package**.
- 5 On the **File Open** dialog box, browse to the software distribution point by using the UNC name.
- 6 Select the package file `Symantec Backup Exec Outlook Add-In.msi`, and then click **Open**.
- 7 When you are prompted, click **Advanced**.
- 8 After Active Directory checks the MSI package, on the **General Properties** tab, ensure that the correct version of the option is selected for installation.
- 9 On the **Deployment** tab, set up the configuration for your environment.
- 10 Ensure that the option **Make this 32-bit x86 application available to WIN64 machines** is selected.
- 11 Close all of the dialog boxes.

## Installing the Backup Exec Outlook Add-In by copying it to a network share

The Backup Exec Outlook Add-In is a component of the Virtual Vault feature, and must be installed on an end user's computer. You can copy the Backup Exec Outlook Add-In to a network share that is accessible to end users. Then, you can send instructions to the end users whom you want to install the Backup Exec Outlook Add-In.

You can copy and paste the instructions that are included in the following procedures in an email message to the end users.

See [“About installing the Backup Exec Outlook Add-In to end users' computers”](#) on page 1276.

### To copy the Backup Exec Outlook Add-In to a network share

- 1 At the Backup Exec server, place the installation media in the appropriate drive.
- 2 Navigate to the following directory on the installation media:  
BE\WinNT\Install\EVE\Outlook Add-In
- 3 Copy the .msi file to a network share to which end users also have access.
- 4 In the following instructions for end users, replace the text in brackets with the actual name of the network share to which you have copied the .msi file.
- 5 Send the following instructions to the end users whom you want to install the Backup Exec Outlook Add-In.

### To install the Backup Exec Outlook Add-In

- 1 On your computer, close Outlook.
- 2 Navigate to the following folder:  
*<Enter the name of the network share to which you have copied the .msi file >*
- 3 Double-click `Symantec Backup Exec Outlook Add-In.msi`.
- 4 Follow the instructions on your screen.
- 5 In Outlook, turn on cached Exchange mode.  
For instructions on how to configure cached Exchange mode, refer to your Outlook Help.
- 6 In Outlook, turn off AutoArchive.  
For instructions on how to turn off AutoArchive, refer to your Outlook Help.
- 7 Restart Outlook.

## About configuring Outlook in cached Exchange mode

The end user must configure Outlook in cached Exchange mode to enable the vault to appear in the Outlook Navigation Pane, as well as to allow preemptive caching. Preemptive caching lets the items that are almost eligible for archiving to be archived in the Vault Cache directly from the Outlook offline folders. These items do not have to be downloaded from the Backup Exec server. The Backup Exec Outlook Add-In copies email messages from the end user's Outlook .OST file to the Vault Cache.

End users should see their Outlook Help for more information about how to set cached Exchange mode.

See [“Installing the Backup Exec Outlook Add-In by copying it to a network share”](#) on page 1280.

## Best practices for Virtual Vault

After you install the Backup Exec Outlook Add-In for a few end users, monitor the Backup Exec server's performance to ensure that it performs within acceptable limits. For large organizations, it may be beneficial to phase the availability of the Virtual Vault feature to the end users.

You can limit the number of end users who can use Virtual Vault by doing one or both of the following actions:

- Enable Virtual Vault for specific mailbox groups.  
See [“About enabling and disabling Virtual Vault ”](#) on page 1286.
- Make the Backup Exec Outlook Add-In available only to specific end users.  
See [“Installing the Backup Exec Outlook Add-In by copying it to a network share”](#) on page 1280.

## About the Vault Cache

A Vault Cache is a location on the end user's computer that stores the archived email messages that are downloaded from the Backup Exec server. These items are downloaded from the Backup Exec server when the Vault Cache synchronizes with the archives on the network. The end user's vault on the Outlook Navigation Pane reflects the contents from the Vault Cache rather than the contents from the archive on the network.

By default, the Vault Cache is created in the following locations when the end user installs the Backup Exec Outlook Add-In:

- For Windows XP, in `\Documents and Settings\`

- For Windows Vista/7, in \Users\\AppData\Local\KVS\Enterprise Vault

The Outlook Reading Pane shows the selected email message header. If the email message is in the Vault Cache, the Reading Pane also shows the content. If only the email message header is shown but no content, the Reading Pane displays a link to the original email message.

The Vault Cache is limited to a maximum of 10% of free space on the end user's computer or to 1 GB, whichever is smaller. After the limit is reached, the oldest email messages are automatically deleted from the Vault Cache to make room for new email messages. Even though the archived email messages are deleted from the end user's Vault Cache, the messages are still kept in the archives on the network.

End users can synchronize another user's archive to their Vault Cache if they have the correct permissions. A separate vault is displayed in the end user's Outlook Navigation Pane for each archive on the network that is synchronized to the Vault Cache. Instructions on how to synchronize to other archives on the network is provided in the Backup Exec Outlook Add-In Help on the end users' computers.

---

**Note:** Vault Cache is not available to Microsoft Entourage users.

---

The end user can edit the settings in the Backup Exec Outlook Add-In to manage their Vault Cache.

See [“About the Backup Exec Outlook Add-In”](#) on page 1275.

See [“About Vault Cache synchronization”](#) on page 1282.

## About Vault Cache synchronization

Vault Cache synchronization updates the end user's Vault Cache with any changes that are made to the archives on the network. These changes include the email messages that were created, updated, and deleted since the last synchronization.

The Vault Cache synchronization process consists of the following:

- Header synchronization

Updates the Vault Cache with information about archived email messages.

The email message header contains enough information to enable the message to be represented in the end user's vault in the Outlook Navigation Pane. The email message header also contains information to associate the header with the content of the email message. Where changes have occurred in the archives on the network, Vault Cache synchronization downloads header information from the Backup Exec server. The changes are then applied to the Vault Cache.

Header synchronization also synchronizes any changes that are made to the folder hierarchy in the archives on the network.

- **Content synchronization**

Downloads the archived email messages from one or more archives on the network to the Vault Cache.

After the end user installs the Backup Exec Outlook Add-In, the initial header synchronization automatically starts three minutes after Outlook starts. Content synchronization may also be performed. If the archive contains a large number of items, content synchronization takes much longer than header synchronization.

A vault is automatically added to an end user's Outlook profile when the following criteria are met:

- The Exchange archive job has processed all of the archives that the end user can access.
- The initial header synchronization has completed.
- The end user has not previously removed the vault from the profile.

After the Exchange Mailbox Archiving job runs and after the Vault Cache synchronization completes, the Vault Cache is current with the mailbox archives on the network.

Vault Cache synchronization can start in the following ways:

- The Backup Exec Outlook Add-In automatically synchronizes the Vault Cache with the archives on the network once a day. If the add-in cannot connect to Backup Exec, then it waits for five minutes before it attempts to contact the Backup Exec server again.

If a scheduled synchronization time is missed, the add-in attempts a synchronization the next time that the end user opens Outlook. By default, the add-in waits three minutes after the end user opens Outlook before it attempts to retry a missed synchronization. This default can be changed by the end user.

- The end user can manually start the Vault Cache synchronization at any time. A manual synchronization does not affect the next scheduled time for automatic synchronization. Unlike a scheduled synchronization, a manual synchronization that fails is not retried.

End users may miss the scheduled Vault Cache synchronization on a weekend when they do not use Outlook. In this situation, a large number of header synchronization requests may occur around the same time on Monday. To avoid an excessive load on the Backup Exec server, only a limited number of header synchronization requests are accepted. Because of this limitation, scheduled synchronization may not process immediately for some end users. No error messages are displayed to end users if their synchronization is not

processed immediately. Their header synchronization request is repeated every five minutes until it succeeds. When the synchronization succeeds, the daily scheduled synchronization time is reset to the time of the successful synchronization.

Backup Exec restricts the number of active content download requests at any given time. Backup Exec preconfigures this setting to control the amount of system resources that the Vault Cache content downloads use. The content download from the Backup Exec server to the Vault Cache uses Microsoft Background Intelligent Transfer Service technology.

End users can access the Backup Exec Outlook Add-In Help for information about how to view the synchronization status, and how to synchronize the Vault Cache.

See [“About Backup Exec Virtual Vault”](#) on page 1273.

## About preemptive caching

To minimize downloads to the Vault Cache, the Backup Exec Outlook Add-In regularly searches the Outlook .OST cache file for any email messages that are due to be archived soon. The Backup Exec Outlook Add-In automatically adds these email messages to the Vault Cache. This feature is called preemptive caching. Preemptive caching takes place on the end user's computer. It reduces the number of items that must be downloaded from the archive on the network to the Vault Cache when the two are synchronized.

The Backup Exec Outlook Add-In performs preemptive caching for email messages seven days before they are due for archiving as per the Exchange archiving settings for the mailbox.

The end user must configure Outlook in cached Exchange mode for preemptive caching to work. The Outlook Add-In copies email messages from the end user's Outlook .OST file to the Vault Cache. If the end user's Outlook does not have a .OST file, then preemptive caching cannot be performed.

See [“About configuring Outlook in cached Exchange mode”](#) on page 1281.

## About the temporary cache location on the Backup Exec server

If new items are added to the archive on the network, copies of these items are held temporarily in a cache on the Backup Exec server. The items are then downloaded to the end user's computer. When you install the Backup Exec Archiving Option, the cache location is set by default to a folder in the installation directory. Typically, this directory is C:\Program Files\Symantec\Backup Exec\AOCache.

Backup Exec notifies you if the cache location on the Backup Exec server reaches the maximum size that is specified. If you do not free some disk space, or specify another cache location, then the oldest items in the cache are deleted to free some space.

You can change the location of the cache, and increase the size of the cache.

See [“Changing the temporary cache location”](#) on page 1285.

See [“Changing the temporary cache size”](#) on page 1285.

## Changing the temporary cache location

You can change the location of the temporary cache on the Backup Exec server. The temporary cache location is used to synchronize the archived email messages with the Vault Cache on the end users' computers. The temporary cache location must be on a local NTFS drive. Mapped drives are not supported. The temporary cache location cannot be at the root of a volume. You must specify a path that has at least one folder name. The Backup Exec service account must be granted the NTFS rights Read and Write for the temporary cache location.

See [“About the temporary cache location on the Backup Exec server”](#) on page 1284.

---

**Note:** You must restart the Backup Exec services before the changes can take effect.

---

### To change the temporary cache location

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Under **Virtual Vault Settings**, enter a new cache location.
- 4 Click **OK**.

## Changing the temporary cache size

The default maximum size of 10 GB is used for the temporary cache on the Backup Exec server. The temporary cache location is used to synchronize the archived email messages with the Vault Cache on the end users' computers. You can increase the size of the temporary cache as needed.

See [“About the temporary cache location on the Backup Exec server”](#) on page 1284.

#### To change the temporary cache size

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Under **Virtual Vault Settings**, in the **Maximum cache size** field, select a size for the cache.
- 4 Click **OK**.
- 5 Restart the Backup Exec services for the changes to take effect.

## About enabling and disabling Virtual Vault

By default, Virtual Vault is enabled for all mailbox groups. The Backup Exec administrator can disable the use of Virtual Vault for all end users that belong to a mailbox group.

Enabling or disabling Virtual Vault on mailbox groups takes effect only after the Backup Exec server synchronizes the settings with the end users' mailboxes. This synchronization operation may take a few minutes. Then, end users must restart Outlook before changes to Virtual Vault can take effect.

If you disable Virtual Vault for end users, the files in the Vault Cache on the end users' computers are not removed automatically. The files can remain in the Vault Cache to be reused if you enable Virtual Vault again.

See [“Enabling and disabling Virtual Vault for mailbox groups”](#) on page 1286.

### Enabling and disabling Virtual Vault for mailbox groups

You can enable or disable Virtual Vault for the end users that are in a mailbox group.

See [“About enabling and disabling Virtual Vault”](#) on page 1286.

#### To enable and disable Virtual Vault for mailbox groups

- 1 Click the Backup Exec button, select **Configuration and Settings**, and then select **Backup Exec Settings**.
- 2 On the left, click **Archive**.
- 3 Click **Mailbox groups**.

**4** Select the domain, and then do one of the following:

To create a new mailbox group for which you want to enable or disable Virtual Vault Click **New**.

To enable or disable Virtual Vault for an existing mailbox group Select the mailbox group, and then click **Edit**.

**5** Do one of the following:

To enable Virtual Vault for all of the end users in the mailbox group Ensure that **Enable Virtual Vault** is selected. This option is enabled by default.

To disable Virtual Vault for all of the end users in the mailbox group Clear the **Enable Virtual Vault** check box.

**6** Click **OK**.



# Accessibility and Backup Exec

This appendix includes the following topics:

- [About accessibility and Backup Exec](#)
- [About keyboard shortcuts in Backup Exec](#)
- [List box navigation in Backup Exec](#)
- [Tabbed dialog box navigation in Backup Exec](#)
- [About setting accessibility options](#)

## About accessibility and Backup Exec

Symantec products meet federal accessibility requirements for software as defined in Section 508 of the Rehabilitation Act:

<http://www.access-board.gov/508.htm>

Symantec products are compatible with operating system accessibility settings as well as a variety of assistive technologies. All manuals also are provided as accessible PDF files, and the online help is provided as HTML displayed in a compliant viewer.

Keyboard navigation is available for all graphical user interface operations and menu items. Backup Exec uses standard operating system navigation keys.

Items in the task pane that do not have keyboard shortcuts can be accessed by using the operating system's "mouse keys", which allow you to control the mouse through the numerical keyboard.

To see a table of the standard Microsoft navigation keys and keyboard shortcuts, select your version of Microsoft Windows from the table at:

<http://www.microsoft.com/enable/products/keyboard.aspx>

## About keyboard shortcuts in Backup Exec

All menu items can be selected by using accelerator or mnemonic keyboard shortcuts. An accelerator is a key combination that provides shortcut access to a user interface function. A mnemonic (sometimes referred to as a "hotkey ") is a key equivalent (used in combination with the **Alt** key) for selecting user interface components such as menu items. The mnemonic "hotkey " letter is on the item in the user interface.

Select secondary menu items by opening the main menu and using the up or down arrow key until the item is highlighted. Press the right arrow key to open a submenu, and press **Enter** to select your choice.

Keyboard shortcuts are not case-sensitive. Mnemonic keystrokes may be pressed either sequentially or simultaneously. All menu items have mnemonics, but not all menu items have accelerators.

Routine functions such as opening, saving, and printing files can be performed using the standard Microsoft keyboard shortcuts. Other menu items are unique to Backup Exec.

The following table lists keyboard shortcuts to display labels and the contents of the Backup Exec button:

**Table T-1** Keyboard shortcuts in Backup Exec

Accelerator	Mnemonic	Result
Alt	F10	Displays the mnemonic label for a tab that you can use in combination with the accelerator to display the tab.
Alt	A	Expands the Backup Exec button. Use the Backup Exec button to connect to the Backup Exec server, configure settings, and access installation and licensing items. You can also access Backup Exec documentation, technical support items, and various Symantec Web sites .

### Home tab keyboard shortcuts

The following table lists the keyboard shortcuts for the **Home** tab.

See [“About keyboard shortcuts in Backup Exec”](#) on page 1290.

**Table T-2** Home tab keyboard shortcuts

Accelerator	Mnemonic	Command	Result
Alt	H	Home tab	Opens the <b>Home</b> tab.
Alt	1	One Column	Displays the <b>Home</b> tab items in one column.
Alt	2	Two Columns	Displays the <b>Home</b> tab items in two columns.
Alt	NW	Narrow/Wide	Displays the <b>Home</b> tab items in two columns with a narrow panel and a wide panel.
Alt	3	Three Columns	Displays the <b>Home</b> tab items in three columns.
Alt	D	Reset Home Tab	Restores the contents of the <b>Home</b> tab to the default configuration.

## Backup and Restore tab keyboard shortcuts

The following table lists the keyboard shortcuts for the **Backup and Restore** tab.

See [“About keyboard shortcuts in Backup Exec”](#) on page 1290.

See [“Backup and Restore tab keyboard shortcuts for the Jobs view”](#) on page 1294.

See [“Backup and Restore tab keyboard shortcuts for the Job History view ”](#) on page 1295.

See [“Backup and Restore tab keyboard shortcuts for the Backup Sets view ”](#) on page 1296.

See [“Backup and Restore tab keyboard shortcuts for the Active Alerts view ”](#) on page 1297.

See [“Backup and Restore tab keyboard shortcuts for the Credentials view ”](#) on page 1298.

**Table T-3 Backup and Restore tab keyboard shortcuts**

Accelerator	Mnemonic	Command	Result
Alt	B	Backup and Restore tab	Opens the <b>Backup and Restore</b> tab.
Alt	ST	Standard	Displays Backup Exec in a view that provides descriptive text.
Alt	CO	Compact	Displays Backup Exec in a view that conserves space.
Alt	F	Sort and Filter	Displays information in a custom view or lets you create and save a custom view.
Alt	T	Tree	Displays items in a hierarchal view.  This command is disabled for the list of servers on the <b>Backup and Restore</b> tab.
Alt	L	List	Displays items in a list that you can sort by columns.  This command is disabled for the list of servers on the <b>Backup and Restore</b> tab.
Alt	G	Groups	Lets you view information by server group. You can add, remove, or edit a server group.
Alt	B	Backup	Defines backup jobs and settings to back up your data.  You can back up data now, or schedule a time to do it.
Alt	O	One-Time Backup	Defines backup jobs and settings to run one time.
Alt	E	Edit Backups	Lets you edit one or more existing backup jobs.  You cannot edit synthetic or one-time backups.
Alt	CA	Backup Calendar	Lets you view all scheduled backup jobs on a calendar.

**Table T-3**      **Backup and Restore** tab keyboard shortcuts (*continued*)

Accelerator	Mnemonic	Command	Result
Alt	RE	Restore	Browses the backup sets from a single server, and then restores the data.
Alt	SE	Search	Searches for backup sets, and then restores the data, or copies and saves the search criteria.
Alt	CV	Convert	Converts backup data to a virtual machine.  You must run a full backup that includes all critical system components before you can convert backup data to a virtual machine.
Alt	AS	Add	Adds one or more servers to the list of servers.  You must add servers to back them up and monitor them.
Alt	AV	Add VMware Server	Adds a VMware vCenter or ESX server to the list of servers.  You must add the VMware server to back up its guest systems from the host server.
Alt	RS	Remove	Removes one or more servers from the list of servers.  You can remove servers from the list if you no longer want to back them up.
Alt	US	Update	Updates the selected Backup Exec servers with the latest hot fixes and service packs.
Alt	HA	Hold Job Queue	Pauses the job queue. Active jobs continue to run, but no new jobs run until the queue is taken off hold.

**Table T-3** Backup and Restore tab keyboard shortcuts (*continued*)

Accelerator	Mnemonic	Command	Result
Alt	RN	Run Next Backup Now	Runs the next scheduled backup for the selected servers.

## Backup and Restore tab keyboard shortcuts for the Jobs view

The following table lists the **Backup and Restore** tab keyboard shortcuts for the Jobs view.

See [“Backup and Restore tab keyboard shortcuts”](#) on page 1291.

**Table T-4** Backup and Restore tab keyboard shortcuts for the Jobs view

Accelerator	Mnemonic	Command	Result
Alt	JE	Edit	Lets you edit a backup definition.  You can edit a backup definition's backup selections, backup settings, and stages.
Alt	JD	Delete	Deletes a backup definition if you no longer need it.
Alt	JC	Cancel	Cancels an active job while it is running.
Alt	JP	Priority	Increases or decreases a job's priority in the job queue .
Alt	JR	Run Now	Runs a job immediately.  If a job is scheduled it still runs at its scheduled time.
Alt	JH	Hold	Pauses a job or the entire job queue.  The job or job queue resumes its normal schedule when you deselect this option.
Alt	JT	Test Run	Runs a test of the selected backup job now.

**Table T-4**      **Backup and Restore** tab keyboard shortcuts for the Jobs view  
*(continued)*

Accelerator	Mnemonic	Command	Result
Alt	JA	Job Activity	Lets you view statistical and system information about a running job. You can also cancel an active job.
Alt	HH	View Job History	Lets you view detailed information about the job history including individual job and job summary statistics.

### Backup and Restore tab keyboard shortcuts for the Job History view

The following table lists the **Backup and Restore** tab keyboard shortcuts for the Job History view.

See [“Backup and Restore tab keyboard shortcuts”](#) on page 1291.

**Table T-5**      **Backup and Restore** tab keyboard shortcuts for the Job History view

Accelerator	Mnemonic	Command	Result
Alt	HR	Run Now	Runs a job immediately. If the job is scheduled, it still runs at its scheduled time.
Alt	HL	View Job Log	Lets you view the job log for the selected job history.  The job log provides detailed job information, storage and media information, job options, file statistics, and job completion status.
Alt	HD	Delete	Deletes the selected job history and its associated job log, if you no longer need them.

**Table T-5** **Backup and Restore** tab keyboard shortcuts for the Job History view *(continued)*

Accelerator	Mnemonic	Command	Result
Alt	HH	View Job History	Lets you view detailed information about the job history including individual job and job summary statistics.
Alt	HC	Duplicate	Creates a duplicate copy of the job history, which includes all of a job's dependent backup sets.  You can duplicate the job history now, or schedule a time to do it.
Alt	HV	Verify	Verifies the integrity of the collection of data and the media on which it resides for this job history.  When you verify a job history, you verify all of a job's dependent backup sets. You can verify the job history now, or schedule a time to do it.

### **Backup and Restore** tab keyboard shortcuts for the Backup Sets view

The following table lists the **Backup and Restore** tab keyboard shortcuts for the Backup Sets view.

See [“Backup and Restore tab keyboard shortcuts”](#) on page 1291.

**Table T-6** **Backup and Restore** tab keyboard shortcuts for the Backup Sets view

Accelerator	Mnemonic	Command	Result
Alt	SD	Delete	Deletes the selected backup set, if you no longer need it.

**Table T-6**      **Backup and Restore** tab keyboard shortcuts for the Backup Sets view *(continued)*

Accelerator	Mnemonic	Command	Result
Alt	SH	Retain	Retains the selected backup set.  You can prevent backup sets from expiring by retaining them.
Alt	SC	Catalog	Catalogs the selected backup set.  Cataloging backup sets lets you view the data that is contained in them and search for files to restore.
Alt	SU	Duplicate	Creates a duplicate copy of the selected backup set.  You can duplicate the backup set now, or schedule a time to do it.
Alt	SV	Verify	Verifies the integrity of the collection of data and the media on which it resides for this backup set.  You can verify the backup set now, or schedule a time to do it.

### **Backup and Restore** tab keyboard shortcuts for the Active Alerts view

The following table lists the **Backup and Restore** tab keyboard shortcuts for the Active Alerts view.

See [“Backup and Restore tab keyboard shortcuts”](#) on page 1291.

**Table T-7 Backup and Restore tab keyboard shortcuts for the Active Alerts view**

Accelerator	Mnemonic	Command	Result
Alt	AR	Respond	Lets you view the alert and any additional information.  You must select Respond OK to clear the alert.
Alt	AO	Respond OK	Clears the alert without displaying information about it.  Respond OK only if you no longer need the alert.
Alt	AL	View Job Log	Lets you view the job log that was generated for this job.  The job log provides detailed job information, storage and media information, job options, file statistics, and job completion status.
Alt	AC	Copy Text	Copies the text of the alert. For example, you can paste the text into a text file or email.
Alt	AH	Show Alert History	Displays alerts that you have responded to or that you have automatically cleared.

### **Backup and Restore tab keyboard shortcuts for the Credentials view**

The following table lists the **Backup and Restore** tab keyboard shortcuts for the Credentials view.

See [“Backup and Restore tab keyboard shortcuts”](#) on page 1291.

**Table T-8**      **Backup and Restore** tab keyboard shortcuts for the Credentials view

Accelerator	Mnemonic	Command	Result
Alt	CT	Test/Edit Credentials	Lets you test or edit the account credentials for the selected backup source. You can also change the credentials for a source if they are not correct.
Alt	CR	Refresh	Updates the list of credentials with any new credential information.

## Storage tab keyboard shortcuts

The following table lists the keyboard shortcuts for the **Storage** tab.

See [“About keyboard shortcuts in Backup Exec”](#) on page 1290.

See [“Storage tab keyboard shortcuts for the Jobs view ”](#) on page 1302.

See [“Storage tab keyboard shortcuts for the Job History view ”](#) on page 1304.

See [“Storage tab keyboard shortcuts for the Backup Sets view ”](#) on page 1305.

See [“Storage tab keyboard shortcuts for the Active Alerts view ”](#) on page 1306.

**Table T-9**      **Storage** tab keyboard shortcuts

Accelerator	Mnemonic	Command	Result
Alt	S	Storage tab	Opens the <b>Storage</b> tab.
Alt	ST	Standard	Displays Backup Exec in a view that provides descriptive text.
Alt	CO	Compact	Displays Backup Exec in a view that conserves space.
Alt	F	Sort and Filter	Displays information in a custom view or lets you create and save a custom view.
Alt	T	Tree	Displays items in a hierarchal view.
Alt	L	List	Displays items in a list that you can sort by columns.

**Table T-9** Storage tab keyboard shortcuts (*continued*)

Accelerator	Mnemonic	Command	Result
Alt	SP	Pause	Pauses a device to prevent scheduled and new jobs from running on it.
Alt	SD	Disable	Disables a device so that it is available for other applications.
Alt	SO	Offline	Troubleshoots the device to bring it online. No operations are allowed on this device until it is online again.
Alt	CC	Configure Storage	Launches the <b>Configure Storage</b> wizard to set up different types of storage to which you can back up data.
Alt	CT	Troubleshoot	Lets Backup Exec troubleshoot the device and provide possible solutions.
Alt	CD	Delete	Removes an item from the Backup Exec Database.
Alt	CS	Share	Shares a device between Backup Exec servers.
Alt	SS	Scan	Let you get information about the media that are in the slots, and then update the Backup Exec Database.
Alt	SI	Inventory	Mounts the media in tape drives, reads the media label, and updates the Backup Exec Database.  You can inventory media now, or schedule when to do it.
Alt	SC	Catalog	Logs information about the backup sets and the storage device on which the backup sets are stored.

**Table T-9** Storage tab keyboard shortcuts (*continued*)

Accelerator	Mnemonic	Command	Result
Alt	SG	Inventory and Catalog	<p>Mounts the media in tape drives, reads the media label, and updates the Backup Exec Database.</p> <p>Also, logs information about the backup sets and the storage device on which the backup sets are stored.</p>
Alt	SZ	Initialize	Sends a startup command to the robotic library.
Alt	SB	Label	<p>Writes a new media label on the media in the drive.</p> <p>Labeling destroys any data that exists on the media.</p>
Alt	SE	Erase	<p>Writes an indicator at the beginning of the media that makes the data on the media inaccessible.</p> <p>Long erase physically erases the entire media.</p>
Alt	VB	Blink	Blinks the status lights on the physical disk to help identify it in a virtual disk.
Alt	VU	Unblink	Turns off the blinking status lights on the physical disk.
Alt	VC	Configure Virtual Disk	Configures a virtual disk on a storage array for use with Backup Exec.
Alt	JR	Run Now	<p>Runs a job immediately.</p> <p>If a job is scheduled it still runs at its scheduled time.</p>

**Table T-9** Storage tab keyboard shortcuts (*continued*)

Accelerator	Mnemonic	Command	Result
Alt	MA	Associate with media set	Specifies the append period and the overwrite protection period of a media set to apply to a media.  You can select storage and press <b>Enter</b> to view more detailed information about media set operations and media vault operations.
Alt	MS	Scratch	Associates the media with the Scratch media set so that Backup Exec can use it in an overwrite backup job.  You can select storage and press <b>Enter</b> to view more detailed information about media set operations and media vault operations.
Alt	MT	Retire	Associates the media with the Retired media set so that Backup Exec cannot use it for backup jobs.  You can select storage and press <b>Enter</b> to view more detailed information about media set operations and media vault operations.
Alt	MV	Move media to vault	Lets you type the labels or scan the barcode labels to move the media to a media vault.  You can select storage and press <b>Enter</b> to view more detailed information about media set operations and media vault operations.

### Storage tab keyboard shortcuts for the Jobs view

The following table lists the **Storage** tab keyboard shortcuts for the Jobs view.

See “[Storage tab keyboard shortcuts](#)” on page 1299.

**Table T-10** Storage tab keyboard shortcuts for the Jobs view

Accelerator	Mnemonic	Command	Result
Alt	JE	Edit Backups	Edits one or more existing backup jobs.  You cannot edit synthetic or one-time backups.
Alt	JE	Edit	Lets you edit a backup definition.  You can edit a backup definition's backup selections, backup settings, and stages.
Alt	JD	Delete	Deletes a backup definition if you no longer need it.
Alt	JC	Cancel	Cancels an active job while it is running.
Alt	JP	Priority	Increases or decreases a job's priority in the job queue.
Alt	JR	Run Now	Runs a job immediately.  If a job is scheduled it still runs at its scheduled time.
Alt	JH	Hold	Pauses a job or the entire job queue.  The job or job queue resumes its normal schedule when you deselect this option.
Alt	JT	Test Run	Runs a test of the selected backup job now.
Alt	JA	Job Activity	Lets you view statistical and system information about a running job. You can also cancel an active job.
Alt	HH	View Job History	Lets you view detailed information about the job history including individual job and job summary statistics.

## Storage tab keyboard shortcuts for the Job History view

The following table lists the **Storage** tab keyboard shortcuts for the Job History view.

See [“Storage tab keyboard shortcuts”](#) on page 1299.

**Table T-11** Storage tab keyboard shortcuts for the Job History view

Accelerator	Mnemonic	Command	Result
Alt	HR	Run Now	Runs a job immediately.  If the job is scheduled, it still runs at its scheduled time.
Alt	HL	View Job Log	Lets you view the job log for the selected job history.  The job log provides detailed job information, storage and media information, job options, file statistics, and job completion status.
Alt	HD	Delete	Deletes the selected job history and its associated job log, if you no longer need them.
Alt	HH	View Job History	Lets you view detailed information about the job history including individual job and job summary statistics.
Alt	HC	Duplicate	Creates a duplicate copy of the job history, which includes all of a job's dependent backup sets.  You can duplicate the job history now, or schedule a time to do it.

**Table T-11** Storage tab keyboard shortcuts for the Job History view *(continued)*

Accelerator	Mnemonic	Command	Result
Alt	HV	Verify	<p>Verifies the integrity of the collection of data and the media on which it resides for this job history.</p> <p>When you verify a job history, you verify all of a job's dependent backup sets. You can verify the job history now, or schedule a time to do it.</p>

### Storage tab keyboard shortcuts for the Backup Sets view

The following table lists the **Storage** tab keyboard shortcuts for the Backup Sets view.

See [“Storage tab keyboard shortcuts”](#) on page 1299.

**Table T-12** Storage tab keyboard shortcuts for the Backup Sets view

Accelerator	Mnemonic	Command	Result
Alt	SD	Delete	Deletes the selected backup set, if you no longer need it.
Alt	SH	Retain	Retains the selected backup set. You can prevent backup sets from expiring by retaining them.
Alt	SC	Catalog	<p>Catalogs the selected backup set.</p> <p>Cataloging backup sets lets you view the data that is contained in them and search for files to restore.</p>
Alt	SU	Duplicate	<p>Creates a duplicate copy of the selected backup set.</p> <p>You can duplicate the backup set now, or schedule a time to do it.</p>

**Table T-12** Storage tab keyboard shortcuts for the Backup Sets view  
*(continued)*

Accelerator	Mnemonic	Command	Result
Alt	SV	Verify	Verifies the integrity of the collection of data and the media on which it resides for this backup set.  You can verify the backup set now, or schedule a time to do it.

### Storage tab keyboard shortcuts for the Active Alerts view

The following table lists the **Storage** tab keyboard shortcuts for the Active Alerts view.

See [“Storage tab keyboard shortcuts”](#) on page 1299.

**Table T-13** Storage tab keyboard shortcuts for the Active Alerts view

Accelerator	Mnemonic	Command	Result
Alt	AR	Respond	Lets you view the alert and any additional information.  You must select Respond OK to clear the alert.
Alt	AO	Respond OK	Clears the alert without displaying information about it.  Respond OK only if you no longer need the alert.
Alt	AL	View Job Log	Lets you view the job log that was generated for this job.  The job log provides detailed job information, storage and media information, job options, file statistics, and job completion status.
Alt	AC	Copy Text	Copies the text of the alert. For example, you can paste the text into a text file or email.

**Table T-13**      **Storage** tab keyboard shortcuts for the Active Alerts view  
*(continued)*

Accelerator	Mnemonic	Command	Result
Alt	AH	Show Alert History	Displays alerts that you have responded to or that you have automatically cleared.

## Reports tab keyboard shortcuts

The following table lists the keyboard shortcuts for the **Reports** tab.

See “[About keyboard shortcuts in Backup Exec](#)” on page 1290.

**Table T-14**      **Reports** tab keyboard shortcuts

Accelerator	Mnemonic	Command	Result
Alt	R	Run Report Now	Runs a selected report immediately.
Alt	C	New Custom Report	Creates a new report that uses the report options that you select.
Alt	N	New Scheduled Report	Schedules a report to run on a specific date and time.
Alt	E	Edit	Edits a scheduled report or report options for a custom report.
Alt	P	Copy	Lets you make a copy of a custom report. Backup Exec saves a copy of the report in the Custom report group, along with the original report.
Alt	D	Delete	Deletes a custom report, a scheduled report, or a completed report.

## General keyboard navigation within the Backup Exec user interface

You can navigate and use Backup Exec with only the keyboard. In the user interface, the current active tree or table has a dark blue highlight, and the current

active tab, radio button, or check box is enclosed within a rectangle formed by dotted lines. These areas are said to have focus and will respond to commands.

All Symantec user interfaces use the following keyboard navigation standards:

- The **Tab** key moves the focus to the next active area, field, or control, following a preset sequence. **Shift+Tab** moves the focus in the reverse direction through the sequence.
- **Ctrl+Tab** exits any console area that you internally navigate with the **Tab** key.
- Up and down arrow keys move focus up and down the items of a list.
- The **Alt** key in combination with the underlined mnemonic letter for a field or command button shifts the focus to that field or button.
- **Enter** activates your selection. For example, after pressing the **Tab** key to select **Next** in a wizard panel, press **Enter** to display the next screen.
- **Shift+F10** provides access to context menus.

## Keyboard navigation within dialog boxes in Backup Exec

Dialog boxes contain groups of controls that are necessary to set options or settings for programs.

The following list contains some general rules about dialog box navigation:

- The **Tab** key moves the focus between controls within the dialog box along a preset sequence.
- A dark border indicates the default command button. Press **Enter** at any time to choose the button with a dark border.
- **Esc** chooses the Cancel button if one exists.
- The spacebar chooses a control you select with the **Tab** key.
- The spacebar changes the state of a check box that has focus. Typing a mnemonic (if one is available) will move the focus to the check box and change its state.
- Arrow keys move the focus in radio buttons, list boxes, sliders, groups of option controls, or groups of page tabs.
- Items that cannot be changed are not visited by the **Tab** key sequence. Options that are unavailable are grayed-out and can neither be selected nor given focus.

While the controls described here are typically found in dialog boxes, they also can occur in other contexts. The same navigation standards will apply.

## List box navigation in Backup Exec

List boxes display a column of available choices.

There are different kinds of list boxes with the following additional navigation conventions:

- Drop-down list boxes by default show only the selected item. A small button to the right of the control shows a downward-pointing arrow. Select the arrow to display more items from the list box. If there are more choices than can fit in the preset list box area, a slider appears along the side of the list box. Show or hide the list using **Alt+Down** arrow, **Alt+Up** arrow, or **F4**. The **Tab** key selects an item.
- Extended selection list boxes support selecting single items, blocks of items, or combinations of the two. After selecting an item, hold down **Ctrl**+navigation keys to select or clear additional items or blocks of items.

## Tabbed dialog box navigation in Backup Exec

Some dialog boxes use tabbed pages to subcategorize groups of many options. Each tabbed page contains different groups of controls. Use **Tab** to move the focus between tabbed pages within a dialog box. Typing the mnemonic for a tab also moves the focus to the tabbed page and displays its page of controls.

The following table lists keyboard navigation rules within tabbed dialog boxes:

**Table T-15** Keyboard navigation within tabbed dialog boxes

Keyboard input	Result
<b>Ctrl+Page Down</b> or <b>Ctrl+Tab</b>	Switches to the next tab and displays the page.
<b>Ctrl+ Page Up</b>	Switches to the previous tab and displays the page.
Right arrow or Left arrow	When the focus is on a tab selector, chooses the next or previous tab in the current row and displays the page.

## About setting accessibility options

Symantec software responds to operating system accessibility settings.

Symantec products are compatible with Microsoft's accessibility utilities. In Windows operating systems, accessibility options involving keyboard

responsiveness, display contrast, alert sounds, and mouse operation can be set through the Control Panel.

Accessibility features are primarily for the English version. Localized versions of this product include support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys.

For more information on setting accessibility options, see the Microsoft documentation.

# Glossary

<b>ADAMM (Advanced Device and Media Management)</b>	A Backup Exec database that automates the tracking of tape and disk cartridge media. ADAMM expires the backup sets that are stored on tape and disk cartridge media according to the associated media set.
<b>administration console</b>	The user interface that allows you to run Backup Exec operations. The user interface can be run from the Backup Exec server or from a remote computer.
<b>Agent for Windows</b>	A Backup Exec system service that runs on Microsoft Windows computers and allows remote backup and restore of those computers.
<b>agent</b>	A component that allows computers such as Microsoft SQL Server to interact with the Backup Exec server.
<b>alert category</b>	A group of one or more events that occur in Backup Exec and that can generate an alert. Examples of alert categories include Job Success, Install Warning, and Database Maintenance Failure.
<b>alert source</b>	A source that can generate an alert. Alert sources include jobs, media, storage devices, and computers.
<b>alert type</b>	The classification of an alert that lets you determine the severity of the alert. Alert types include Error, Warning, Information, and Attention Required.
<b>alert</b>	An event in Backup Exec that usually requires some form of user interaction or acknowledgment.
<b>allocated media</b>	The tape or disk cartridge media that are associated with a media set and that have current append and overwrite protection periods.
<b>append period</b>	The length of time that data can be added to tape or disk cartridge media. The append period starts when the first backup job is written to the media.
<b>archive</b>	A logical group of archived items that the Backup Exec Archiving Option creates. Archives are contained in vault store partitions. Each archived file system share has its own archive. Each archived Exchange mailbox has its own archive.
<b>audit log</b>	A running history of all actions that are performed in Backup Exec. An entry into the log is created each time an action occurs that is configured to display in the audit log.
<b>Backup Exec server pool</b>	A feature of the Backup Exec Central Admin Server Option that lets you group managed Backup Exec servers in a pool to which you can restrict backup jobs.

<b>Backup Exec server</b>	The computer on which Backup Exec is installed and where the Backup Exec services are running.
<b>Backup Exec service account</b>	A user account that is configured for the Backup Exec system services. It contains a user name and password and provides the rights to log on as a service and to act as a Backup Exec administrator.
<b>backup method</b>	An option that you select when you run a backup job to specify a full, differential, or incremental backup.
<b>backup set</b>	A collection of data that is backed up from a single source of content. For example, a single source of content can be a server or it can be a Microsoft Exchange dataset. If you select multiple sources of contents, Backup Exec creates multiple backup sets.
<b>backup strategy</b>	The procedures that you implement for backing up your network. Backup strategies include what methods of backup are performed and when backups are performed.
<b>baseline</b>	The first backup job to run in a synthetic backup. The baseline backup runs one time only and backs up all of the files on the selected computer. A full backup is assembled, or synthesized, from a baseline backup and the subsequent incremental backups.
<b>catalog</b>	A database that Backup Exec creates during a backup or archive operation. When you select data to restore, Backup Exec uses the catalog information to find the restore selections and the storage devices on which they reside.
<b>central administration server</b>	A Backup Exec server on which the Central Admin Server Option (CASO) is installed. In a CASO environment, the central administration server provides centralized administration, delegated job processing, and load balancing functionality for managed Backup Exec servers.
<b>centralized catalog</b>	A catalog location in the Central Admin Server Option. All of the files in the catalog are kept on the central administration server.
<b>cloud storage</b>	An online storage location on multiple virtual servers to which you can back up data.
<b>common encryption key</b>	A type of encryption key that anyone can use to back up data using encryption and to restore encrypted data.
<b>custom error-handling rule</b>	An error-handling rule that you can define for a specific error code in an error category. When a job fails with the error code that is associated with the custom error-handling rule, the retry options and the final job disposition are applied to the job.
<b>differential</b>	A backup method that includes all files that have changed since the last full backup.
<b>disk storage</b>	A location on a locally attached internal hard drive, a USB device, a FireWire device, or a network-attached storage device to which you can back up data.

<b>distributed catalog</b>	A catalog location in the Central Admin Server Option. Image files in the catalog are distributed to the central administration server from every managed Backup Exec server. These distributed files are small because they do not contain the entire catalog. They contain only information about the backup set. The history files, which contain detailed information about the backup set, remain on the managed Backup Exec server.
<b>error-handling rule</b>	A default or custom rule that sets retry options and the final job disposition for failed or canceled jobs. Retry options let you specify how often to retry a job if it fails and the time to wait between retry attempts. The final job disposition lets you place the job on hold until you can fix the error.
<b>event</b>	An action that occurs during a Backup Exec operation, such as a job cancellation.
<b>full</b>	A backup method that includes all of the files that you select for backup.
<b>granular restore</b>	A restore of individual items from a backup for which you enable the Granular Recovery Technology option.
<b>GRT (Granular Recovery Technology)</b>	A backup option that is available with some Backup Exec agents. Granular Recovery Technology lets you restore individual items from database backups. A separate backup of the individual items is not required for you to recover one item.
<b>imported media</b>	The media that are created by a product other than this installation of Backup Exec, but are in storage devices in the Backup Exec environment.
<b>incremental</b>	A backup method that backs up only the files that have changed since the last full or incremental backup.
<b>job delegation</b>	A process by which jobs are distributed by a central administration server to available storage devices on managed Backup Exec servers. Job delegation is only available with the Central Admin Server Option.
<b>job history</b>	A list of completed and failed backup, restore, and storage operation jobs.
<b>job log</b>	A log that contains the results of a job. It is created when the job runs. You can review the job log for job errors and job details.
<b>job</b>	An operation that has been scheduled for processing by the Backup Exec server. Jobs contain source or destination information, settings, and a schedule. Types of jobs include backup, restore, data discovery, reports, test run, and storage operations.
<b>legacy backup-to-disk folder</b>	A storage device used in versions prior to Backup Exec 2012 that you could create to back up data to a folder on a hard disk. For Backup Exec 2012, these legacy backup-to-disk folders are read-only. Symantec recommends that you use disk storage devices instead.
<b>load balancing</b>	A feature in Backup Exec that automatically distributes jobs among any available storage devices in a storage device pool.

Also a feature of the Backup Exec Central Admin Server Option in which jobs are automatically distributed from a central administration server to multiple managed Backup Exec servers for processing among the various storage devices.

<b>logon account</b>	An account that stores the credentials of a Windows user account and that enables Backup Exec to manage user names and passwords. It can be used to browse data sources or to process jobs.
<b>mailbox group</b>	A group of user mailboxes to which you want to assign the same archive rules, retention categories, and vault stores in the Backup Exec Archiving Option. In Enterprise Vault, this is called a provisioning group.
<b>managed Backup Exec server</b>	A Backup Exec server that is managed by a central administration server. Managed Backup Exec servers are responsible for the actual processing of backup and restore jobs in a Central Admin Server Option environment. Managed Backup Exec servers are only available with the Backup Exec Central Admin Server Option.
<b>media ID</b>	A unique internal label that Backup Exec assigns to each media used in Backup Exec. The ID keeps statistics for each media. The media ID cannot be erased or changed.
<b>media label</b>	A label used to identify media. Backup Exec can assign the label automatically, but you can rename it. If the media was first used in a library with a barcode reader, the media label will already have a barcode label.
<b>media overwrite protection level</b>	A global setting in Backup Exec that lets you specify whether to overwrite scratch, imported, or allocated tape drive or disk cartridge media regardless of the media's overwrite protection period.
<b>media rotation</b>	A strategy that determines when tape or disk cartridge media can be reused, or rotated back into use, by Backup Exec. Common examples of a media rotation strategy are Son, Father/Son, and Grandfather/Father/Son.
<b>media set</b>	A set of rules that apply to tape and disk cartridge media that are associated with a media set. These rules specify append periods, overwrite protection periods, and vaulting periods.
<b>media vault</b>	A logical representation of the actual physical location of tape and disk cartridge media, such as a special media room, a scratch bin, or an offsite location.
<b>offhost backup</b>	A feature of the Backup Exec Advanced Disk-based Backup Option that enables the backup operation to be processed on a Backup Exec server instead of on the remote computer, or host computer. Moving the backup from the remote computer to a Backup Exec server enables better backup performance and frees the remote computer as well.
<b>Offline Tape/Disk Cartridge Media vault</b>	A location on the <b>Storage</b> tab that displays the tape and disk cartridge media that are on-site but are not in tape drives, robotic libraries, or media vaults. Media are

	automatically moved to the offline vault if you use Backup Exec to remove media from a tape drive or robotic library.
<b>Online Tape/Disk Cartridge Media vault</b>	A location on the <b>Storage</b> tab that displays the tape and disk cartridge media that are available in tape drives or robotic libraries. You cannot add or move media to the online media vault. Backup Exec does that automatically.
<b>overwrite protection period</b>	The length of time that data is retained on a specific tape or disk cartridge media before being overwritten (unless the media is erased, formatted, moved to scratch media, or if the media overwrite protection level is set to None). The overwrite protection period is measured from the last time data was appended to the media.
<b>preferred server configuration</b>	A collection of one or more servers and sites that you select as preferred backup sources. Preferred server configurations take priority as backup sources in instances where data is replicated between multiple servers.
<b>recyclable media</b>	Tape or disk cartridge media that are assigned to a media set but have expired data overwrite protection periods.
<b>remote administrator</b>	The Backup Exec user interface (Administration Console) that is run on remote computers.
<b>replicated catalog</b>	A catalog location in the Central Admin Server Option. All of the files in the catalog are replicated from the managed Backup Exec server to the central administration server.
<b>data discovery</b>	A Backup Exec feature that allows the detection of new backup content within a Windows domain.
<b>restricted encryption key</b>	A type of encryption key that anyone can use to back up data using encryption. Only the key owner or a user with knowledge of the pass phrase can restore data that was encrypted with a restricted encryption key.
<b>retention category</b>	A setting in the Backup Exec Archiving Option that lets you specify the period of time for which you want to keep items in the archives. You can name a retention category to make it easier to search for and retrieve archived items.
<b>retired media</b>	Tape or disk cartridge media that has been taken out of service, usually because of an excessive number of errors. Media that is retired is available for restore jobs but not for backup jobs. Media must be retired before it can be deleted. If you want to use media that has been deleted, Backup Exec recognizes it as imported media. You must catalog retired media before you can restore from it.
<b>scratch media</b>	Tape or disk cartridge media that are not associated with a media set and that can be overwritten. Scratch media includes new or blank media, erased media, and media moved from another group.
<b>simulated tape library</b>	A tape library that emulates an Advanced Intelligent Tape (AIT) media type and has the AIT media type label. A simulated tape library is created by the Tape Library Simulator.

<b>stage</b>	An additional task that you can run with a backup job, such as duplicating a copy of the backup data to disk storage.
<b>storage device pool</b>	A group of similar types of storage devices that enables load-balancing of Backup Exec jobs.
<b>storage device</b>	A disk storage device, disk cartridge, cloud storage device, robotic library drive, stand-alone drive, virtual drive, removable storage drive, or other type of data storage that is supported by Backup Exec.
<b>synthetic backup</b>	A feature of the Advanced Disk-based Backup Option that enables a full backup to be assembled, or synthesized, from a baseline and subsequent incremental backups.
<b>Tape Library Simulator</b>	A utility that lets you create a virtual device on a hard disk or on any mounted volume on a computer on which the Backup Exec Remote Media Agent for Linux is installed. The virtual device that is created is called a simulated tape library.
<b>true image restore</b>	A feature of the Advanced Disk-based Backup Option that enables Backup Exec to restore the contents of directories to what they were at the time of any full or incremental backup. Restore selections are made from a view of the directories as they existed at the time of the particular backup. Files that were deleted before the time of the backup are not restored. In true image restore, only the correct versions of files are restored from the appropriate full or incremental backups that contain them. Previous versions are not unnecessarily restored and then overwritten.
<b>UMI (Unique Message Identifier)</b>	A unique code that is associated with an error reported in the job log, or on some alerts. These codes contain hyperlinks that you can click to go to the Symantec Technical Support Web site. You can access technical notes and troubleshooting tips that are related to a specific error.
<b>vault store partition</b>	The physical location on a disk where archived items are stored, if the Backup Exec Archiving Option is installed. Backup Exec creates one vault store partition in each vault store by default. As the data in a vault store grows, you can create more vault store partitions to provide additional capacity.
<b>vault store</b>	A disk-based container for the archived data that the Backup Exec Archiving Option archives from one server.
<b>virtual disk</b>	A logical disk that you configure on a storage array to provide storage to the Backup Exec server.

# Index

## A

- accelerator
  - defined 1290
- accessibility
  - dialog boxes 1308
  - keyboard navigation 1307
  - keyboard shortcuts 1290
    - Backup and Restore tab 1291
    - Backup and Restore tab for the Active Alerts view 1297
    - Backup and Restore tab for the Backup Sets view 1296
    - Backup and Restore tab for the Credentials view 1298
    - Backup and Restore tab for the Job History view 1295
    - Backup and Restore tab for the Jobs view 1294
    - Home tab 1290
    - Reports tab 1307
    - Storage tab 1299
    - Storage tab for the Active Alerts view 1306
    - Storage tab for the Backup Sets view 1305
    - Storage tab for the Job History view 1304
    - Storage tab for the Jobs view 1302
  - overview 1289
  - settings 1309
- active alerts
  - responding to 285
- Active Directory
  - backing up in Exchange 847
- Active File Exclusion 848
- active jobs
  - about managing and monitoring 247
  - canceling 252
  - holding 253
  - job activity options 248
  - removing a hold 253
  - statuses 254
  - viewing job activity 248
  - viewing properties 248
- Add
  - Remote Media Agent for Linux 1143
- administration console
  - overview 131
  - role in backup process 44
- Advanced Disk-based Backup Option
  - baseline
    - setting 1048
  - best practices for offhost backup 1054
  - host computer
    - defined 1052
  - offhost backup 1055
  - offhost backup overview 1052
  - transportable snapshots
    - defined 1052
  - true image restore
    - overview 1050
- Agent for Linux
  - about backing up 1090
  - about establishing trust 734
  - about exclusions from backup 1082
  - backing up Novell OES components 1093
  - backup job options 1091
  - beoper group, defined 1078
  - configuration options in the ralus.cfg file 1083
  - configuring the ralus.cfg file 1081
  - creating the beoper group 1079
  - default options 1097
  - editing configuration options in the ralus.cfg file 1083
  - editing default options 1096
  - establishing trust relationship 1080
  - installing 1076
  - Novell OES, requirements for backup 1094
  - publishing to Backup Exec servers 1081
  - push-installing 1075
  - requirements 1074
  - restore options 1095
  - restoring 1095
  - runtime scripts 1102
  - saving the installatoin log 1076
  - starting the Linux agent daemon 1103

- Agent for Linux *(continued)*
  - stopping the Linux agent daemon 1103
  - troubleshooting 1104
  - uninstalling 1100
  - uninstalling manually 1100
  - using SSH 1075
- Agent for Mac
  - about the ralus.cfg file 1116
  - default options 1126
  - editing default options 1125
  - installing 1110
  - manually starting 1122
  - manually stopping 1123
  - requirements 1108
  - restore options 1128
  - restoring 1128
  - supported backup methods 1125
  - troubleshooting 1128
  - uninstalling 1113
- Agent for Microsoft Active Directory
  - about 987
  - about restoring individual objects 991
  - Granular Recovery Technology (GRT)
    - overview 988
  - passwords 991
  - recreating purged objects 992
  - requirements 985–986
  - tombstones 991
- Agent for Microsoft Hyper-V
  - backup options 802
  - backup selections 800
  - enabling Granular Recovery Technology (GRT) 802
  - highly available virtual machines 805
  - installation overview 800
  - overview 797
  - requirements 798
  - restoring 805
- Agent for Microsoft SharePoint
  - about 866
  - adding a farm 870
  - backing up SharePoint data 871
  - backup options 872
  - deleting a farm 871
  - disabling or enabling communication between
    - Web servers and Backup Exec 876
  - installing 866
  - overview 866
  - recovering SharePoint 2007 after a disaster 881
- Agent for Microsoft SharePoint *(continued)*
  - recovering SharePoint 2010 after a disaster 877
  - requirements 867
  - restore options 874
  - restoring SharePoint data 872
  - system requirements 867
  - using with SharePoint Portal Server 2003 and
    - Windows SharePoint Services 2.0 869
  - using with SharePoint Server 2007 and Windows
    - SharePoint Services 3.0 869
  - using with SharePoint Server 2010 and Windows
    - SharePoint Foundation 2010 868
- Agent for VMware
  - adding VMware vCenter and ESX servers 783
  - backing up Microsoft application data 788
  - backup defaults 784
  - backup methods 783
  - backup options 785
  - components 782
  - delete existing virtual machines 794
  - dynamic inclusion 788
  - Granular Recovery Technology
    - about 788
  - Granular Recovery Technology (GRT)
    - requirements 782
  - installing 783
  - log truncation for VSS Provider 791
  - overview 781
  - redirection options 794
  - requirements 782
  - requirements for backing up Microsoft
    - application data 789
  - restore options 792
  - restoring resources 791
  - selecting storage location for redirected
    - restore 794
  - selecting transport method for VMDK file 787
  - transport mode priority 793
  - turn on virtual machine after restore 794
  - VSS Provider 790
- Agent for Windows
  - about establishing trust 734
  - about installing to remote computers 83
  - Backup Exec Agent Utility 735
  - establishing trust 735
  - hardware requirements 732
  - installing 83
  - installing in an Active Directory network 90
  - installing on a Microsoft cluster 678

- Agent for Windows *(continued)*
  - installing updates 89
  - installing using a command script 98
  - installing using the command prompt 94
  - licenses 732
  - publish to Backup Exec servers 738
  - push-installing to remote computers 86
  - stopping and starting 733
  - uninstalling using a command script 99
  - uninstalling using command prompt 97
- agents
  - Backup Exec
    - trial version 114
    - upgrading 124
- Alert History by Backup Exec server report 595
- Alert History report 595
- alerts
  - about notification 288
  - alert category options 287
  - categories 279
  - clearing informational alerts 286
  - configuring categories 286
  - configuring groups for notification 295
  - configuring individual recipient 293
  - defined 279
  - deleting recipients 298
  - email notification 290
  - filters 284
  - recipient management 292
  - responding to 285
  - response options 285
  - sending job complete notification 299
  - setting up notification 289
  - severity 279
  - showing on the Home tab 281
  - stopping notification for recipient 298
  - text message notification 291
  - viewing job log 284
- allocated media
  - overwriting 377
- Alternate location
  - setting an SDR 709
- Any virtual disk storage device pool
  - description 1171
- append period
  - defined 369, 375
  - setting for media set 375
- archive bit
  - using to determine backed up status 532
- Archive Job Success Rate 625
- Archive logging
  - Lotus Domino 972
  - Lotus Domino recovery 979
- Archive Selections by Archive Rules and Retention
  - Categories report 625
- archive settings
  - overview 1247
- archives
  - deleting 1241
  - deleting items with expired retention
    - periods 1241
  - editing properties 1240
  - overview 1240
- Archiving Option
  - archives, overview 1240
  - arranging mailbox groups for provisioning 1244
  - assigning a vault store 1229
  - audit log entries 1242
  - backing up components 1262
  - backing up from remote Backup Exec
    - server 1261
  - best practices 1224
  - configuring archiving rules for file system
    - selections 1253
  - data not archived 1223
  - deleting a vault store 1237
  - deleting archives 1241
  - deleting data after archiving 1247
  - deleting items from archives 1260
  - deleting items with expired retention
    - periods 1231, 1241, 1262
  - Disabled job status 1221
  - disabling backup mode 1265
  - editing archive properties 1240
  - editing default retention category 1231
  - editing retention categories 1251
  - editing vault store partition properties 1239
  - editing vault store properties 1236
  - enabling single instance storage 1231
  - granting permissions on Exchange Server 1205
  - installing 1217
  - installing Enterprise Vault 1221
  - item deletion mode 1236
  - items not supported 1199
  - managing mailbox groups 1231, 1243
  - overview 1198, 1222
  - overview of archive settings 1247
  - overview of components 1262

**Archiving Option** (*continued*)

- overview of mailbox groups 1242
- overview of retention categories 1250
- redirecting restores for Directory database 1268
- redirecting restores of all components 1266
- redirecting restores with Backup Exec Utility 1266, 1268
- reinstalling 1220
- reports 1272
- requirements 1199
- restoring from remote Backup Exec server 1261
- restoring items from archives 1259
- running Backup Exec Utility 1270
- running consistency checks on databases 1265
- running Enterprise Vault services 1221
- searching archives for data 1260
- selecting administrative shares 1227
- selecting file system shares and folders 1227
- setting defaults 1231
- setting rules for archiving mailbox groups 1245
- specifying archive settings 1248
- specifying retention period 1252
- synchronizing permissions and settings 1231, 1234
- troubleshooting 1271
- uninstalling 1220
- updating SQL Server name 1266
- vault store partitions, overview 1238
- vault stores, overview 1235
- viewing the Enterprise Vault event log 1272
- viewing vault store partition status 1239
- viewing vault store status 1236

**ARCserve media**

- about restoring data from 240

**audit log**

- about 516
- Archive Option entries 1242
- configuring 516
- for media operations 380
- options 518
- removing entries 517
- saving to a file 518
- viewing 517

**Audit Log report** 596**Automated System Recovery** 637**automatic exclusion of SQL data during volume level backups** 823**automatic updates**

- about scheduling 117

**automatic updates** (*continued*)

- scheduling 117

**B****back up and delete the files method**

- freeing disk space 535

**Backup**

- using the Remote Media Agent for Linux 1149

**backup**

- overview 155

**backup definition**

- creating 163
- creating from an existing backup definition 165
- defined 155
- editing 170
- menu options 171
- one-time 164
- selecting data 177

**Backup Exec****overview**

- how it works 44

**Backup Exec Agent Utility**

- activity status
  - viewing 737
- command line applet 746
  - switches 747
  - using 747

**database access**

- configuring 742
- options 743

**default publishing interval** 740**Event Viewer**

- open 735

**job template name for DBA-initiated jobs** 894**Linux**

- configure Oracle instance on 896

**port**

- configure for Oracle operations 897

**publish to Backup Exec servers** 738, 740**publishing**

- adding Backup Exec servers 739
- editing Backup Exec server information 741
- publishing options 740
- removing Backup Exec servers 742

**Real Application Cluster (RAC)**

- publish to Backup Exec server 893

**refresh interval** 737

- setting 738

Backup Exec Agent Utility *(continued)*

- Registry Editor
    - open 735
  - security
    - options 745
    - removing certificate 745
  - Services
    - open 735
  - start the utility at log on 737
  - starting 736
  - starting automatically 737
  - status options 736
  - update credentials for Linux instances 894
  - view status 736
  - Windows
    - configure Oracle instance on 892
- Backup Exec Archiving Site
- backing up 1262
- Backup Exec diagnostic application
- diagnostic file
    - generating 666
    - generating using command line 667
  - options 666
  - overview 665
- Backup Exec License Assessment Tool 120
- Backup Exec Migrator
- about 940
  - about retrieving Enterprise Vault data 957
  - about staged migrations 945
  - about the Backup Exec Backup Sets view 956
  - Backup Exec server
    - working with 951
  - best practices 960
  - communicating with Enterprise Vault 953
  - configuring 948
  - data migration process 945
  - Enterprise Vault retention periods 947
  - events
    - about 946
  - how it works 941
  - log file location 947
  - logs
    - about 946
  - migrated files
    - about deleting 947
  - Migrator for Enterprise Vault options 952
  - requirements 941
  - retrieving Enterprise Vault data 957
  - troubleshooting 961

## Backup Exec server 44

- viewing properties 524
- Backup Exec services
- about the Backup Exec Services Manager 511
  - Backup Exec Services Manager options 512
  - changing service account information 513
  - changing startup options 514
  - service account 512
  - service account information options 515
  - stopping and starting 511
- Backup Exec settings
- about 463
  - changing preferences 465
  - database maintenance 466
  - DBA-initiated jobs 483
  - discover data to back up 469
  - Granular Recovery Technology (GRT)
    - options 482
  - network and security 470
  - preferences 465
- Backup Exec Utility
- redirecting restores for Archiving Option
    - Directory database 1268
  - redirecting restores of Archiving Option 1266
  - running for Archiving Option 1270
- backup job
- creating 163
  - creating from an existing backup definition 165
  - deduplication 774
  - editing 170
  - Exchange Agent options 854
  - excluding selections globally 462
  - one-time 164
  - pre/post commands 542
  - preparing for 154
  - required user rights 157
  - running the next scheduled instance 169
  - selecting data 177
- backup job settings
- about 185
  - Advanced Open File options 199
  - exclude files and folders options 210
  - exclusions options 209
  - files and folders options 204
  - network options 195
  - pre/post commands options 202
  - schedule options 188
  - security options 201
  - storage options 190

- backup job settings *(continued)*
    - test run options 196
    - verify options 197
    - verify schedule options 198
  - Backup Job Success Rate report 597
  - backup methods
    - about 528
    - advantages and disadvantages 530
    - delete selected files and folders after successful backup 528, 535
    - differential 529
    - duplicate 528
    - full 528
    - incremental 530
    - VMware data 783
  - backup network
    - overview 548
  - Backup Recommendations report 597
  - Backup Resource Success Rate report 598
  - backup selections 177
    - using fully qualified domain names 536
  - backup sets
    - about 212
    - about duplicating 218
    - about keeping 213
    - about verifying 222
    - cataloging 217
    - deleting 214
    - duplicate job options 221
    - duplicating 219
    - releasing from retention 216
    - retaining 215
    - retention options 215
    - verify job options 224
    - verifying 223
    - viewing contents 217
    - viewing properties 218
  - Backup Sets by Media Set report 598
  - Backup Size By Resource report 599
  - backup strategies
    - about 526
    - amount of data to be backed up 527
    - choosing data to back up 528
    - frequency of backups 526
    - how to choose 526
    - increase throughput with Agent for Windows 732
    - length of data retention 527
    - protecting against viruses 527
  - backup-to-disk folder
    - as read only legacy storage 327
    - changing the location of 330
    - importing 328
    - properties 329
    - recovering with Simplified Disaster Recovery 327
    - recreating 331
  - barcode labels
    - default 382
    - overview 382
    - robotic library support 382
  - baseline
    - setting for synthetic backup 1048
  - beoper group
    - Agent for Linux, about 1078
    - creating 1079
  - blink feature
    - about 1194
    - how to identify the physical disks 1195
  - block size
    - for tape drive 338
  - Boot managers
    - restoring in SDR 718
  - buffer count
    - setting for tape drives 341
  - buffer size
    - setting for disk cartridge devices 320
    - setting for tape drives 340
  - byte count
    - incorrect 656
- ## C
- calendar
    - excluding dates 226
    - options 227
    - viewing scheduled backup jobs 226
  - CASO
    - about upgrading 1011
    - alerts 1026
    - alias for managed Backup Exec server 1010
    - alias for SQL Express 1009
    - Backup Exec server
      - changing to a managed Backup Exec server 1014
    - Backup Exec server pool
      - adding managed Backup Exec servers 1031
      - creating 1031
      - deleting 1032

CASO *(continued)*

- Backup Exec server pool *(continued)*
  - overview 1029
  - removing a managed Backup Exec server 1032
  - selecting for backup 1030
- Backup Exec Utility
  - running 1044
- catalog locations 1016
- central administration server
  - setting for a managed Backup Exec server 1014
- centralized restore
  - multiple storage devices 1033
  - overview 1033
- changing to a central administration server 1013
- changing to a static port 1008
- communication thresholds 1025
- copying alert configurations to managed Backup Exec servers 1027
- creating an alias 1009–1010
- disabling communications 1026
- disaster recovery 1043
- enabling communications 1025
- installing 1001
- installing across a firewall 1007
- installing managed Backup Exec server 1002
- job delegation 1028
- managed Backup Exec server
  - changing to standalone server 1015
  - configuration options 1006
  - settings 1018
  - viewing properties 1039
- network interface cards
  - using any available 1028
- network traffic
  - reducing 1015
- notifications 1026
- overview 996
- pausing managed Backup Exec server 1037
- port numbers for SQL instance 1010
- recovering failed jobs 1035
- requirements 998
- restoring 1035
- restoring data from multiple devices 1034
- resuming a paused server 1038
- settings for managed Backup Exec servers 1018
- starting Backup Exec services 1039

CASO *(continued)*

- status 1025
- stopping Backup Exec services 1038
- storage and media data 999
- troubleshooting 1044
- uninstalling Backup Exec from central administration server 1045
- uninstalling Backup Exec from managed Backup Exec server 1046
- upgrading central administration server 1012
- upgrading managed Backup Exec server 1013
- catalog
  - defined 242
  - editing global options 242
  - global options 243
  - levels 242
  - media with encrypted backup sets 391
- catalog operation errors
  - DLT tape drive hangs 653
- cataloging
  - media 424
- centralized catalogs in CASO 1016
- centralized restore
  - best practices 1035
- CHECKCATALOG utility 814
- CHECKDB utility 814
- checkpoint restart
  - about 538
- checkpoint restart on Microsoft cluster failover
  - enabling or disabling 683
  - overview 681
- Circular logging
  - Lotus Domino 973
  - recovery of Lotus Domino server 982
- circular logging
  - Exchange Agent
    - reviewing in 848
- cleaning a drive 429
- cleaning slots
  - defining for robotic libraries 351, 358
- client-side deduplication
  - overview 773
- cluster failover error-handling rule 276
- clusters
  - disaster recovery 694
    - entire cluster manually 697
    - nodes using SDR 696
    - using SDR to prepare 696

- clusters *(continued)*
    - Microsoft 684
      - adding or removing a failover node 683
      - all drives pool 680
      - BEUtility 684
      - changing the order in which nodes fail over 683
      - configurations 686–689, 691
      - disaster recovery 699–700
      - disaster recovery of Backup Exec on a cluster using SDR 697
      - failover restart 676
      - installation 677, 679
      - overview 693
      - uninstalling Backup Exec 680
    - troubleshooting 701
    - using with Backup Exec 674
  - command line
    - installing Backup Exec 104
    - installing Remote Administrator 100
    - switches for installation 105
  - command prompt
    - uninstalling Agent for Windows 97
  - common encryption keys 553
  - compression
    - enable for tape drive 338
  - configuration settings
    - copying to another server 519–520
  - Configure Storage Wizard
    - about 145
    - changing or adding hot spares 1192
    - configuring a storage array 1162–1163
    - description 1162
  - configuring
    - holidays 458–461
  - consistency check options
    - Exchange Agent 855
    - SQL Agent 813
  - continuing Exchange backup if consistency check fails 855
  - control connection with the Remote Media Agent for Linux 1133
  - conversion to virtual machines
    - about editing a job 451
    - adding a stage for 444
    - after a backup job 441
    - default settings 452
    - disk configuration details 450
    - from point in time 444
  - conversion to virtual machines *(continued)*
    - Hyper-V conversion options 446
      - overview 437
      - requirements 439
      - schedule options 442
      - setting default options 451
      - simultaneously with backup job 440
      - VMware conversion options 446
    - copy settings
      - options 520
    - credentials
      - about testing or editing 175
      - properties 176
      - test/edit options 175
      - viewing or editing 176
    - custom installation
      - about 67
      - installing 70
    - Custom reports
      - filter criteria and expressions 570
- ## D
- Daily Device Utilization report 600
  - damaged media
    - removing 388
  - DAOS
    - .nlo files 966
    - about the Lotus Domino Agent and DAOS 966
    - DAOS-enabled databases 966
  - data connection to remote computers 1133
  - data discovery
    - used with Exchange Agent 836
  - Data Migration report 127
  - database maintenance
    - about 466
    - changing 467
    - options 467
  - database server
    - in Microsoft clusters 684
  - Database snapshots
    - SQL 822
  - DBA-initiated jobs
    - about configuring 483
    - creating a template 485
    - deleting a template 485
    - duplicate job settings 494
    - editing 485
    - general options 493
    - network options 493

- DBA-initiated jobs *(continued)*
  - settings 484
  - storage options 486
- Debug Monitor 670
- Deduplication Device Summary report 602
- deduplication disk storage
  - changing logon account password 769
  - overview 760
- deduplication disk storage devices
  - about disaster recovery 778
  - editing properties 761
  - preparing for disaster recovery 779
  - requirements 755
- Deduplication Option
  - about backing up 774
  - about copying deduplicated data to tapes 778
  - about restoring 778
  - changing logon account password for deduplication disk storage 769
  - client-side deduplication overview 773
  - copying data between OpenStorage devices or deduplication disk storage devices 775
  - deduplication disk storage overview 760
  - deduplication disk storage properties 761
  - deduplication methods for agents 754
  - direct access
    - editing properties 772
    - overview 771
    - selecting storage devices 771
  - disaster recovery of deduplication disk storage 778
  - disaster recovery of OpenStorage devices 780
  - installing 757
  - OpenStorage device overview 757
  - OpenStorage device properties 758
  - overview 752
  - preparing for disaster recovery 779
  - requirements 755
  - setting up optimized duplication 776
  - sharing devices 770
  - with encryption 778
- Deduplication Summary report 603
- Default options
  - Simplified Disaster Recovery settings 712
- default options
  - Advanced Open File 199
  - Agent for VMware 784
  - backup jobs 185
  - default options *(continued)*
    - configuring 455
    - conversion to virtual machines 451
    - Exchange Agent 854
    - exclusions 209
    - files and folders 204
    - NDMP 1071
    - network 195
    - pre/post commands 202
    - schedule 188
    - security 201
    - SQL Agent 817
    - storage 190
    - test run 196
    - verify 197
  - default preferred configuration settings for tape drives 341
  - deleting
    - media 389
  - destination Backup Exec server
    - add server options 522
    - adding 521
    - importing a list 521
  - Device Summary report 601
  - devices
    - adding iSCSI-attached 335
    - OpenStorage overview 757
    - reconnecting USB tape devices 335
  - diagnostic file
    - command line switches 668
    - remote Backup Exec server 669
  - differential backups
    - about 529
    - advantages and disadvantages 531
  - direct access
    - editing properties 772
    - overview 771
    - selecting storage devices 771
  - DirectCopy to tape
    - copying data 225
    - overview 225
  - directories
    - about including and excluding for NDMP 1066
  - Directory database
    - backing up for Archiving Option 1262
  - disabled job status 1221
  - disabling backup mode in Archiving Option 1265
  - disaster preparation
    - Disaster Preparation Plan (DPP) 634

- disaster preparation (*continued*)
    - Exchange Server 862
    - hardware protection 634
    - off-site storage 635
    - overview 634
  - Disaster recovery
    - alternate path in SDR 713
    - Lotus Domino Agent 977–978
    - setting path locations
      - disaster recovery information file 711
  - disaster recovery
    - clusters
      - Backup Exec on a Microsoft cluster using SDR 697
      - entire cluster manually 697
      - nodes using SDR 696
      - overview 694
      - using SDR to prepare 696
    - data protected by Backup Exec agents 637
    - deduplication disk storage 779
    - different types of computers
      - overview 637
    - Exchange Server 862
    - local Windows 2000 computers
      - (non-authoritative) 638
    - manual recovery of Windows system 637
    - Microsoft clusters
      - Backup Exec 700
      - data files 699
      - shared disks 699
    - Microsoft SharePoint 2007 881
    - Microsoft SharePoint 2010 877
    - OpenStorage devices 780
    - overview 637
    - remote Windows 2000 computers
      - (non-authoritative) 643–644
  - discover data to back up
    - about 537
    - configuring 469
    - options 470
  - disk cartridge storage
    - about 317
    - properties 317
  - disk space management settings 310
  - disk storage
    - about 307
    - editing properties 309
    - limit Backup Exec to read-only operations 310
    - low disk space thresholds 310
  - disk storage (*continued*)
    - properties 310
    - reserve disk space 310
  - Disk Storage Summary report 603
  - disk-based storage
    - about 305
  - distributed catalogs in CASO 1016
  - DLT tape
    - drive hangs when cataloging 653
  - drive pools
    - creating in a Microsoft cluster 680
  - duplication between OpenStorage devices or deduplication disk storage devices 775
  - dynamic inclusion
    - for Hyper-V 804
- ## E
- editions of Backup Exec
    - listed and described 43
  - eject media 428
    - after job completes 193
  - email notification
    - configuring 290
  - encrypted files
    - about cataloging media 391
  - encrypted SQL database restore 826
  - encryption
    - about 551
    - hardware 552
    - restoring encrypted SQL databases 826
    - software 551
    - types 551
    - with deduplication 778
  - encryption keys
    - 128-bit AES 551
    - 256-bit AES 551
    - about deleting 481
    - common 553
    - creating 478
    - deleting 481
    - encryption types 551
    - managing 477
    - options 478–479
    - overview 552
    - pass phrases 553
    - replacing 480
    - restoring encrypted data 233
    - restricted 553

- Enterprise Vault
  - running services for 1221
  - viewing event log 1272
- Enterprise Vault Agent
  - about redirecting a restore job 936
  - about restoring 929
  - About restoring individual files and folders 935
  - automatic redirection of Enterprise Vault
    - components 935
  - available backup methods 924
  - Backup Exec Migrator
    - about 940
    - about deleting migrated files 947
    - about events 946
    - about logs 946
    - about retrieving Enterprise Vault data 957
    - about staged migrations 945
    - about the Backup Exec Backup Sets
      - view 956
    - best practices 960
    - communicating with Enterprise Vault 953
    - configuring 948
    - data migration process 945
    - Enterprise Vault retention periods 947
    - how it works 941
    - log file location 947
    - Migrator for Enterprise Vault options 952
    - requirements 941
    - retrieving Enterprise Vault data 957
    - troubleshooting 961
    - VxBSA logs 946
    - working with a Backup Exec server 951
  - Backup Exec server
    - log file location 947
    - logs 946
  - best practices 940
  - collections
    - configuring 949
    - vault store partition properties 950
  - installing 922
  - migration
    - vault store partition properties 955
  - non-operational state 929
  - Partition Recovery Utility
    - about 958
    - finding an archive ID 959
    - log file location 947
    - logs 946
    - requirements 958
- Enterprise Vault Agent (*continued*)
  - Partition Recovery Utility (*continued*)
    - running 959
    - troubleshooting 961
  - ready-to-use state 929
  - redirection options 937
  - requirements 922
  - restore options 931
  - selecting a backup method 923
- Environment Check
  - overview 61
  - running before installation 62
- error codes
  - Unique Message Identifier
    - viewing 266, 286
- error-handling rules
  - cluster failover rule 276
  - creating 270
  - custom rules
    - defined 270
  - custom rules for recovered jobs 275
  - default rules
    - defined 270
  - deleting a custom rule 274
  - enabling for a failed job 274
  - enabling or disabling 274
  - overview 270
  - recovered jobs custom rule 270
  - settings 271
- Error-Handling Rules report 604
- ESX server, adding 783
- Event Recipients report 605
- Exchange Agent
  - Active Directory
    - backing up 847
  - automatic exclusion of files during volume level
    - backups 848
  - backing up
    - Exchange 2003/2007 852
    - recommended selections 847
  - backup job options 854
  - best practices 844
  - circular logging
    - reviewing 848
  - data discovery feature
    - using with 836
  - databases
    - configuring 858
  - disaster recovery 862

Exchange Agent (*continued*)

- Exchange 2003 with VSS
    - backing up 850
  - Exchange 2007 snapshot backup method 851
  - Exchange high availability server option 856
  - Exchange Web Services
    - overview 849
  - excluding files during volume level backups 848
  - Granular Recovery Technology (GRT)
    - overview 849
    - requirements for 836
    - setting for backup 854
  - installation 838
  - Internet Information Service (IIS) metabase
    - backing up 847
  - mailbox access requirements 845
  - offhost backup
    - with Granular Recovery Technology (GRT) 849
  - overview 834
  - protecting Exchange using VSS 850
  - redirecting data 860
  - requirements 834
  - restore of individual items
    - requirements for 836
  - restore requirements 857
  - restoring data from snapshot backups 860
  - restoring data to server 857
  - restoring Exchange 2003 and 2007 with Recovery Storage Group 858
  - services accounts
    - overview 835
  - setting backup job default options 854
  - snapshot backup
    - configuring 851
  - snapshot technology 850
  - storage groups
    - backing up 852
  - strategies for backing up 846
  - system state
    - backing up 847
  - troubleshooting snapshot and offhost jobs 852
  - volume level backups
    - automatic exclusion of files 848
- Exchange Mailbox Archiving Option
  - overview 1198
- Exchange Mailbox Group Archive Settings report 626
- Exchange Web Services
  - using with the Exchange Agent 849

## exclude dates

- deleting dates 460
  - exporting dates to another server 460
  - importing a list of dates 459
  - options 461
  - selecting dates 459
- exclude selections options 462
- executing a command
  - after backup 203
  - before backup 202
- exporting expired media 431
- exporting media 432

**F**

## failback

- defined 676

## Failed Archive Jobs report 627

## Failed Backup Jobs report 606

## failover

- adding or removing a failover node 683
- changing the order in which nodes fail over 683
- defined 674
- restart 676

## FAT

- partition 656

## father/son media rotation strategy 399

## file history

- enabling for NDMP 1071

## File System Archive Settings report 628

## File System Archiving Option

- overview 1198

## files

- about including and excluding for NDMP 1066

## Filter expressions for reports 570

## filters

- for alerts 284

## fingerprint database

- backing up for Archiving Option 1262
- for vault stores 1235

## firewall

- browsing systems through 474
- enabling a SQL instance behind 474
- using Backup Exec with 472

## formatting media 427

## full backups

- about 528
- advantages and disadvantages 531

**G**

- grandfather media rotation strategy 400
- Granular Recovery Technology (GRT)
  - about restoring individual items 543
  - Agent for Microsoft Servers 804
  - enabling for Microsoft Hyper-V 802
  - Exchange data 849
    - offhost backup 849
  - job settings 482
  - recommended devices for 545
  - requirements 547
  - setting default options 482
  - using Exchange Web Services 849
- Group Policy Object, configuring 93
- groups
  - configuring to receive notifications 295

**H**

- hardware
  - creating profile 636
  - enable hardware compression option 338
  - protection in case of disaster 634
  - troubleshooting 650
- hardware compression
  - enabling 343
- high water count
  - setting for tape drives 341
- highly available virtual machines
  - about backing up and restoring 805
- Home tab
  - about 136
  - configuring 140
  - Layout items 137
  - restoring the default configuration 140
  - Support items 139
  - System Health items 137
- hot key
  - defined 1290
- hot spare
  - best practices 1191
  - changing or adding 1192
  - description 1191
  - specifying 1162-1163

**I**

- IBM computers
  - recovering with Simplified Disaster Recovery 719

- imported media
  - labeled by Backup Exec 382
  - overwriting 377
- importing media 430
- include/exclude
  - files for backup jobs 180
  - options 181
- incremental backups
  - about 530
  - advantages and disadvantages 532
- index locations
  - backing up for Archiving Option 1262
- initializing a robotic library 426
- installation
  - about typical and custom 67
  - additional options 75
  - Agent for Windows 83
  - Agent for Windows from command prompt 94
  - Agent for Windows in Active Directory
    - network 90
  - Agent for Windows with command script 98
  - checklist 60
  - command line switches 105
  - configuring Group Policy Object 93
  - creating a software distribution point 93
  - creating a transform 92
  - custom 70
  - Environment Check
    - overview 61
    - running pre-install 62
  - from command line 104
  - Media Agent for Linux 1135
  - Microsoft SQL Server 2005 Desktop Engine (MSDE 2005) 63
  - Migration report 127
  - NDMP Option 1063
  - overview 58
  - parameter files
    - creating 112
    - using 113
  - post-installation tasks 127
  - pre-upgrade checklist 126
  - push-installing Agent for Windows 83, 86
  - push-installing to remote computers 77
  - Remote Administrator 99
  - Remote Administrator from command line 100
  - special considerations for remote computers 76
  - standard features 64
  - system requirements 65

installation *(continued)*

- trial version 114
  - typical 68
  - uninstalling Agent for Windows using command prompt 97
  - uninstalling Agent for Windows with command script 99
  - uninstalling Backup Exec 128
  - uninstalling options from local Backup Exec server 129
  - updates to Agent for Windows 89
  - Windows Management Instrumentation performance counter 303
  - Windows Management Instrumentation SNMP provider 304
- installation log 114
- Agent for Linux 1076
- installation overview 800
- installation parameter file
- creating 113
  - using 113
- installed updates
- viewing 119
- installing
- additional Backup Exec options on a Microsoft cluster 679
  - Backup Exec in a Microsoft cluster 677
  - SharePoint Agent 866
  - to an existing Microsoft SQL Server 2005 instance 63
  - using Terminal Services 70
- Internet Information Services (IIS) metabase
- backing up 847
- inventory
- robotic libraries when Backup Exec services start 350
- IPv4 550
- IPv6 550
- iSCSI-attached devices
- adding 335

**J**

## job activity 248

## job defaults

- about 456
- backup jobs 456
- exclude dates 458
- exclude selections 462
- global schedule 457

job defaults *(continued)*

- global schedule options 458

## job history

- about duplicating 218
- about verifying 222
- deleting jobs 262
- duplicate job options 221
- duplicating 220
- overview 260
- running a job 263
- verify job options 224
- verifying 223
- viewing report 564

## job log 264

- configuring default options 268
- default options 268
- finding text 267
- linking to technical support web site 266
- options to find text 267
- properties for completed jobs 265
- status overview 263
- viewing from an alert 284
- with vertical applications 266

## job progress indicators

- displaying 466

## job queue

- holding 253
- removing the hold 254

## job status and recovery 277

## jobs

- canceling 252
- changing priority for scheduled 258
- completion status 263
- configuring error-handling rules 270
- deleting from Job History 262
- deleting scheduled 259
- holding 253
- holiday scheduling 458–461
- managing and monitoring 247
- placing job queue on hold 253
- removing a hold 253
- removing hold on the job queue 254
- running from Job History 263
- running scheduled job 258
- sending notification when complete 299
- setting status and recovery options 277
- status and recovery options 277
- status and recovery overview 276
- viewing the job log 264

Jobs Summary report 607

## K

keyboard navigation

- dialog boxes 1308
- standards 1308

keyboard shortcuts

- Backup and Restore tab 1291
- Backup and Restore tab for the Active Alerts view 1297
- Backup and Restore tab for the Backup Sets view 1296
- Backup and Restore tab for the Credentials view 1298
- Backup and Restore tab for the Job History view 1295
- Backup and Restore tab for the Jobs view 1294
- Home tab 1290
- Reports tab 1307
- Storage tab 1299
- Storage tab for the Active Alerts view 1306
- Storage tab for the Backup Sets view 1305
- Storage tab for the Job History view 1304
- Storage tab for the Jobs view 1302

## L

labeling media 428

- imported media label 382
- renaming 383
- using barcode labels 382

last known good menu 636

Library Expansion Option

- about 335
- SCSI addresses for hardware 349
- setting up hardware 349

license information

- finding in your environment 120
- viewing 120

licenses 58

- Agent for Windows 732
- finding in your environment 120

limit Backup Exec to read-only operations on disk-based storage 418

list boxes

- navigation 1309

list of servers

- about 157
- adding servers 158

list of servers *(continued)*

- removing servers 159
- server groups 159

LiveUpdate

- about 116
- about scheduling automatic updates 117
- running manually 119
- scheduling automatic updates 117

local Backup Exec server

- breaking connection with 102

local server properties

- about viewing 523
- viewing 524

logon accounts

- about 498
- changing default 505
- changing the password 503
- copy options 510
- copying to another server 505
- creating 500
- credentials options 508–509
- default
  - about 499
- deleting 504
- editing 502
- management options 506
- replacing 503
- restricted 500
- SQL databases 812
- system logon account 501

logon information

- copying to another server 505

Lotus Domino

- transaction logs
  - about 972

Lotus Domino Agent

- Active File Exclusion 971
- APIs 968
- archive logging 972
- automatic exclusion of files
  - volume level backups 971
- backup options 970
- circular logging 973
- DAOS NLO
  - restore redirection 977
- database backup overview 968
- database backup requirements 965
- disaster preparation 977

Lotus Domino Agent *(continued)*

- disaster recovery
  - archive logging 979
  - circular logging 982
  - of server 978

- Microsoft Cluster Server 965
  - restoring 975

- monitor change journal
  - disabling 980
  - re-enabling 981

overview 964

redirecting restore 977

requirements 964

restore options 975

selecting for restore 973

supported configurations 971

## Lotus Domino transaction logs

viewing 968

## low disk space thresholds 310

editing for a virtual disk 1173

**M**

## Mac Agent

manual install and uninstall 1114

## mailbox access requirements for Exchange 845

## mailbox groups

arranging for provisioning 1244

managing 1231, 1243

overview 1242

setting rules for archiving 1245

## maintenance contract information

about 121

managing customer numbers 124

viewing details 122

## majority node in a cluster 677

## managed Backup Exec server

about upgrading 1011

changing settings 1018

copying jobs to 1029

installing 1002

network interface card

using any available 1028

pools 1029

settings 1018

## Managed Backup Exec Servers report 608

## master database (SQL)

backup 813

## media

associating with a media set or vault 391

media *(continued)*

damaged 388

deleting 389

displaying media ID 392

erasing 389

overwrite options 378

overwriting allocated or imported 377

properties 392

retired

defined 367

scanning barcode labels 387

scratch

defined 367

with excessive errors 388

## Media Agent for Linux

beoper group 1135

installing 1135

## Media Audit report 609

## Media Errors report 610

## media ID

defined 381

## media label

barcodes 382

imported 382

overview 381

renaming 383

## media operations

associating media with media sets 391

audit log for 380

## media overwrite protection level

defined 377

## Media Required for Recovery report 610

## media rotation

strategies

father/son 399

grandfather 400

son 398

## media set

creating 373

default 373

defined 366

deleting 376

media vault rules 374

overwrite and append properties 374

renaming 376

vault rule properties 386

## Media Summary report 611

## Media Vault Contents report 612

## media vaults, about 384

- messages
  - error 654
- Microsoft Cluster Server
  - using with Backup Exec 675
- Microsoft SharePoint data
  - backing up 871
  - restoring 872
- Microsoft SQL Server 2005 Desktop Engine (MSDE)
  - installing 63
- Microsoft Terminal Services
  - and installing Backup Exec 70
- Microsoft Virtual Hard Disk files
  - about managing 542
- Migration report 127
- mnemonic
  - defined 1290
- modified time
  - using to determine backed up status 532
- Move Media to Vaultreport 613
- MSCS
  - using with Backup Exec 675
- MSDE
  - 2005 components
    - installed with Backup Exec 63

## N

- named transaction
  - restore up to
    - SQL 2000 826
- navigation
  - list boxes 1309
  - Tabbed pages 1309
- NDMP Option
  - adding an NDMP server 1063
  - backing up resources 1063
  - duplicate backed up data 1068
  - how to use patterns 1066
  - installing 1063
  - overview 1062
  - redirecting restored data 1071
  - requirements 1062
  - restoring data 1068
  - setting default options 1071
  - sharing devices on an NDMP server 1063
  - viewing properties 1071
- network
  - overview of backup networks 548
- network and security
  - options 471

- Network Attached Storage (NAS)
  - protecting 1062
- network traffic
  - reducing in CASO 1015
- nodes
  - configurations in a Microsoft cluster 686
  - defined 674
  - disaster recovery using SDR 696
  - Microsoft
    - adding or removing a failover node 683
    - changing the order in which nodes fail
      - over 683
- notification
  - about 288
  - configuring email 290
  - configuring group recipient 295
  - configuring individual recipient 293
  - configuring SNMP 300
  - configuring text messages 291
  - editing recipient properties 297
  - managing recipients 292
  - removing recipient from group 297
  - sending for completed jobs 299
  - setting up 289
  - stopping 298
- Novell OES
  - about restoring 1095
  - requirements for back up 1094
  - supported components 1093
- NTFS
  - partition 656

## O

- off-site storage of backups 635
- offhost backup
  - best practices 1054
  - host computer
    - defined 1052
  - overview 1052
  - single volume snap 1055
  - transportable snapshots
    - defined 1052
- open files
  - unable to back up 655
- OpenStorage devices
  - disaster recovery 780
  - editing properties 758
  - overview 757
  - properties 758

- OpenStorage devices *(continued)*
    - requirements 755
  - Operations Overview report 614
  - optimized duplication 775
    - setting up 776
  - Oracle Agent
    - authentication credentials 897
      - deleting 899
      - setting 898
    - authentication credentials options 899
    - authentication for Oracle operations 897
    - back up with 900
    - Backup Exec Agent Utility options 890
    - backup options 903
    - channel time-out
      - change default for 912
    - configuring 887
    - database time-out
      - change default 911
    - DBA-initiated backup 902
    - DBA-initiated job settings
      - create template for 483
    - DBA-initiated jobs
      - job template name for 894
    - DBA-initiated restore 906
    - default options 889
    - features 885
    - install 886
    - Linux servers
      - configuring an Oracle instance 893
      - deleting an Oracle instance 895
      - editing an Oracle instance 895
      - enabling database access 896
      - viewing an Oracle instance 894
    - multiple data streams
      - specify 904
    - Oracle Net Service name 890
    - port
      - configure for Oracle operations 897
    - publish Oracle databases on Linux 894
    - Real Application Cluster (RAC) 893, 901
    - recovery catalog 890, 894
    - redirected restore 906
    - restore 904
    - troubleshooting 911
    - update credentials for instances 889, 894, 900
    - Windows computers
      - configuring an Oracle instance 888
      - deleting an Oracle instance 892
  - Oracle Agent *(continued)*
    - Windows computers *(continued)*
      - editing an Oracle instance 891
      - enabling database access 892
      - viewing an Oracle instance 890
  - Overnight Archive Summary report 628
  - Overnight Summary report 616
  - overwrite protection
    - disabling 417
  - overwrite protection levels
    - full 416
    - partial 416
  - overwrite protection period
    - defined 370, 375
    - setting for media set 375
- P**
- parameter files
    - creating 112
    - using 113
  - partial overwrite protection 416
  - partition
    - creating for robotic library 355
    - FAT 656
    - NTFS 656
  - Partition Recovery Utility
    - about 958
    - finding an archive ID 959
    - log file location 947
    - logs
      - about 946
    - requirements 958
    - running 959
    - troubleshooting 961
  - pass phrases 553
  - password
    - changing for logon account 503
  - patterns in NDMP excludes 1066
  - performance
    - increase during backups of remote Windows computers 732
  - physical check
    - SQL 2000 819
  - physical disk
    - creating a physical disk group 1162–1163
    - viewing properties 1164
  - PHYSICAL\_ONLY utility 814
  - point in time
    - conversion to virtual machine 444

- point in time log restore option
  - SQL Agent 826
- Port number
  - changing for Remote Media Agent for Linux 1144
- ports used by Backup Exec
  - default 475
  - listening 476
- post-job command
  - for backup jobs 542
  - setting for backup job 203
- Post-Migration report 127
- pre-installation checklist 60
- pre-job command
  - for backup jobs 542
  - setting for backup job 202
- pre-upgrade checklist 126
- preferred server configurations
  - about 839
  - creating 840
  - deleting 840
  - designating a default 841
  - editing settings 840
  - removing as default 841
- priority
  - changing for scheduled job 258
- Problem Files report 617
- prompt before overwriting allocated or imported media 417
- Properties
  - report 588
- properties
  - active job 248
  - tape cartridge media 392
- Publish
  - Linux computers to Backup Exec servers 1081
- publish
  - default interval 740
  - disable on remote computer 740
  - to Backup Exec servers
    - using Agent for Windows 738

## R

- ralus.cfg
  - about, for the Agent for Linux 1081
  - about, for the Remote Media Agent for Linux computer 1140
  - configuration options 1083
  - editing configuration options in 1083
- ralus.cfg (*continued*)
  - for the Agent for Mac 1116
- Recently Written Media report 617
- recipients
  - about managing 292
  - configuring an individual 293
  - configuring groups 295
  - deleting 298
  - editing 297
  - removing from a group 297
  - stopping notification 298
- Recover This Computer Wizard
  - Advanced Disk Configuration
    - original disk layout geometry 727
    - simplified volume layout view 723
  - requirements 720
  - running 721
- recovered jobs
  - setting thresholds 277
- recovered jobs custom error-handling rule 270
- Recovery Storage Group 858
- redirected restore
  - Exchange data 860
- Remote Administrator
  - installing 99
  - installing using the command line 100
  - running 102
- remote computers
  - about installing options 83
  - push-installing 77
  - special considerations for installing 76
- Remote Media Agent for Linux
  - adding to Backup Exec database 1143
  - backing up data 1149
  - changing port number 1144
  - creating a simulated tape library 1150
  - deleting simulated tape library 1153
  - determining server status 1147
  - how it works 1133
  - ICMP ping 1144
  - managing simulated tape libraries from the command line 1154
  - requirements 1133
  - restoring data 1149
  - Simulated Tape Library options 1151
  - simulated tape library properties 1152
  - Tape Library Simulator Utility 1149
    - Command line switches 1154
  - troubleshooting 1155

Remote Media Agent for Linux *(continued)*

- uninstalling 1138
- viewing properties 1147
- viewing properties of simulated tape libraries 1151
- renaming
  - media labels 383
- repair option 115
- replicated catalogs in CASO 1016
- Reports
  - Alert History 595
  - Alert History by Backup Exec server 595
  - Application settings 587
  - Archive Job Success Rate 625
  - Archive Selections by Archive Rules and Retention Categories 625
  - Audit Log 596
  - available reports 589
  - Backup Job Success Rate 597
  - Backup Recommendations 597
  - Backup Resource Success Rate 598
  - Backup Sets by Media Set 598
  - Backup Size By Resource 599
  - custom
    - about grouping fields 577
    - copying 585
    - deleting 586
    - editing 586
    - filter criteria and expressions 570
    - filter expressions 571
    - graph options 582
    - grouping options 578
    - name and description options 568
    - overview 566
    - previewing 585
    - setting filters 574
    - setting graph options 581
    - sort options 580
    - sorting fields 579
  - Daily Device Utilization 600
  - Deduplication Device Summary 602
  - deleting custom reports 565
  - deleting scheduled reports 565
  - Device Summary 601
  - Disk Storage Summary report 603
  - editing application settings 586
  - Error-Handling Rules 604
  - Event Recipients 605
  - Exchange Mailbox Group Archive Settings 626

Reports *(continued)*

- Failed Archive Jobs 627
- Failed Backup Jobs 606
- field selection options 569
- File System Archive Settings 628
- Jobs Summary 607
- Managed Backup Exec Servers 608
- Media Audit 609
- Media Errors 610
- Media Required for Recovery 610
- Media Summary 611
- Media Vault Contents 612
- Move Media to Vault 613
- notification recipients
  - setting recipients 566
- Operations Overview 614
- Overnight Archive Summary 628
- Overnight Summary 616
- Problem Files 617
- properties 588
- Resource Protected Recently 619
- Resource Risk Assessment 618
- Restore Set Details by Resource 619
- Retrieve Media from Vault 620
- Robotic Library Inventory 621
- Scheduled Server Workload 622
- scheduling report jobs 566
- Scratch Media Availability 623
- Test Run Results 624
- Vault Store Usage Details 629
- Vault Store Usage Summary 630
- viewing properties 588
- reports
  - Deduplication Summary 603
  - overview 556
  - Recently Written Media 617
  - running 558
  - viewing 558
  - viewing in job history 564
- Reports reports
  - custom
    - creating 567
- Requirements
  - Lotus Domino Agent 964
- requirements
  - Agent for Microsoft Hyper-V 798
  - Backup Exec 65
  - Central Admin Server Option 998
  - Exchange Agent 834

- requirements (*continued*)
    - NDMP Option 1062
    - off-host backup 1053
    - Remote Media Agent for Linux 1133
    - synthetic backup 1049
    - user rights for backup jobs 157
  - Resource Protected Recently report 619
  - Resource Risk Assessment report 618
  - Restore
    - creating restore jobs for the Remote Media Agent for Linux 1149
    - Lotus Domino Agent
      - redirecting Lotus Domino 977
      - Lotus Domino databases 973
  - Restore Set Details by Resource report 619
  - Restore Wizard 229–230
  - restoring
    - about restoring data 229
    - about System State data 234
    - ARCserve tapes 240
    - canceling a restore job 241
    - encrypted data 233
    - Exchange data 857
    - global defaults 231
    - launching the Restore Wizard 229
    - media created with other backup software 239
    - online restore of a Windows computer 234
    - searching for data to restore 229
    - setting global defaults 231
    - Shadow Copy Components 236
    - SQL master database 827
    - System State to a domain controller 235
    - UEFI system partitions 237
    - utility partitions 237
  - restricted encryption keys
    - defined 553
  - restricted logon accounts
    - about 500
  - retensioning a tape 426
  - retention categories
    - default retention category 1231
    - editing 1251
    - overview 1250
    - specifying properties 1252
  - retired media
    - defined 367
    - moving damaged media 388
  - Retrieve Media from Vault report 620
  - robotic library
    - cleaning slot 351
    - configuring partitions 355
    - creating partitions 355
    - example configuration 350
    - initializing when Backup Exec services start 351
    - inventory when Backup Exec services start 350
    - setting up hardware 350
    - using with Backup Exec 349
  - Robotic Library Inventory report 621
  - runtime scripts, for Agent for Linux 1102
- ## S
- SAN
    - hardware errors 659
    - resetting the SAN 660
    - troubleshooting 656
    - troubleshooting offline storage devices 657
  - scan
    - detecting storage arrays 1193
  - schedule
    - deleting exclude dates 460
    - exclude dates 459
    - exclude dates from 458
    - exclude dates options 461
    - exporting exclude dates 460
    - importing a list of dates to exclude 459
  - scheduled jobs
    - about managing and monitoring 247
    - changing priority 258
    - deleting 259
    - editing a single job 251
    - editing multiple jobs 252
    - holding 253
    - removing a hold 253
    - running immediately 258
    - statuses 256
  - Scheduled Server Workload report 622
  - Scheduling report jobs 566
  - scratch media
    - creating 377
    - defined 367
  - Scratch Media Availability report 623
  - SCSI
    - pass-through mode for tape drives 342
    - setting address for robotic library drives 349
  - SCSI bus
    - configuring for tape devices in a Microsoft cluster 689

- Search 230
- Search Knowledge Base 131
- Search Wizard 229
- Section 508 of the Rehabilitation Act
  - compliance 1289
- server groups
  - about 159
  - backing up 168
  - creating 160
  - deleting 162
  - editing 161
  - options 161
  - viewing 160
- Server properties
  - Remote Media Agent for Linux 1147
- server properties
  - about viewing 523
  - viewing 524
- service account
  - about 512
  - changing 512–513
  - options 515
- services
  - about the Backup Exec Services Manager 511
  - Backup Exec Services Manager options 512
  - changing service account information 513
  - changing startup options 514
  - service account 512
  - service account information options 515
  - starting and stopping 511
- SGMon 670
- Shadow Copy Components
  - about restoring 236
  - file system 540
- Share Your Ideas, described 131
- SharePoint Agent
  - about 866
  - adding a farm 870
  - backing up SharePoint data 871
  - backup options 872
  - deleting a farm 871
  - disabling or enabling communication between
    - Web servers and Backup Exec 876
  - installing 866
  - overview 866
  - recovering SharePoint 2007 after a disaster 881
  - recovering SharePoint 2010 after a disaster 877
  - requirements 867
  - restore options 874
- SharePoint Agent (*continued*)
  - restoring SharePoint data 872
  - system requirements 867
  - using with SharePoint Portal Server 2003 and Windows SharePoint Services 2.0 869
  - using with SharePoint Server 2007 and Windows SharePoint Services 3.0 869
  - using with SharePoint Server 2010 and Windows SharePoint Foundation 2010 868
- SharePoint farms
  - adding 870
  - deleting 871
  - properties 876
  - viewing properties 876
- silent mode installation 104
- simple recovery model
  - SQL 2000 810
- Simplified Disaster Recovery
  - About the System Recovery Disk 705
  - Advanced Disk Configuration
    - about 724
  - automated restore
    - restoring from a remote Backup Exec server 722
  - best practices 729
  - boot managers 718
  - catalog entries
    - added to \*.dr file 708
  - clusters
    - recovering Backup Exec on a Microsoft Cluster 697
    - recovering nodes 696
  - Create Simplified Disaster Recovery Disk Wizard
    - about 714
    - running 715
  - Create Simplified Disaster Recovery Disk Wizard requirements 714
  - editing the default path 712
  - installing 707
  - Microsoft Exchange Server
    - recovering 728
  - Microsoft SQL Server
    - recovering 727
  - OS/2 boot manager
    - restoring 718
  - overview 704
  - Recover This Computer Wizard
    - about 720
    - automated restore 721

- Simplified Disaster Recovery *(continued)*
  - Recover This Computer Wizard *(continued)*
    - encrypted backup sets 720
    - restoring from a remote Backup Exec server 722
    - running 721
  - recovering IBM computers 719
  - recovery requirements in SDR 718
  - setting an alternate location 709
  - SharePoint Portal Server
    - recovering 728
  - System Commander boot manager
    - restoring 718
- Simulated tape library
  - creating 1150
  - delete 1153
  - viewing properties 1151
- single block mode
  - setting for tape drives 341
- snapshot technology
  - using with Exchange Agent 850
- SNMP
  - configuring notification 300
  - configuring system service for Windows 303
  - installing WMI provider 304
  - object identifier prefix 300
  - traps
    - defined 300
- software distribution point, creating 93
- son media rotation strategy 398
- Sort and Filter 134
- splash screen
  - show at startup 465
- SQL 2000
  - named transaction 826
  - simple recovery models 810
- SQL Agent
  - backing up
    - backup methods 822
    - consistency check after backup 819
    - consistency check recommendations 813
    - databases 815
    - strategies for 812
    - Windows registry 813
  - consistency check 814
    - recommendations 813
  - Database Consistency Check (DBCC)
    - recommendations 813
- SQL Agent *(continued)*
  - database snapshots
    - overview 824
  - default options 817
  - disaster recovery 831
    - how to prepare 830
    - manual 832
    - overview 830
    - requirements 831
  - features 810
  - installation 811
  - logon accounts 812
  - overview 810
  - requirements 811
  - restoring
    - master database 827
    - point in time log restore option 826
    - redirecting restores 830
    - TDE-encrypted database backups 826
    - very large databases 825
  - snapshot technology
    - using 814
  - strategy recommendations 813
  - transaction logs 823
  - truncate log on checkpoint option 823
- stages
  - about 183
  - editing 184
- stalled jobs
  - setting thresholds 277
- statistics
  - tape drive usage 345
- storage
  - about deleting 420
  - about sharing 418
  - about tape drives and robotic libraries 334
  - change to online 425
  - disabling 425
  - editing global settings 415
  - enabling 425
  - global settings 415
  - Hot-swappable Device Wizard 335
  - Library Expansion Option 335
  - pausing 425
  - renaming 421
  - sharing deduplication devices 770
  - Symantec Device Driver Installation Wizard 336
  - unpausing 425

- storage (*continued*)
    - Virtual Tape Library Unlimited Drive Option 334
  - storage and media data
    - location of in CASO 999
  - storage array
    - about identifying physical disks 1194
    - blink 1194
    - capacity 1165
    - configuring 1162–1163
    - configuring virtual disks 1173
    - detecting 1193
    - hardware health 1165
    - hardware status 1165
    - identifying the physical disks 1195
    - renaming 1193
    - status 1165
    - viewing components 1162
    - viewing properties 1164
  - Storage device pools
    - any virtual disk storage device pool 1171
  - storage device pools
    - about 403
    - creating 405
    - editing properties 406
    - properties 406
    - system-defined 403
  - storage devices
    - installing 60
  - storage operations
    - about inventory 422
    - cataloging 424
    - cleaning a drive 429
    - ejecting media 428
    - exporting expired media 431
    - exporting media 432
    - importing media 430
    - initializing a robotic library 426
    - inventorying 423
    - inventorying and cataloging 423
    - locking the front portal 433
    - overview 410
    - retensioning 426
    - scanning 424
    - simulated tape libraries 412
    - unlock front portal 433
    - virtual tape libraries 412
  - Storage Provisioning Option
    - configuring in CASO 1161
  - Storage Provisioning Option (*continued*)
    - description 1160
    - detecting storage arrays 1193
    - installing 1161
    - requirements 1161
    - upgrading 1161
  - storage trending 306
  - Symantec Device Driver Installation Wizard 336
  - Symantec Endpoint Protection
    - using with Backup Exec 550
  - Symantec Knowledge Base 662
    - searching 663
  - Symantec RSS Reader
    - customizing 141
    - options 142
    - overview 140
    - removing default RSS feed 142
    - viewing articles 141
  - synchronizing archiving permissions and settings 1234
  - synthetic backup
    - baseline 1048
    - encryption
      - requirements for 1049
  - system logon account
    - about 501
    - creating 505
  - System Recovery Disk
    - about the Simplified Disaster Recovery 705
  - system requirements
    - Backup Exec 65
  - System State
    - restoring 234
    - restoring to a domain controller 235
- T**
- Tabbed dialog boxes
    - navigation 1309
  - Tabs 133
  - tape cartridge media
    - properties 392
  - tape drives
    - buffer count 341
    - buffer size 340
    - default settings 341
    - high water count 341
    - properties 338
    - statistics 344
    - statistics on usage 345

- Tape Library Simulator Utility
    - creating a simulated tape library 1150
    - deleting library 1153
    - overview 1149
    - running from command line 1154
    - viewing properties 1151
  - tape/disk cartridge media
    - description 365
  - tapeinst.exe
    - Symantec Device Driver Installation Wizard 336
  - tapes
    - DLT tape drive 653
  - TCP/IP
    - required for Mac agent 1108
  - technical support
    - contacting 663
  - test run job
    - about 222
  - Test Run Results report 624
  - text message notification
    - configuring 291
  - ThreatCon levels 550
  - transaction logs
    - Lotus Domino DBIID 972
    - recycling
      - Lotus Domino 970
  - transform, creating 92
  - Transparent Database Encryption
    - SQL Agent 826
  - trial version
    - agents and options 114
  - Troubleshooting
    - Remote Media Agent for Linux 1155
  - troubleshooting
    - Backup Exec performance
      - improving 661
    - backup issues 655
    - clusters 701
    - error messages 654
    - hardware-related issues 650
  - true image restore
    - overview 1050
  - truncate log on checkpoint option
    - SQL Agent 823
  - trust
    - establishing 734
    - establishing for a remote computer 735
    - establishing for a remote Linux computer 1080
  - trust (*continued*)
    - establishing for a Remote Media Agent for Linux
      - computer 1140
  - typical installation
    - about 67
    - installing 68
- ## U
- unconfigured virtual disk
    - configuring 1173
    - hardware health 1174
    - hardware status 1174
    - viewing properties 1174
  - uninstallation
    - Backup Exec 128
    - Backup Exec options from local Backup Exec
      - server 129
    - using command line 129
  - uninstalling
    - Backup Exec from a Microsoft cluster 680
  - Unique Message Identifier (UMI) error code
    - viewing 266, 286
  - updates
    - about scheduling 117
    - installing to Agent for Windows 89
    - performing manually 119
    - scheduling 117
    - viewing what is installed 119
  - upgrades
    - checklist 126
    - overview 124
  - USB tape devices
    - reconnecting 335
  - utility partitions
    - restoring 237
- ## V
- vault
    - scan barcode labels to move media 387
  - vault rules for media sets 386
  - vault store
    - assigning 1229
    - changing item deletion mode 1236
    - deleting 1237
    - editing properties 1236
    - viewing status 1236
  - vault store group
    - backing up for Archiving Option 1262

- vault store partitions
    - backing up for Archiving Option 1262
    - editing properties 1239
    - open and closed 1238
    - overview 1238
    - viewing open and closed states 1239
  - Vault Store Usage Details report 629
  - Vault Store Usage Summary report 630
  - vault stores
    - backing up for Archiving Option 1262
    - fingerprint database 1235
    - overview 1235
  - VHD files
    - about managing 542
  - virtual disk
    - blink 1194
    - capacity 1180
    - concurrent jobs 1180
    - configuring 1173
    - creating 1162–1163
    - description 1171
    - editing default options 1173
    - editing general properties 1180
    - editing low disk space thresholds 1173
    - hardware health 1180
    - hardware status 1180
    - identifying the physical disks 1195
    - number of files 1180
    - renaming 1193
    - status 1180
    - unconfigured virtual disk 1174
  - Virtual Disk Service
    - installing for the Storage Provisioning Option 1161
  - virtual machine conversion
    - about editing a job 451
    - adding a stage for 444
    - after a backup job 441
    - default settings 452
    - disk configuration details 450
    - from point in time 444
    - Hyper-V 446
    - overview 437
    - requirements 439
    - schedule options 442
    - setting default options 451
    - simultaneous with backup job 440
    - VMware conversion options 446
  - virtual machines
    - automatic protection for Hyper-V 804
  - virtual tape library
    - DirectCopy to physical devices 225
  - Virtual Tape Library Unlimited Drive Option,
    - about 334
  - virus
    - effect on data storage requirements 527
  - VMware vCenter Server, adding 783
  - volume level backups
    - automatic exclusion of SQL data 823
  - VSS
    - perform consistency check before Exchange backup 855
    - using to protect Exchange data 850
  - VSS Provider
    - log truncation setting 791
    - protecting databases and applications 790
- ## W
- Windows Change Journal
    - using to determine backed up status 532
  - Windows Management Instrumentation (WMI)
    - adding WMI capability 303
  - Windows registry
    - backing up with SQL Agent 813
  - Windows Server 2003
    - backing up 540
    - disaster recovery 637
  - Windows Server 2008
    - backing up 540
    - Read Only Domain Controller 66
    - Server Core 66
  - Windows user rights 157
  - Windows XP
    - disaster recovery 637
  - WMI
    - installing performance counter provider 303
    - installing SNMP provider 304
    - uninstalling performance counter provider 304
    - uninstalling SNMP provider 304
  - WORM media, about 383