

# Veritas Backup Reporter 6.6 Guide



# Veritas Backup Reporter 6.6 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 6.6

## Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

Symantec, 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>

## Acknowledgments

examples: This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), namely Tomcat Servlet Container, Jakarta Commons, Sprint Framework, Active MQ, Ehcache, Xerces XML Parser, Piccolo XML Parser, Log4J and Apache XML-RPC. A copy of Apache Software License 1.1 and 2.0 can be found at [www.apache.org/licenses/](http://www.apache.org/licenses/). The Piccolo XML Parser library is copyright Yuval Oren.

# 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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Contacting Technical Support

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

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/techsupp/](http://www.symantec.com/techsupp/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

Customer Service is available to assist with 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 maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

## Maintenance agreement resources

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

Asia-Pacific and Japan	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

## Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

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

Select your country or language from the site index.

# Contents

Technical Support .....	4	
Chapter 1	Overview of Veritas Backup Reporter 6.6 .....	17
	About Veritas Backup Reporter .....	17
	About compliance reporting .....	18
	About business planning .....	19
	About reporting on archive data .....	20
	About what's new in Veritas Backup Reporter 6.6 .....	20
	About Veritas Backup Reporter components .....	22
	About the Veritas Backup Reporter Management Server .....	22
	About the Veritas Backup Reporter Agent .....	26
	About the Veritas Backup Reporter Java View Builder .....	30
	About Veritas Backup Reporter documentation .....	31
Chapter 2	Installing Veritas Backup Reporter .....	35
	Planning your Veritas Backup Reporter installation .....	35
	Prerequisites .....	35
	About operating system requirements .....	36
	About Windows updates .....	39
	Installing Solaris updates .....	39
	About supported upgrade paths .....	40
	About products and their versions supported by Veritas Backup Reporter .....	187
	About Veritas Backup Reporter Agent deployment .....	42
	About configuring Veritas Backup Reporter firewall .....	46
	About AT configuration in Veritas Backup Reporter .....	54
	Verifying the authentication mode for Symantec Product Authentication Service .....	57
	Installing Veritas Backup Reporter on Solaris and Windows .....	59
	Installing Veritas Backup Reporter on Solaris .....	60
	Installing Veritas Backup Reporter on Windows .....	65
	Resolving agent authentication failures manually on Solaris and Windows .....	110
	Verifying that Veritas Backup Reporter is running properly .....	111

Uninstalling Veritas Backup Reporter on Solaris and Windows .....	74
Upgrading Veritas Backup Reporter .....	76
About database upgrade in VBR 6.6 .....	76
Upgrade prerequisite .....	79
Upgrading to Veritas Backup Reporter 6.6 on Solaris .....	79
Upgrading Veritas Backup Reporter on Windows .....	81
Identifying the version of .jar files .....	84
Modifying Veritas Backup Reporter on Solaris .....	85
Modifying Veritas Backup Reporter on Windows .....	85
Clustering Veritas Backup Reporter .....	86
About a Veritas Backup Reporter cluster .....	87
Clustering Veritas Backup Reporter on Windows .....	88
Clustering Veritas Backup Reporter on Solaris .....	100
Removing VBR completely from the cluster .....	106
Known issues .....	107
Resolving agent authentication failures manually on Solaris and Windows .....	110
Verifying that Veritas Backup Reporter is running properly .....	111
Stopping and starting Veritas Backup Reporter services .....	112
About Veritas Backup Reporter services .....	112
Stopping and restarting the Veritas Backup Reporter Management Server .....	113
Stopping and starting the Veritas Backup Reporter Agent .....	115
 Chapter 3	
Introducing the Veritas Backup Reporter console .....	119
Logging on to Veritas Backup Reporter console .....	119
About the Veritas Backup Reporter console .....	122
About the Veritas Backup Reporter console header .....	123
About the Veritas Backup Reporter console tabs .....	123
About the Veritas Backup Reporter console task pane .....	125
About the Veritas Backup Reporter console content pane .....	125
Accessing product Help .....	126
Using the Symhelp search tool .....	126
Accessing NetBackup Operations Manager host .....	127
 Chapter 4	
Configuring Veritas Backup Reporter Management Server .....	129
Editing links to Symantec products .....	130
Configuring the data retention period .....	131
Disabling demo database purging .....	131

About changing the database password .....	132
About changes in the vbr_conf.properties file .....	133
About changes in the the support.exe file .....	133
Backing up the Veritas Backup Reporter database .....	133
Restoring the Veritas Backup Reporter database .....	134
Configuring SMTP server using global system settings .....	137
Defining view-level aliases .....	138
Copying user-defined content .....	138
Configuring Web server settings .....	139
Configuring the SMTP server .....	139
Changing the Web server port .....	140
Configuring Veritas Backup Reporter Management Server logging .....	142
Modifying AT configuration manually .....	143
Upgrading VBR Management Server from AB > Root + AB .....	144
Downgrading VBR Management Server from AB > Root + AB or moving the remote Root .....	146
About creating and importing views in XML .....	150
Modifying the default export directory for scheduled reports .....	150
Cleaning temporary files generated with reports .....	152
Setting up trust relationships between Veritas Backup Reporter on hosts .....	153
Managing Veritas Backup Reporter Management Server SSL certificates .....	155
Viewing SSL certificate information .....	155
Creating a self-signed SSL certificate .....	156
Exporting an SSL certificate to a file .....	157
Configuring a CA-signed SSL certificate .....	158
About cloning SSL certificates .....	159
Managing licenses .....	160
About licensing model .....	160
Adding license keys .....	161
Viewing license keys .....	162
Deleting license keys .....	162
Managing user accounts .....	163
Adding existing domain users to Veritas Backup Reporter .....	163
Creating a private domain user account .....	164
Viewing Veritas Backup Reporter user account information .....	165
Editing Veritas Backup Reporter user accounts .....	166
Deleting Veritas Backup Reporter user accounts .....	166
Creating Veritas Backup Reporter user groups .....	166
Adding users to Veritas Backup Reporter user groups .....	167

Editing user groups .....	167
Deleting Veritas Backup Reporter user groups .....	168
Merging objects .....	168

## Chapter 5

Understanding data collection .....	171
About data collection in Veritas Backup Reporter .....	172
About data collection checklist .....	173
Modifying Veritas Backup Reporter Agent configuration .....	174
Changing Management Server host for an Agent .....	176
Viewing agent status .....	177
Viewing all agents status summary .....	178
Viewing status of configured data collectors .....	179
About data collection status .....	180
Viewing the complete agent status summary .....	181
Viewing agent data transmission errors .....	184
Removing agent configurations from the management server .....	184
Viewing agent alerts .....	185
About data collectors .....	185
About products and their versions supported by Veritas Backup	
Reporter .....	187
Managing data collectors .....	188
Configuring a data collector .....	189
Modifying data collector configurations .....	195
Collecting data by the force poll method .....	196
Copying data collector configurations .....	197
Deleting data collectors .....	197
Collecting NetBackup data .....	198
About Policy and Scheduled Jobs data collected in VBR 6.6 .....	198
Configuring NetBackup data collector .....	201
About Breakup Jobs option .....	210
Collecting data from NBAC enabled NetBackup Master Server	
.....	213
About the Library Capacity option .....	218
NetBackup data collection checklist .....	219
Collecting data from Backup Exec .....	221
Collecting data from PureDisk .....	223
About AT configuration scenarios specific to PureDisk backup	
product .....	226
Configuring NetBackup PureDisk data collector .....	229
Moving the Root Broker from PureDisk SPA host to VBR	
Management Server .....	230
Installing a release update on PureDisk 6.2.2 host .....	233

Collecting data from Legato Networker .....	234
Collecting data from IBM Tivoli Storage Manager .....	235
Collecting data from CommVault .....	236
Collecting data from Enterprise Vault .....	237
About Enterprise Vault .....	237
About data collected from Enterprise Vault .....	238
About versions supported by Veritas Backup Reporter .....	240
Planning the Enterprise Vault data collector deployment .....	240
About Enterprise Vault data collector deployment modes .....	241
Accessing MS SQL Server host .....	243
About creating a user for integrated login .....	246
Configuring the Veritas Backup Reporter Agent properties for integrated login .....	248
Installing MS SQL Server JDBC driver .....	250
Configuring Enterprise Vault data collector .....	251
About enhancement in agentdatacollectionutility .....	258
 Chapter 6	
Managing User Settings .....	261
Updating your personal information .....	261
Changing your password .....	261
Configuring and managing report-based notifications .....	262
Managing report schedules .....	263
Managing email distribution lists .....	264
Managing email notifications .....	265
Configuring reports to trigger alerts .....	269
About substituting tokens to provide variable data in notifications .....	272
Exporting reports .....	273
About managing export schedules .....	273
Setting up exporting of reports .....	273
Setting a default currency for cost reports .....	275
 Chapter 7	
Managing Veritas Backup Reporter views .....	277
About Java View Builder .....	278
About Java View Builder enhancements in VBR 6.6 .....	279
Running the Veritas Backup Reporter Java View Builder .....	281
Creating views in Java View Builder .....	281
Creating levels in views .....	282
Adding objects to views .....	282
Searching for objects .....	283
Removing views, levels, or objects .....	283
Renaming views, levels, and objects .....	284

Managing user access to views .....	284
Managing user access to levels or objects .....	285
Viewing object views .....	285
About navigating object views .....	286
Selecting object view categories .....	286
About object levels .....	287
Viewing a list of hosts .....	288
Searching for hosts .....	288
Viewing details about hosts and file systems .....	288
About viewing tabular information about a class of objects .....	291
Customizing views .....	291
About creating custom views using the View Builder .....	292
About creating backup views to display data by file system .....	292
Verifying your customized host views .....	292
Managing attributes .....	293
About viewing attributes .....	294
Editing attributes .....	294
Chapter 8      Understanding Veritas Backup Reporter alerts .....	295
About alerts and the Alert Manager .....	295
Working with alert recipients .....	298
Viewing alert recipients .....	298
Creating email recipients .....	300
Creating SNMP trap recipients .....	303
Modifying email / trap recipient information .....	305
Adding alert recipient groups .....	306
Working with alert policies .....	307
Creating alert policies .....	307
About modifying alert policies .....	312
Viewing alert policies .....	312
Managing alert policies .....	313
Setting alert filters .....	314
Configuring pagination settings .....	315
Working with alerts .....	315
Viewing alerts .....	315
Managing alerts .....	318
About Alert Manager log files .....	320
Customizing Alert Manager settings .....	321
Enabling or disabling Alert Manager .....	322
About customizing autoclear and autcount alert settings .....	322
Using SNMP with Veritas Backup Reporter .....	323
About SNMP .....	323

	About SNMP versions .....	324
	About SNMP version supported in Veritas Backup Reporter .....	325
	About the Management Information Base (MIB) and Veritas Backup Reporter support .....	325
	About generating SNMP traps using Alert Manager .....	325
	Configuring the SNMP trap community name for Veritas Backup Reporter .....	325
	Configuring the port for sending SNMP traps .....	326
	Frequently asked SNMP questions .....	327
<b>Chapter 9</b>	<b>Reporting on backup and archive data .....</b>	<b>329</b>
	About VBR reports .....	329
	About report types .....	330
	Using report formats .....	331
	About backup and recovery reports .....	333
	About disk-based data protection reports .....	336
	About deduplication backup reports .....	337
	About the new nomenclature in post-VBR-6.5 versions .....	338
	Using reports for notification .....	340
	Using report data to notify staff when problems occur .....	341
	Using report data to trigger alerts .....	341
	Sending routine report information .....	342
	Using the reports portal pages .....	343
	Refreshing reports portal pages .....	344
	About selecting reports using the tree view .....	344
	Creating sections on a portal page .....	344
	Editing sections on a portal page .....	345
	Deleting sections on reports' portal page .....	345
	Managing the report folders .....	346
	Updating cached reports .....	347
	Using default reports .....	348
	About changes in the default / canned reports UI .....	349
	Loading sample reports .....	349
	Specifying the report scope and time frame .....	350
	Customizing an existing report .....	351
	About Report Wizard parameters .....	352
	Generating backup reports .....	357
	Generating Client Risk Analysis report .....	357
	About Advanced Success Rate reports .....	358
	About Drive Analysis reports .....	360
	About viewing Drive Utilization and Drive Throughput reports in a heat chart format .....	360



Chapter 10	Managing cost analysis and chargeback for services .....	451
	About generating cost reports .....	451
	Estimating baseline (chargeback) costs .....	452
	Creating cost variables .....	455
	Modifying cost variables .....	457
	Managing cost formulas .....	458
	Creating cost formulas .....	458
	Modifying cost formulas .....	459
	Deleting a cost formula .....	459
	Generating a cost report .....	460
	Viewing a cost report with the currency of your choice .....	462
	Setting global currencies .....	463
	Setting the default currency .....	464
	Generating savings reports .....	465
Chapter 11	Performance tuning .....	467
	Setting the max heap size .....	467
Chapter 12	Resolving Veritas Backup Reporter issues .....	469
	Troubleshooting Veritas Backup Reporter issues .....	469
	About troubleshooting Veritas Backup Reporter console issues .....	469
	About Veritas Backup Reporter log files .....	472
	About Veritas Backup Reporter status codes and recommended troubleshooting steps .....	475
	Gathering troubleshooting data with the support script .....	511
	About contacting the Veritas Backup Reporter support team .....	512
	About using the Symantec support Web site .....	512
	About subscribing to the Symantec email notification service .....	512
	About accessing Symantec telephone support .....	513
	About support for software updates .....	513
	About obtaining license information .....	513
	About purchasing Symantec products .....	513
	About commenting on Symantec product documentation .....	513
Appendix A	About the Veritas Backup Reporter database .....	515
	About the VBR database schema .....	515
	About namespaces for the VBR Management Server .....	516

	About querying the VBR database .....	516
	About accessing the VBR database using dbisql .....	517
	About accessing the database using JDBC .....	518
Appendix B	Command and configuration file reference .....	519
	Command and configuration file locator .....	519
Appendix C	XML interface reference .....	559
	About the XML API .....	559
	About the XML DTD .....	560
	About the DTD elements .....	561
	About the <application> element .....	561
	About <objects> and <object> elements .....	561
	About <attribute> elements .....	563
	About the <view> element .....	563
	About <node> elements .....	563
	About <aliaslevel> elements .....	564
	About <user> elements .....	564
	About <mergeitems> and <mergeitem> elements .....	566
	Examples of XML files .....	566
	Example 1: Adding objects and a tree .....	567
	Example 2: Updating two hosts .....	570
	Example 3: Deleting a host .....	570
	Example 4: Merging objects .....	571
Appendix D	Using the Veritas Backup Reporter Knowledge Base .....	575
	About the Veritas Backup Reporter Knowledge Base .....	575
	Browsing Knowledge Base entries .....	575
	Creating Knowledge Base entries .....	576
	Modifying Knowledge Base entries .....	577
	Deleting Knowledge Base entries .....	578
Appendix E	Attributes of NetBackup data .....	579
	About backup data attributes .....	579
	Veritas Backup Reporter Glossary .....	611
	Index .....	613

# Overview of Veritas Backup Reporter 6.6

This chapter includes the following topics:

- [About Veritas Backup Reporter](#)
- [About what's new in Veritas Backup Reporter 6.6](#)
- [About Veritas Backup Reporter components](#)
- [About Veritas Backup Reporter documentation](#)

## About Veritas Backup Reporter

Veritas™ Backup Reporter (VBR) is a Web-based software application that helps organizations by providing visibility into their data protection environment. By using Veritas Backup Reporter, you can track the effectiveness of data backup and archive operations by generating comprehensive business-level reports.

---

**Note:** Archive data collection from Symantec Enterprise Vault is introduced with VBR 6.6 version.

---

Veritas Backup Reporter displays customizable, multi-level views of backup and archive resources and customizable reports for tracking service usage and expenditures. It also contains tools for defining cost metrics and chargeback formulas or handling alerts.

A wide range of audiences benefit from the reporting and management capabilities of Veritas Backup Reporter. The audiences include IT (Information Technology) managers, application owners, IT finance teams, external compliance auditors,

legal teams, line-of-business managers, external customers, IT architects, and capacity planning teams.

The primary objectives of Veritas Backup Reporter are as follows:

- Help organizations assess their compliance with business standards by allowing them to accomplish the following:
  - Manage service level agreements
  - Report to legal department, auditors, IT managers, and administrators
  - Verify compliance with internal as well as external business-level regulations
  - Identify risks in terms of shortfall of backup resources
  - Assess recovery of clients and applications
- Assist organizations in effective business planning by enabling them to do the following:
  - Estimate backup resources required in the future, with the help of backup trend analysis
  - Calculate the cost of data protection management and chargeback to customers and business units

---

**Note:** You can generate cost reports only for backup data. Cost reports for archive data are not available.

---

- Provide support to multiple backup products

## About compliance reporting

Veritas Backup Reporter helps organizations evaluate their compliance with internal and external business standards by providing accurate and customizable reports. By using internal compliance reports, you can measure performance of the system against service level agreement (SLA). The results are then used to optimize data protection management. The reports, such as history or trend analysis, ensure your compliance with SLA. By using these reports, you can track the usage of backup resources and identify the risks involved. For example, you can generate a report that anticipates a shortfall of resources in the future based on the current backup trend. This report is then used to determine the time required to purchase new tape drives, master servers, or media servers.

External compliance reports help you follow the policies laid down by various regulatory bodies that are related to federal, healthcare, internal processes, and

others. These policies include Sarbanes-Oxley act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

In addition to tracking the backup or archive information, Veritas Backup Reporter reports ensure recovery of key information assets. The reports can help you ensure that the data recovery meets the recovery-time and recovery-point objectives.

Veritas Backup Reporter can generate reports filtered by views. A view shows a set of enterprise assets (hosts or file systems) organized in logical groups. For example, you can create views to display assets according to their locations in the organization, the line of business they represent, or the applications that are installed. Veritas Backup Reporter can generate reports according to views created. These reports help you identify locations or departments containing assets with critical data. These reports are then used in resource planning.

## About business planning

Veritas Backup Reporter is a management tool that helps you optimize your data protection environment with effective business planning. It delivers backup services to organizations, which include reporting on backup and recovery trends and managing data centers. Veritas Backup Reporter supports a wide range of backup and recovery solutions including Symantec's NetBackup and BackupExec. It seamlessly integrates with Symantec's as well as third-party backup products and provides consistent reporting across them. Veritas Backup Reporter can collect data from the following target products:

- Veritas NetBackup
- Symantec BackupExec
- Veritas NetBackup PureDisk
- IBM Tivoli Storage Manager
- CommVault Galaxy Backup & Recovery
- EMC Legato Networker
- Symantec Enterprise Vault - Veritas Backup Reporter 6.6 supports Symantec Enterprise Vault.

Veritas Backup Reporter's ability to forecast backup resource requirements helps data center executives to decide whether to maintain the existing resources or add new capacity. The detailed, drill-down Veritas Backup Reporter reports help you determine the applications, databases, or business departments that are the heaviest consumers of backup resources. For example, in an environment running 20 instances of Oracle applications, you can generate a report showing resource consumption by department, server, or location. Depending on this information, organizations can provide appropriate resource planning in advance.

Veritas Backup Reporter offers you a set of chargeback reports that detail backup services expenditures. By using these reports, you can track the backup and recovery usage and the associated cost. By using the chargeback function, you can define pricing models for backup service delivery and allocate costs to customers based on these models. For example, you can create a formula that determines charges based on kilobytes of backed up data over a period of time. Using this chargeback data, you can then present itemized invoices to internal customers, export chargeback tables to third-party billing systems, or use the data to analyze and justify expenditures.

---

**Note:** You can generate cost reports only for backup data. Cost reports for archive data are not available.

---

## About reporting on archive data

In Veritas Backup Reporter 6.6, a new report category called Archives has been added. This report category contains a number of new reports that are generated based on the archive data collected from Enterprise Vault. You can report on the number of messages that are archived across mailboxes, the size of these messages before and after the archive operation.

See [“Reporting on archive data”](#) on page 405.

## About what's new in Veritas Backup Reporter 6.6

This section describes the new functions in Veritas Backup Reporter 6.6.

[Table 1-1](#) lists the new function and their descriptions.

**Table 1-1** New functions in Veritas Backup Reporter 6.6

New function	Description
Enterprise Vault Data Collection and Reporting	Archive data collection from Symantec Enterprise Vault is introduced in Veritas Backup Reporter 6.6.  You can now report on the number of messages / emails that were archived or the size of those messages before and after the archive operation. You can also compare these values across mailboxes or Enterprise Vault servers.  See <a href="#">“Reporting on archive data”</a> on page 405.

**Table 1-1**      New functions in Veritas Backup Reporter 6.6 (*continued*)

New function	Description
Scheduled Jobs Reporting for NetBackup	<p>Veritas Backup Reporter can now collect additional policy and job data, such as Policy Type, Schedule Time of Jobs, or Policy Storage Unit.</p> <p>See <a href="#">“About Policy and Scheduled Jobs data collected in VBR 6.6”</a> on page 198.</p> <p>In Veritas Backup Reporter 6.6, you can generate a new set of Scheduled Jobs reports, using which you can determine whether the jobs that were scheduled to run in future, have been run on time or not.</p> <p>See <a href="#">“Reporting on scheduled jobs data”</a> on page 390.</p>
Additional data collection from Backup Exec	<p>Veritas Backup Reporter can now collect Skipped File and Media data types from backup Exec.</p>
Windows Cluster Support (VCS)	<p>Veritas Backup Reporter is now clusterable on Windows. If you have VCS (Veritas Cluster Server) present, you can install Veritas Backup Reporter on a Windows machine in a clustered mode.</p> <p>See <a href="#">“Clustering Veritas Backup Reporter on Windows”</a> on page 88.</p>
Sybase SA 10 Upgrade	<p>VBR 6.6 uses Sybase SA (SQL Anywhere) 10 as the database management system, which is an upgrade from ASA 9. To upgrade VBR from previous versions to 6.6, you need to migrate the existing data within the database files to match the new database file format. This is because the Sybase SA 10 database engine is not compatible with an ASA 9 database file. This data migration is automatically done during the VBR 6.6 upgrade process.</p> <p>See <a href="#">“About database upgrade in VBR 6.6”</a> on page 76.</p>
New Alert Manager	<p>Alert Manager is a component that comprises an alerting mechanism. It keeps track of the alert conditions specified in the policies and generates alerts appropriately.</p> <p>The new Alert Manager replaces VxAM, a shared alerting component.</p> <p>See <a href="#">“About alerts and the Alert Manager”</a> on page 295.</p>

**Table 1-1** New functions in Veritas Backup Reporter 6.6 (*continued*)

New function	Description
Qualifications / support for new product versions	Veritas Backup Reporter now supports the following product versions: <ul style="list-style-type: none"><li>■ NetBackup 6.5.3, 6.5.4</li><li>■ PureDisk 6.2.2, 6.5.0.1, 6.5.1</li><li>■ Backup Exec 12.5</li><li>■ TSM 5.5</li></ul>

## About Veritas Backup Reporter components

This section describes the following Veritas Backup Reporter components:

- [About the Veritas Backup Reporter Management Server](#)
- [About the Veritas Backup Reporter Java View Builder](#)
- [About the Veritas Backup Reporter Agent](#)

### About the Veritas Backup Reporter Management Server

Veritas Backup Reporter Management Server, the core of the architecture, is a Web application that normalizes backup / archive data collected from various applications. This normalized data is used for reporting on backup related information.

VBR Management Server is supported on Windows and Solaris platforms.

See “[About operating system requirements](#)” on page 36.

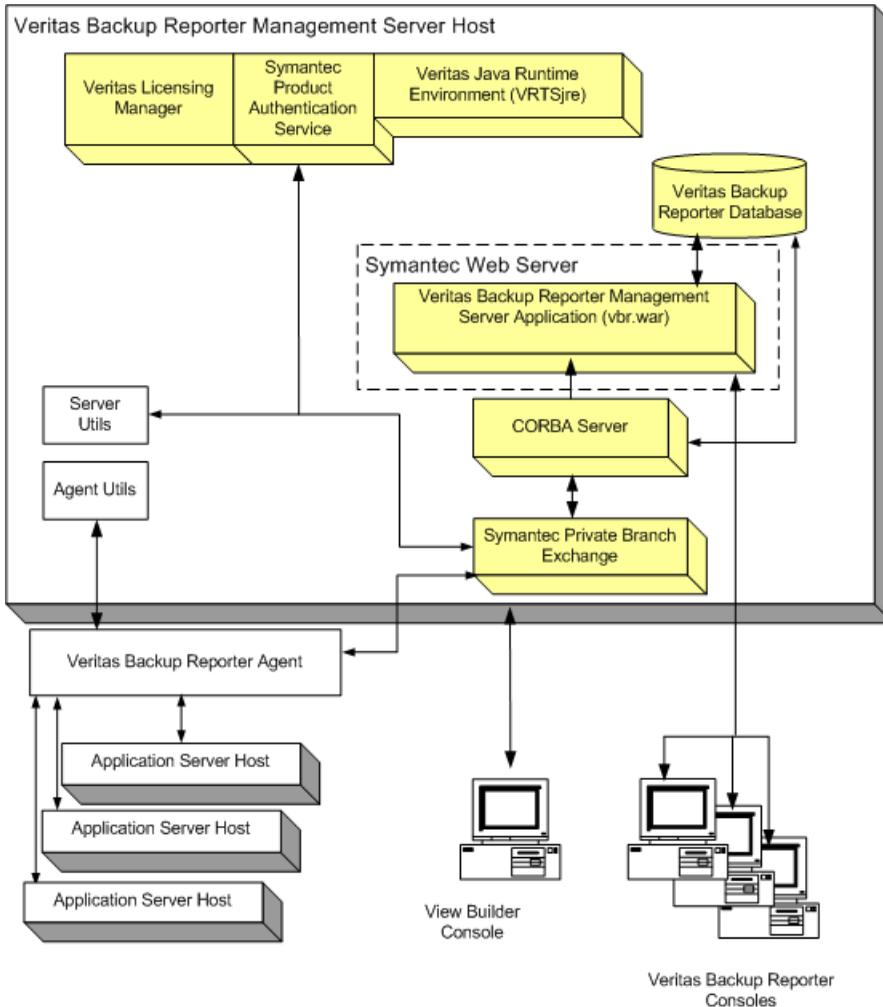
The Veritas Backup Reporter Management Server comprises the following components:

Veritas Backup Reporter database	Sybase SA (SQL Anywhere) database management system containing data related to backup /archive service usage and expenditure, cost metrics and chargeback formulas, and alerts.  VBR 6.6 uses Sybase SA 10 version. Previous VBR versions used Sybase SA 9.  See “ <a href="#">About the Veritas Backup Reporter database</a> ” on page 24.
----------------------------------	---

Symantec Product Authentication Service	<p>A set of common authentication runtime libraries and processes that enable users to log on once to access multiple products. It also validates identities based on NT, NIS, or private domains.</p> <p>See <a href="#">“About the Symantec Product Authentication Service”</a> on page 25.</p>
Alert Manager	<p>Component that provides policy-based alert management, including notification, custom actions, and SNMP management capabilities.</p> <p><b>Note:</b> VBR 6.6 replaces VxAM (Veritas Alert Manager) with the new Alert Manager component.</p> <p>See <a href="#">“About alerts and the Alert Manager”</a> on page 295.</p>
Symantec Web Server and Java Runtime Environment (JRE)	<p>A common Web server (that uses Java Server Pages) and a JRE to serve the Veritas Backup Reporter console.</p>
Veritas Licensing Manager	<p>A common Veritas licensing Module and API used to add, change, and remove Veritas product license keys.</p>
Symantec Private Branch Exchange	<p>A common component that uses socket passing to reduce the number of ports required to be open across a firewall. Symantec Private Branch Exchange uses a paradigm similar to that of a telephone switchboard in which calls placed to a switchboard are redirected to a known extension. In the PBX exchange, client connections that are sent to the exchange’s port are redirected to an extension associated with the Veritas Backup Reporter Management Server.</p>

[Figure 1-1](#) shows Veritas Backup Reporter Management Server architecture.

Figure 1-1 Veritas Backup Reporter Management Server architecture



## About the Veritas Backup Reporter database

Veritas Backup Reporter 6.6 uses Sybase SQL Anywhere 10 (SA 10) database management system as a repository for the backup data sent by VBR Agent, such as backup service usage and expenditure reports, cost metrics, chargeback formulae, and alerts.

Except for a very small number of system settings, all information that is in the Web UI is contained in the Veritas Backup Reporter database, which consists of a single cross-platform database file. You do not need to install the VBR database

yourself, it's embedded in the application. Sybase SA is also self tuning and does not require a database administrator to maintain it.

VBR supports upgrade from earlier versions to VBR 6.6, by introducing the DB consistency checker utility that runs during upgrade and ensures the consistency between SA 9 and SA 10 schemas.

See “[About database upgrade in VBR 6.6](#)” on page 76.

## About the Symantec Product Authentication Service

The VBR Management Server relies on Symantec Product Authentication Service (AT) for user authentication for connections between , VBR Management Server, Agent, and VBR Java View Builder.

The Symantec Product Authentication Service is referred to as AT.

Symantec Product Authentication Service is a shared component and is used for:

- Authenticate users to the VBR console based on external authentication systems such as Active Directory, NIS, NIS+, LDAP and even standard unix password.
- Provide for a secure transport of data between VBR agent's and the VBR server.
- Enable trust between VBR and other Symantec products that also use AT.

For more details on AT, refer to the documents at the following locations:

- AT Install Guide: <http://support.veritas.com/docs/311442>
- AT Admin Guide: <http://support.veritas.com/docs/311441>
- AT Release Notes: <http://support.veritas.com/docs/311440>

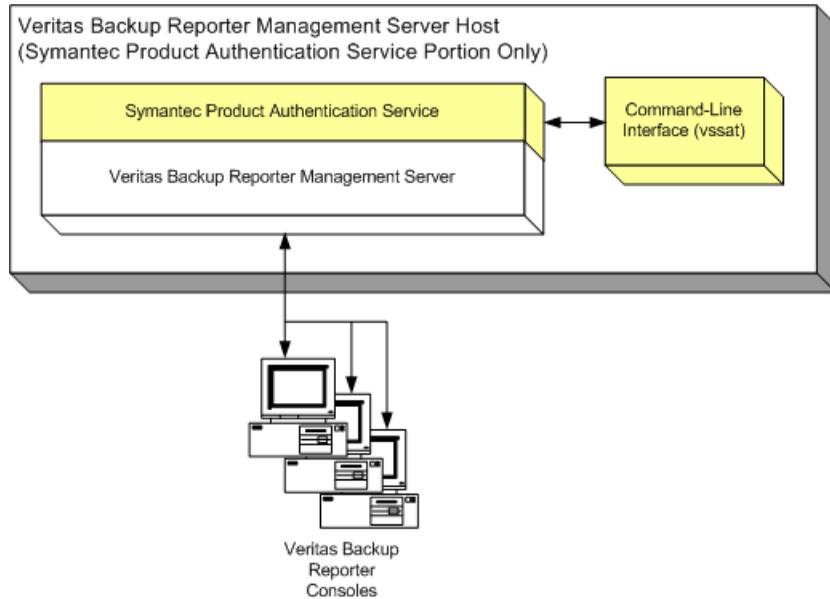
See “[About AT configuration in Veritas Backup Reporter](#)” on page 54.

When the Symantec Product Authentication Service library authenticates a user for Veritas Backup Reporter, it returns a Web credential that Veritas Backup Reporter passes along when cross-linking to other Symantec products such as NetBackup Operations Manager. The Web credential provides a limited form of user authentication so that products do not prompt the user to log on again.

See “[Accessing NetBackup Operations Manager host](#)” on page 127.

[Figure 1-2](#) shows Veritas Backup Reporter Management Server architecture with respect to Symantec Product Authentication Service.

**Figure 1-2** Symantec Product Authentication Service: architecture



## About the Veritas Backup Reporter Agent

The Veritas Backup Reporter Agent collects data from various Symantec and third-party backup / archiving products. These products can reside on the VBR Agent host or on remote hosts. The VBR Agent relies on the Java Runtime Environment (JRE) to perform its functions. The VBR Agent also requires embedded AT (Symantec Product Authentication Service) to authenticate itself with the VBR Management Server. Both JRE and AT are installed automatically with the Agent installation.

VBR Agent is supported on Windows and Solaris platforms.

See [“About operating system requirements”](#) on page 36.

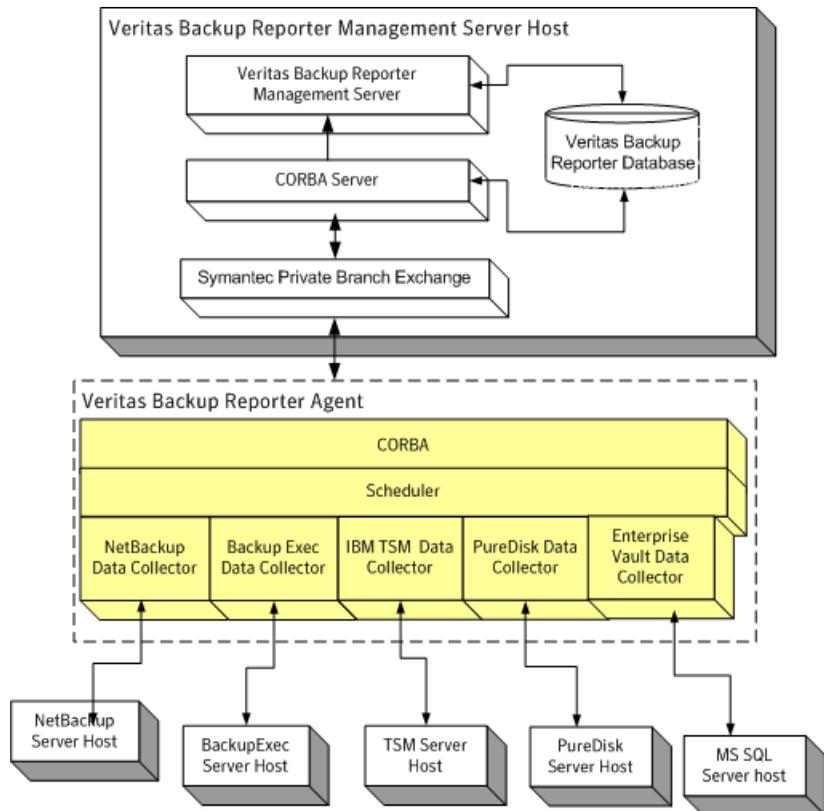
Veritas Backup Reporter formats the information collected from the following target products and displays it through the VBR console:

- Veritas NetBackup PureDisk
- Veritas NetBackup
- Symantec Backup Exec (Windows only)
- EMC Legato Networker
- IBM Tivoli Storage Manager

- CommVault Galaxy Backup & Recovery
- Symantec Enterprise Vault (Windows only)

Figure 1-3 shows VBR Agent architecture.

**Figure 1-3** Veritas Backup Reporter Agent architecture



The VBR Agent can reside on the same host as the VBR Management Server, or can be installed on a remote host. All VBR data collectors are configured on every Agent. Configure and run only these data collectors for the target product that you want to monitor / report on.

---

**Note:** Data collector was called 'Agent Module' in previous Veritas Backup Reporter versions.

---

A number of combinations of VBR Agent and Management Server installations are possible. For example, you can install an Agent on the Management Server

host and configure the NetBackup data collector to collect data from a remote NetBackup master server. Alternatively, you can install an agent on the NetBackup master server host and configure the NetBackup data collector to collect data from the local NetBackup master server.

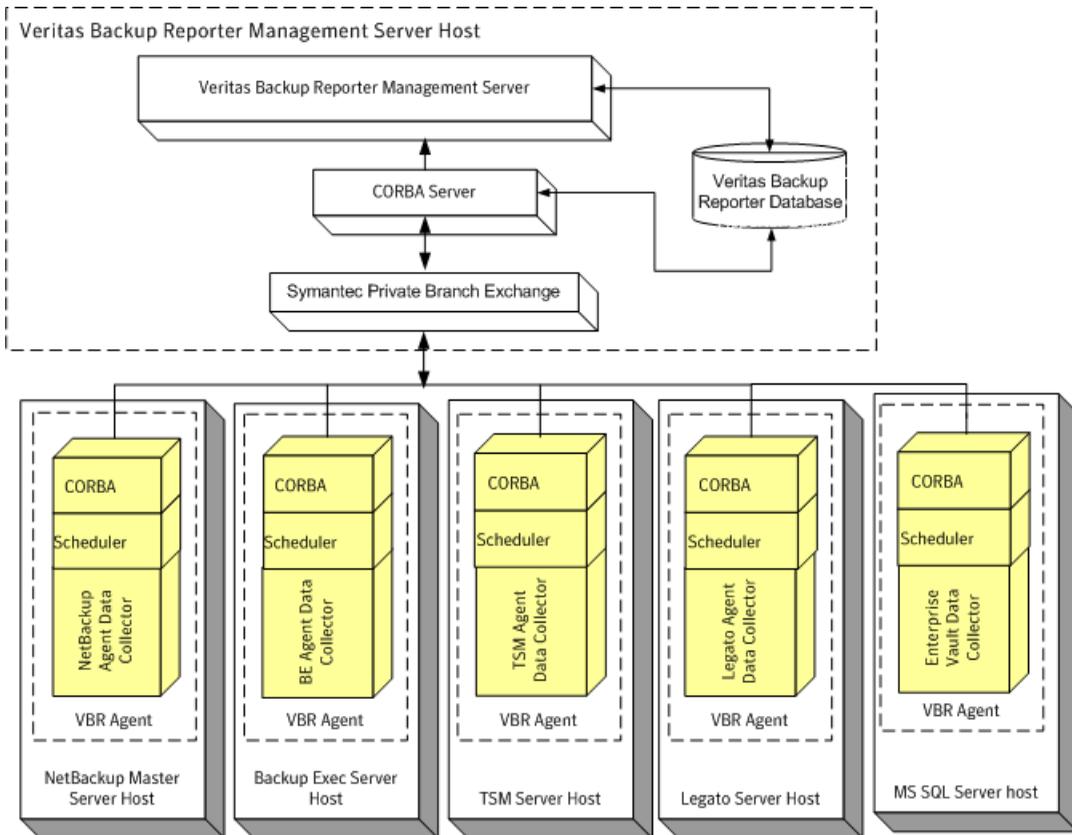
---

**Note:** Legato data collector does not support remote data collection. Therefore, the agent must be installed on the Legato server host.

---

Figure 1-4 shows the alternate Veritas Backup Reporter Agent deployment.

**Figure 1-4** Veritas Backup Reporter Agent: alternate installation



The core of the VBR Agent is a Java virtual machine (JVM) in which you run different data collectors. The VBR Agent communicates with the Management Server, schedules backup / archive data collection data types, and receives commands through the CORBA API.

As the VBR Management Server relies on Symantec Product Authentication Service to authenticate agent - management server connections, the Symantec Product Authentication Service client libraries reside on the agent host.

The Veritas Backup Reporter Agent comprises Scheduler, CORBA Client/Server, and data collectors that collect backup data from all available backup application. The Scheduler and CORBA form the agent core.

[About the scheduler](#)

[About the CORBA Client/Server](#)

[About data collectors](#)

## About the scheduler

The scheduler performs three basic functions for the VBR Agent:

- Checks the data collection schedules of all running data collectors and queues them.
- Periodically sends a heartbeat message to the VBR Management Server to ensure the reliability of communications between the agent and the server.
- Monitors modifications made to the agent configuration using the VBR console, which are stored on the VBR Management Server.

## About the CORBA Client/Server

The VBR Agent implements a CORBA server that listens on a configurable port (default 7806) that allows the VBR console to get the runtime status of the Agent. When you send a request to get the Agent status through the VBR UI, the VBR Management Server send the request to CORBA Server to receive the requested information.

The Agent behaves as a CORBA client when sending data or alerts to the Veritas Backup Reporter Management Server.

## About data collectors

The data collectors (formerly known as 'agent modules') convert the data specific to backup or archive products into a format that can be used by the Veritas Backup Reporter Management Server. Each data collector must conform to an interface that defines its interaction with the VBR Agent. The data collector is implemented in a way that suits the underlying product.

Data collector configurations consist of general parameters (such as log configurations and data collection event definitions, which are shared by all data collectors) and product-specific values.

You need to configure a data collector on the VBR Agent host that collects data from a backup or archive product host.

## About Agent configuration and logging

Agent configuration settings are stored in the Veritas Backup Reporter database. The VBR Agent also caches the latest version of the configuration settings in the `agent.conf` file. The agent compares the local `agent.conf` file with the one stored in the database when the agent process is started. If the agent process has already started, any changes made to the local `agent.conf` file do not take place until the agent is restarted.

---

**Note:** You should not modify the `agent.conf` file. You should change the agent configuration settings using the VBR Agent Configuration UI.

---

The changes that you have made to the agent configuration settings using the VBR UI or console are reflected after the next heartbeat.

A heartbeat is a request that the VBR Agent sends to the Management Server to check for any new changes in the configuration settings. By default, a heartbeat is sent every minute.

Logging for the agent core and individual data collector is administered in the same fashion but written to different log files.

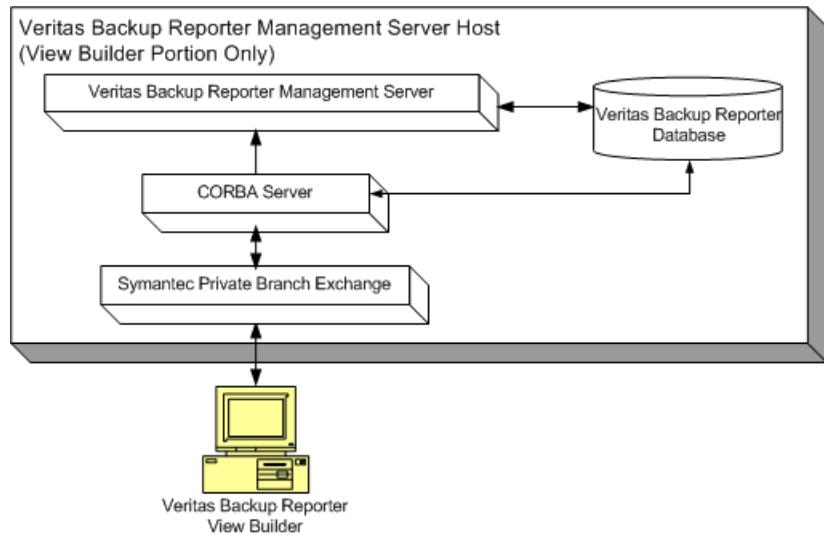
See “[About Veritas Backup Reporter log files](#)” on page 472.

## About the Veritas Backup Reporter Java View Builder

The Veritas Backup Reporter Java View Builder is an application in which an administrator creates, modifies, and manages access to the Veritas Backup Reporter views that users see in the console.

[Figure 1-5](#) shows Veritas Backup Reporter Java View Builder architecture.

**Figure 1-5** Veritas Backup Reporter Java View Builder architecture



The Java View Builder relies on the AT client libraries which is installed automatically to communicate properly with the management server. To use the Java View Builder, you need to provide login credentials as you do while logging onto the VBR console.

See [“Logging on to Veritas Backup Reporter console”](#) on page 119.

When you run the Java View Builder exe, it is directly connected to the Veritas Backup Reporter Management Server. The View Builder fetches the existing object view definitions from Veritas Backup Reporter database and displays them in the Veritas Backup Reporter console. Actions performed using the View Builder console are then stored in the Veritas Backup Reporter database.

## About Veritas Backup Reporter documentation

The following documents provide information about Veritas Backup Reporter, which are available on the product CD:

- Veritas Backup Reporter Guide (vbrguide.pdf)  
 This document replaces the following documents that were shipped with the previous Veritas Backup Reporter versions.
  - Veritas Backup Reporter getting Started Guide
  - Veritas Backup Reporter Installation Guide
  - Veritas Backup Reporter Clustering Guide

- Veritas Backup Reporter Administrator's Guide
- Veritas Backup Reporter User's Guide
- Veritas Backup Reporter Hardware and Software Compatibility List (HSCL.pdf)
- Veritas Backup Reporter Release Notes (notes.pdf)

---

**Note:** The Symantec End User License Agreement (EULA.pdf) is provided along with these user documents.

---

---

**Note:** For the latest support information, for example, supported products or operating systems, see the *Veritas Backup Reporter Hardware and Software Compatibility List*, which is regularly updated on the Symantec Support Web site. Access the following URL:

<http://www.symantec.com/enterprise/support/index.jsp>

---

You can find the Veritas Backup Reporter documents on the following default locations on the Veritas Backup Reporter Management Server host:

Windows	C:\Program Files\Symantec\Veritas Backup Reporter\Docs
Solaris	/opt/VRTS/docs

In addition to the PDF (Portable Document Format) documents, Veritas Backup Reporter is also shipped with the following Online Help documents:

Veritas backup Reporter online Help	This WebGUI Help contains all information about the Veritas Backup Reporter application. See <a href="#">“Accessing product Help”</a> on page 126.
Man pages for utilities	Veritas Backup Reporter is shipped with man pages / manual pages for various utilities that you can run from command prompt. Man pages are used to find reference and usage information about product-specific commands on UNIX computers. See <a href="#">“Command and configuration file locator”</a> on page 519.

### Symhelp search

Veritas Backup Reporter provides a next generation context-sensitive help search tool called Symhelp that you can use to search for a particular Veritas Backup Reporter topic.

See [“Using the Symhelp search tool”](#) on page 126.

**Note:** The Symhelp may not be updated. For the most recent information about Veritas Backup Reporter, refer to the PDF documents.

### Java View Builder context-sensitive Help

This Java Help contains information about all information about Java View Builder dialog boxes and the procedures you carry out. You can access the context-sensitive Help by clicking the ‘Help’ button available on a dialog box in the Java View Builder console.



# Installing Veritas Backup Reporter

This chapter includes the following topics:

- [Planning your Veritas Backup Reporter installation](#)
- [Installing Veritas Backup Reporter on Solaris and Windows](#)
- [Upgrading Veritas Backup Reporter](#)
- [Clustering Veritas Backup Reporter](#)
- [Resolving agent authentication failures manually on Solaris and Windows](#)
- [Verifying that Veritas Backup Reporter is running properly](#)
- [Stopping and starting Veritas Backup Reporter services](#)

## Planning your Veritas Backup Reporter installation

This section provides information on what all you need to take care of, before proceeding to Veritas Backup installation or upgrade.

### Prerequisites

This section lists the prerequisites for Veritas Backup Reporter installation.

- On Windows system, the Veritas Backup Reporter Management Server, Agent, and Java View Builder require the Microsoft C Runtime library 7.1 and Microsoft C++ runtime library 7.1.

## About operating system requirements

This section provides information about the operating systems supported by Veritas Backup Reporter and their requirements.

[Table 2-1](#) lists the operating system requirements for Veritas Backup Reporter hosts.

**Table 2-1** Veritas Backup Reporter operating system requirements

Veritas Backup Reporter component	Supported configuration	System resources
<p>Management Server</p>	<p>Solaris 8.0, 9.0, or 10.0 [64-bit only]</p> <p>Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)</p> <p>Windows Server 2003 (Standard Edition [32-bit], Enterprise Edition [32-bit], Datacenter Edition [32-bit], Web Edition)</p> <p>Windows Server 2003 64-bit Edition</p> <p>VMware ESX Server 3.0</p> <p>See <a href="#">“About important notes on operating systems and VBR deployment limitations”</a> on page 38.</p>	<p>Solaris</p> <ul style="list-style-type: none"> <li>■ 2 x 1 GHz UltraSPARC® IIIi processor or faster CPUs, 4 GB RAM, 40 GB of file system space (Minimum)</li> <li>■ 4 x 1 GHz UltraSPARC® IIIi processor or faster CPUs, 12 GB RAM, 2 dedicated disks of 20 GB each, for DB (Recommended)</li> </ul> <p>Windows</p> <ul style="list-style-type: none"> <li>■ 2 x 2.5 GHz or faster CPUs, 4 GB RAM, 40 GB of file system space (Minimum)</li> <li>■ 4 x 2.5 GHz or faster CPUs, 8 GB RAM, 2 dedicated disks of 20 GB each, for DB (Recommended)</li> </ul>
<p>Agent</p>	<p>Solaris 8.0, 9.0, or 10.0 [64-bit only]</p> <p>Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)</p> <p>Windows Server 2003 (Standard Edition [32-bit], Enterprise Edition [32-bit], Datacenter Edition [32-bit], Web Edition)</p> <p>Windows Server 2003 64-bit Edition</p> <p>VMware ESX Server 3.0</p> <p>See <a href="#">“About important notes on operating systems and VBR deployment limitations”</a> on page 38.</p>	<p>Solaris</p> <ul style="list-style-type: none"> <li>■ 1 GHz, 1 GB RAM (Minimum)</li> </ul> <p>Windows</p> <ul style="list-style-type: none"> <li>■ 2.5 GHz, 1GB RAM (Minimum)</li> </ul>

**Table 2-1** Veritas Backup Reporter operating system requirements (*continued*)

Veritas Backup Reporter component	Supported configuration	System resources
Java View Builder	Solaris 8.0, 9.0, or 10.0 [64-bit only]  Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)  Windows Server 2003 (Standard Edition [32-bit only], Enterprise Edition [32-bit only], Datacenter Edition [32-bit only], Web Edition)  Windows Server 2003 64-bit Edition	Solaris ■ 1 GHz, 1 GB RAM (Minimum)  Windows ■ 2.5 GHz, 1GB RAM (Minimum)
Console	Any platform with network access to the Veritas Backup Reporter Management Server host and a supported Web browser.  Veritas Backup Reporter supports the following Web browsers: ■ For Solaris - Mozilla Firefox 1.5 ■ For Windows - Mozilla Firefox 1.5, Internet Explorer 6.0 or 6.x	The minimum required resolution for the console is 1024 x 768.

[Table 2-2](#) provides the matrix for the operating systems and VBR deployments that these operating systems support.

**Table 2-2** Operating systems-VBR deployment support matrix

Operating System	Architecture	Fresh Installation	Upgrade	Push Installation	Cluster with VCS	Remote AT Root Broker (Fresh Installation and Upgrade)
Windows 2003	32-bit VBR binaries on 32-bit machine	X	X	X	X	X
	32-bit VBR binaries on 64-bit machine	X	X			X
Windows 2000 SP4	32-bit VBR binaries on 32-bit machine	X	X			X
Solaris 8.0	64-bit VBR binaries on 64-bit machine	X	X		X	X

**Table 2-2** Operating systems-VBR deployment support matrix (*continued*)

Operating System	Architecture	Fresh Installation	Upgrade	Push Installation	Cluster with VCS	Remote AT Root Broker (Fresh Installation and Upgrade)
Solaris 9.0	64-bit VBR binaries on 64-bit machine	X	X		X	X
Solaris 10.0	64-bit VBR binaries on 64-bit machine	X	X		X	X

“X” indicates that the configuration is supported in VBR.

### About important notes on operating systems and VBR deployment limitations

This section provides a few important notes regarding the supported operating systems and a few limitations that you need to take care of during VBR deployment.

#### Important notes on operating systems

- On Windows system, the VBR Management Server, Agent, and Java View Builder require the Microsoft C Runtime library 7.1 and Microsoft C++ runtime library 7.1.
- The VBR Management Server is not supported on non-global Solaris zones.
- The VBR Management Server and Agent are supported in a VMware virtual machine guest operating system environment.

#### VBR deployment limitations

- You must install VBR Management Server and Agent of the same versions. For example, Agent 6.2 MP3 works only with Management Server 6.2 MP3 or Management Server 6.5 is compatible only with Agent 6.5.
- The VBR Management Server and Agent can be installed in a clustered mode on Solaris and Windows, with Veritas Cluster Server (VCS).
- VBR Management Server and Agent must be installed on different hosts if they both need to be in clustered mode. If they are installed on the same host, only Management Server can be clustered.
- Veritas Backup Reporter does not support a set up in which NetBackup Operations Manager and VBR Management Server are installed on the same host.

- The Veritas Backup Reporter installer automatically sets the max heap size to 1024MB. Your system may require a lesser max heap size to properly run all applications. You can set the max heap size to 512MB. For more information, refer to the Performance Tuning section in the Veritas Backup Reporter Guide.

## About Windows updates

Table 2-3 lists the required Windows 2000 software updates to be run on Veritas Backup Reporter components.

**Table 2-3** Required Windows 2000 software updates

Veritas Backup Reporter component	Operating systems supported
Veritas Backup Reporter Management Server	Windows 2000 Service Pack 3
Veritas Backup Reporter Agent	Windows 2000 Service Pack 3

## Installing Solaris updates

This section provides the Solaris patches that you need to install on Veritas Backup Reporter host.

In addition to the required patches listed here, you may want to install the latest full patch cluster for your version of Solaris. Patch clusters include additional security patches that are recommended. You can download Solaris patches and patch clusters from <http://sunsolve.sun.com>.

### To view the currently installed Solaris patches

- 1 Type the following command to view the list of patches:  
**showrev -p**
- 2 Type the following command to check whether a particular patch is installed:  
**showrev -p | grep <patch-id>**  
where patch-id is the patch number in the format xxxxxx-xx

## About the Solaris 8 patches

You must install the following Solaris 8 patches on the Veritas Backup Reporter host:

112396-03 111111-07 108987-18 112003-03 111310-01 108528-29 108989-02 112472-01  
 111308-05 112438-03 117000-05 111023-03 115827-01 116602-01 113648-04 109147-43  
 110386-04 111317-07 108993-66 108434-22 119067-06 108921-25 109326-18 113886-42  
 108435-22 108773-27 108940-76 113887-42 117350-46

## About the Solaris 9 patches

You must install the following Solaris 9 patches on the Veritas Backup Reporter host:

113096-03 111711-16 112963-30 111712-16 113886-42 113887-42 112785-60

## About supported upgrade paths

Veritas Backup Reporter 6.6 supports direct upgrades from the following versions:

- VBR 6.0 GA -> VBR 6.6
- VBR 6.0 MP1a -> VBR 6.6
- VBR 6.2 GA -> VBR 6.6
- VBR 6.2MP1 -> VBR 6.6
- VBR 6.2MP2 -> VBR 6.6
- VBR 6.2MP3 -> VBR 6.6
- VBR 6.5 GA -> VBR 6.6
- VBR 6.5.1 -> VBR 6.6
- VBR 6.5.1.1 -> VBR 6.6

VBR 6.6 also supports upgrade from the CommandCentral Service (CCService) 4.2 version, if you follow this upgrade path:

- CCService 4.2 -> CCService 4.2FP1 -> VBR 6.0 GA -> VBR 6.6

## About products and their versions supported by Veritas Backup Reporter

This section lists the backup products and their versions that are supported by Veritas Backup Reporter.

[Table 2-4](#) lists backup products supported by Veritas Backup Reporter.

**Table 2-4** Backup products supported by Veritas Backup Reporter

Backup product	Versions	Support level
Veritas NetBackup	3.4, 3.4.1, 4.5, 5.0, 5.1, 6.0, 6.0 MPx, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4	All supported NetBackup platforms via remote agent  Native agent for Windows 2000, 2003 and Solaris 8, 9, and 10
Veritas NetBackup PureDisk	6.2, 6.2.1, 6.2.2, 6.5, 6.5.0.1, 6.5.1	PureDisk supported platform (PDOS) via remote agent
Symantec Backup Exec	10.0, 10d, 11d, 12, 12.5  <b>Note:</b> Symantec Backup Exec running on NetWare is not supported by Veritas Backup Reporter.	All supported Symantec Backup Exec platforms via remote agent  Native agent on backup servers on Windows 2000, 2003  <b>Note:</b> VBR 6.6 does not support data collection from Backup Exec 9.x version. You need to create a data collector to collect data from Backup Exec 10d and later versions. However, you can run the reports on the Backup Exec 9.x data.
EMC Legato NetWorker	6.x, 7.x	Native agent on backup servers on Windows 2000, 2003 and Solaris 8, 9, and 10
IBM Tivoli Storage Manager (TSM)	5.1, 5.2, 5.3, 5.4, 5.5	All supported TSM platforms via remote agent  Native agent for backup server on Windows 2000, 2003 and Solaris 8, 9, and 10
CommVault Galaxy Backup & Recovery	5.9 SP3	All supported CommVault platforms via remote agent
Symantec Enterprise Vault	2007 SP3, 2008	All supported Symantec Enterprise Vault platforms via remote agent  Native agent on Microsoft SQL Server 2005 or 2008 (where Enterprise Vault database resides) on Windows 2000 and 2003

## About Veritas Backup Reporter Agent deployment

This section describes the deployment scenarios of Veritas Backup Reporter Agent. It helps you decide the Agent deployment in your environment.

---

**Note:** You must install VBR Management Server and Agent of the same versions. For example, Agent 6.2 MP3 works only with Management Server 6.2 MP3 or Management Server 6.5 is compatible only with Agent 6.5.

---

Veritas Backup Reporter Agent can either be deployed on the Management Server host, product host (for example, NetBackup host), or a separate host (remote Agent). This depends on the product that you want to collect data from and its operating system. The prerequisites for collecting data from each product vary and which are described in their respective data collection sections.

See [“About products and their versions supported by Veritas Backup Reporter”](#) on page 187.

A single Agent can have multiple data collectors configured, one for each product / product version, which collect data from various products.

See [“About data collection in Veritas Backup Reporter”](#) on page 172.

Only one Agent can be installed on a single host, which can have multiple data collectors (were called 'Agent Modules' previously) configured.

See [“Installing Veritas Backup Reporter on Solaris and Windows”](#) on page 59.

---

**Note:** The **Create** link on the **Settings > Global Settings > Agent Configuration** page guides you on where to look in the VBR documentation to install an Agent or change the VBR Management Server host for the existing Agent.

See [“Installing Veritas Backup Reporter on Solaris and Windows”](#) on page 59.

See [“Changing Management Server host for an Agent”](#) on page 176.

In VBR 6.6, you cannot create an Agent using the VBR console. However, you can modify the Agent that you have installed through VBR installation wizard.

See [“Modifying Veritas Backup Reporter Agent configuration”](#) on page 174.

---

### About Agent deployment in case of different product versions

The following section describes what should be the Agent deployment if you want to collect data from different product versions.

NetBackup	You need separate VBR Agents to collect data from different versions of NetBackup Master Server. NetBackup binaries (Remote Admin Console for Windows and Master or Media Server for Solaris) installed on the Agent host should match the version of the NetBackup Master Server.
PureDisk	If the AT Root Broker hierarchy is maintained, you can use same VBR Agent to collect data from PureDisk servers with different versions.
Backup Exec	You can use same VBR Agent to collect data from Backup Exec servers with different versions. <b>Note:</b> To collect data from Backup Exec Server host, you need to install the VBR Agent on a Windows host, as Backup Exec supports only Windows platform.
Tivoli Storage Manager (TSM)	You can use same VBR Agent to collect data from TSM servers with different versions.
EMC Legato Networker	You need separate VBR Agents for Legato servers with different versions. Agent needs to be installed on the Legato server host.
Enterprise Vault	You can use the same VBR Agent to collect Enterprise Vault data from MS SQL Servers with different versions. <b>Note:</b> To collect Enterprise Vault / archive data, you need to install the VBR Agent on a Windows host, as Enterprise Vault supports only Windows platform.

## About installing Agent on a product host

VBR Agent can be installed on a product host.

The following products support local Agent installation:

- Symantec Enterprise Vault
- Veritas NetBackup
- Symantec BackupExec
- IBM Tivoli Storage Manager
- CommVault Galaxy Backup & Recovery
- EMC Legato Networker

---

**Note:** EMC Legato Networker does not support remote VBR Agent installation. You must install the Agent on the EMC Legato Networker host.

---

Installing Agent in this fashion has a very low impact on the backup environment by adding only agent. The operating system of the backup application host must be supported by the Veritas Backup Reporter Agent.

Advantages of installing the Agent on a remote backup application host include the following:

- Ease of maintenance to upgrade agent; you only service one host.
- Minimal intrusion on backup hosts; one agent installed on a backup host.

A disadvantage of installing the Veritas Backup Reporter Agent on a remote backup application host is that the Agent may use significant system resources, which can impact the backup application host's performance.

## About installing the Agent on a host different than a product host

VBR Agent can be installed on a host different than the product host, this may be the Management Server host or a separate host.

You should deploy remote Agent in the following situations:

- As per the company rules, foreign applications, for example Veritas Backup Reporter, cannot reside on a product host / production server that needs to be backed up
- When the product is running on an operating system that is not supported by the Veritas Backup Reporter Agent, for example HP-UX
- In case of low performance as a result of both backup application and Veritas Backup Reporter Agent residing on the same host

In such situations, the Agent should remotely communicate with backup products.

The following products support remote Agent installation:

- Symantec Enterprise Vault
- Veritas NetBackup
- Veritas NetBackup PureDisk

---

**Note:** PureDisk does not support local Agent installation, because VBR does not support PDOS (PureDisk Operation System). Therefore PureDisk Server and VBR Agent cannot reside on the same host.

---

- Symantec BackupExec
- IBM Tivoli Storage Manager
- CommVault Galaxy Backup & Recovery

---

**Note:** Make sure that the remote Agent host has Remote Admin Console (RAC) or Master or Media Server installed, to collect data from another Master Server that you want to monitor / report on.

Solaris does not support RAC.

For other backup products, you need to have backup application client (.exe) on the Agent host to collect data remotely.

the section called “Collecting data from Enterprise Vault ”

---

Advantages of installing the Agent on the Management Server host or a separate host include the following:

- You do not have to install additional software on backup application hosts as the backup data is gathered remotely.
- You need to maintain only one machine for both Management Server and agent, which avoids the maintenance that might otherwise be involved in upgrading the agent.

Disadvantages of installing the Agent on the Management Server host include the following:

- You must install a component of the backup application on the Management Server host or a separate host.
- In some situations, a backup application license key is required for the component installed on the Veritas Backup Reporter Management Server host.

## Examples of Agent deployment in a NetBackup setup

In a NetBackup setup, the following VBR deployment scenarios are valid:

- VBR Management Server is installed on *VBRHost 1*, Agent is installed on *AgentHost 1*, and NetBackup 6.0 Master Server is installed on *ProdHost 1*. You need to install NetBackup 6.0 Remote Admin Console or NetBackup Master Server on *AgentHost 1* and configure a data collector to collect data from *ProdHost 1*.
- VBR Management Server and Agent are installed on *VBRHost 1* and NetBackup Master Server is installed on *ProdHost 1*

You need to install NetBackup 6.0 Remote Admin Console or NetBackup Master Server on *VBRHost 1* and configure a data collector to collect data from *ProdHost 1*.

- VBR Management Server is installed on *VBRHost 1* and NetBackup Master Server and Agent are installed on *ProdHost 1*

You need to configure a data collector on *VBRHost 1* to collect data from *ProdHost 1*.

- VBR Management Server and Agent are installed on *VBRHost 1*, NetBackup 6.0 Master Server is installed on *ProdHost 1* and another NetBackup 6.0 Master Server is installed on *ProdHost 2*.

You need to install NetBackup 6.0 Remote Admin Console or Master Server on *VBRHost 1* and configure two data collectors, one to collect data from *ProdHost 1* and another to collect data from *ProdHost 2*.

- VBR Management Server is installed on *VBRHost 1*, Agent A1 is installed on *AgentHost 1*, and Agent A2 is installed on *AgentHost 2*. NetBackup 6.0 Master Server is installed on *ProdHost 1* and NetBackup 6.5 Master Server is installed on *ProdHost 2*.

You need to install NetBackup 6.0 Remote Admin Console or Master Server on *AgentHost 1* and configure a data collector to collect data from *ProdHost 1* and install NetBackup 6.5 Remote Admin Console or Master Server on the *AgentHost 2* and configure a data collector to collect data from *ProdHost 2*

## About configuring Veritas Backup Reporter firewall

For the Veritas Backup Reporter Management Server, Agent, and Java View Builder to communicate across a firewall, the firewall must be configured to allow `http` access to several specific ports.

[Table 2-5](#) lists the default ports that Veritas Backup Reporter uses to transfer information.

**Table 2-5** Default ports used by Veritas Backup Reporter

Port number	Protocol	Communication Initiator > Recipient	Purpose	Impact if blocked
25	SMTP over TCP/IP	From Veritas Backup Reporter Management Server > email server  The port should be open on the Email Server	To email reports and alert notifications	Users will not be able to receive scheduled email reports if the management server cannot reach the email server that is configured to use.

**Table 2-5** Default ports used by Veritas Backup Reporter (*continued*)

Port number	Protocol	Communication Initiator > Recipient	Purpose	Impact if blocked
1556	CORBA over SSLIOP	Agent, Java View Builder, CLI tools > Veritas Backup Reporter Management Server  The port should be open on CORBA Server	To communicate with Veritas Backup Reporter Management Server (through PBX)	Veritas Backup Reporter Management Server will not respond to Agent or Java View Builder.
1885	TCP/IP	Veritas Backup Reporter Management Server > Veritas Backup Reporter Management Server host	To share trap	None. Not used across firewall.
2821	TCP/IP	Agent / Java View Builder / CLI tools > Veritas Backup Reporter Management Server  The port should be open on the Symantec Authentication Service (AT) Server host	To authenticate with Veritas Backup Reporter Management Server	Agent will not be able to communicate to server if Agent is on a remote system.
13799	TCP/IP	Veritas Backup Reporter Management Server > Database	<ul style="list-style-type: none"> <li>■ To authenticate with Veritas Backup Reporter Management Server</li> <li>■ To store data collector data, alerts, policy settings</li> </ul>	<ul style="list-style-type: none"> <li>■ Users will not be able to authenticate with Symantec Private Branch Exchange and VBR Management Server; users will be denied the access.</li> <li>■ None. Not used across firewall.</li> </ul>
7806	CORBA over TCP/IP	Veritas Backup Reporter Management Server and CLI tools > Agent  The port should be open on the Agent host	To send status and data requests for frequent updates of the agent	Agent status page will not work, CLI tools for querying agent do not work remotely.

**Table 2-5** Default ports used by Veritas Backup Reporter (*continued*)

Port number	Protocol	Communication Initiator > Recipient	Purpose	Impact if blocked
8181	HTTP over TCP/IP	<ul style="list-style-type: none"> <li>■ Web browser &gt; Veritas Backup Reporter Management Server</li> <li>■ Veritas Backup Reporter Agent &gt; Veritas Backup Reporter Management Server</li> </ul> <p>The port should be open on the Management Server host</p>	<ul style="list-style-type: none"> <li>■ To run Veritas Enterprise Reporter console</li> <li>■ To receive connections from the <code>agentauth</code> command on remote Agents or to authenticate Agent with Management Server</li> </ul>	<ul style="list-style-type: none"> <li>■ Users will not be able to access the console.</li> <li>■ Installation of remote Agents will not be successful as the <code>agentauth</code> command on remote Agents will not be able to connect to the VBR Management Server. Agent will not be able to communicate with the Management Server therefore, data will not be sent to the Management Server.</li> </ul>
8443	HTTPS over TCP/IP	<p>Web browser &gt; Veritas Backup Reporter Management Server</p> <p>The port should be open on the Management Server host</p>	To run Veritas Enterprise Reporter console	Users will not be able to access the console.

---

**Note:** If the default Web server `http` port 8181, is deleted either by manually editing the Web server configuration file or executing the `webgui.exe -delport` CLI, the VBR Agent authentication may fail. 8181 port must be open to establish the communication between VBR Management Server and Agent.

---

Figure 2-1 shows the default port assignments.



data collection. VBR runs a number of NetBackup CLIs (Command-line Interface) to collect data remotely, which require certain ports to be open inbound and outbound (on the Agent host and NetBackup Master Server host) on a firewall.

[Table 2-6](#) lists the ports required to communicate with NetBackup

**Table 2-6** Ports and CLIs required to communicate with NetBackup

Port number	Communication	NetBackup CLI / process
13701	This port should be open on VBR Agent and NetBackup Master/Media server hosts  This is applicable for VBR 6.0 or prior versions	vmglob.exe.exe, vmoprcmd.exe, and vmpool.exe vmquery CLIs are used to run the vmd process on the NetBackup Master Server host
13705 (for TL8 library types)	This port should be open on VBR Agent and NetBackup Master/Media server hosts	vmchange.exe
13711 (for TLD library types)	This port should be open on VBR Agent and NetBackup Master/Media server hosts	vmchange.exe
13721	This port should be open on VBR Agent and NetBackup Master/Media server hosts	bpdbm process on the NetBackup Master Server host
13723 & 13724	13723 port should be used to connect to the NetBackup Master Server and 13724 port should be used to respond to the Agent host. The response is sent on a port in the reserved port range 512-1023 if not configured to use vnetd	bpdbjobs.exe CLI is used to run the bpjobd process on the Agent host and vnetd on the Master Server host
13782 & 13724	13782 port should be used to connect to the NetBackup Master Server and 13724 port should be used to respond to the Agent host. The response is sent on a port in the reserved port range 512-1023 if not configured to use vnetd	bpstulist.exe bperror.exe bpclist.exe bpretlevel.exe bppllist.exe bpimagelist.exe bpmedialist.exe bpgetconfig.exe

## About ports required to communicate with other backup products

This section provides information about the ports that Veritas Backup Reporter uses to communicate with other backup products, such as Backup Exec, Puredisk, TSM, and CommVault.

Table 2-7 lists the ports that VBR data collectors require to collect data from various backup products.

**Table 2-7** Ports required to communicate with other backup product

Backup product	Communication	Port number
Backup Exec	VBR (Backup Exec data collector) communicates with Backup Exec Server using Backup Exec API	6106
PureDisk	VBR (Puredisk data collector) communicates with PureDisk SPA via atssl	443 (HTTPS) 2821 (AT)
TSM	VBR (TSM data collector) communicates with TSM Server using TSM CLI <code>dsmadm</code>	1500
CommVault	VBR (CommVault data collector) communicates with CommVault Server	No specific port is required
Legato Networker	VBR (Legato data collector) communicates with Legato Server locally	This is a local host communication

## Changing the VRTSweb HTTP port

Use the `webgui delport` and `webgui add` commands to delete and add ports. If you need to change the VRTSweb HTTP port on either Windows or Solaris, use the following procedures.

For additional information about the `webgui` command, refer to help provided by running the `webgui help delport` and `webgui help addport` commands.

### To change the VRTSweb HTTP port on Windows

- 1 Before changing the port, confirm that no other service is listening on the port by typing the following command:

```
netstat -an | find "9191"
```

No lines should be returned. The `-an` option is important in case any program has updated the services list.

- 2 Type the following command:

```
cd "c:\Program Files\VERITAS\VRTSweb\bin"
```

- 3 To delete and add the new port number, type the following commands:

```
webgui delport 8181
```

```
webgui addport 9191 HTTP
```

where port 8181 is the original port that you want to change, and port 9191 is whatever new port number you chosen.

### To change the VRTSweb HTTP port on Solaris

- 1 Before changing the port, confirm that no other service is listening on the port by typing the following command:

```
netstat -an | grep 9191
```

No lines should be returned. The `-an` option is important in case any program updated the services list.

- 2 Type the following command:

```
/opt/VRTSweb/bin
```

- 3 To delete and add the new port number, type the following commands:

```
./webgui delport 8181
```

```
./webgui addport 9191 HTTP
```

where port 8181 is the original port that you want to change, and port 9191 is whatever new port number you chose.

## Configuring Veritas Backup Reporter Management Server behind NAT firewall

When a firewall is configured to act as a Network Address Translation (NAT) device to route packets to hidden addresses behind the firewall, you must change the actual public IP address (the NAT address) of the Veritas Backup Reporter Management Server and the Veritas Alert Manager.

**To configure the Veritas Backup Reporter Management Server behind a NAT**

- 1 On the Veritas Backup Reporter Management Server, do one of the following:
  - On Solaris, open a console and log in as root.
  - On Windows, open a Windows command prompt and log in as an administrator or user in the Administrators group.
- 2 Stop the Veritas Backup Reporter Management Server.
  - On Solaris, enter `/opt/VRTSccsvs/bin/vbrserver stop`
  - On Windows, use the Windows Service Control Manager (SCM) and stop the Veritas Backup Reporter Management Server.
- 3 Using a text editor, open the `vbr_conf.properties` present in the following default location:
  - On Solaris, enter `/opt/VRTSccsvs/conf`
  - On Windows, enter `\Program Files\Symantec\Veritas Backup Reporter\Server\conf`
- 4 Using your text editor, search for the following string.  
`corba.external.ip=`  
If the string is not present, add it.
- 5 Enter the actual public IP address (the “natted” address) for the Veritas Backup Reporter Management Server. For example:  
`corba.external.ip=255.255.255.255`
- 6 Save your changes and close the `vbr_conf.properties` file.
- 7 Restart the Veritas Backup Reporter Management Server by doing one of the following:
  - On Solaris, enter `/opt/VRTSccsvs/bin/vbrserver start`
  - On Windows, use the Windows SCM and restart the Veritas Backup Reporter Management Server.

---

**Note:** To enable users to select a domain at logon, Veritas Backup Reporter Management Server hosts running Windows must be configured either in DNS or with a fully qualified domain name.

---

## About AT configuration in Veritas Backup Reporter

This section provides information about Symantec Product Authentication Service (AT) and its configuration in Veritas Backup Reporter.

---

**Note:** VBR does not support clustered AT.

---

### About AT

Veritas Backup Reporter uses AT to handle user authentication.

AT enables product components to communicate securely through secure sockets layer (SSL) technology. It also allows products to verify the identity of other components that communicate with it and end users who need to log on. In order for product components to verify each other's identity and to encrypt their communications, they must belong to the same security hierarchy. A root broker maintains the hierarchy. The hierarchy itself is known as a root broker hierarchy.

The root broker is the ultimate authority that vouches for the certificates that are used for communication. To vouch for a certificate means to sign a certificate. Each root broker can have many authentication brokers. Authentication brokers are helpers that issue the certificate, but the certificate is signed under the authority of the root broker. All certificates that the authentication broker issues can be trusted because the root broker that trusts each of the authentication brokers signs the certificates. To summarize, root brokers create a signature that authentication brokers use to issue certificates.

A best practice is to use a single root broker hierarchy in an enterprise. At a minimum, installations of the same product type should share the same root broker hierarchy. Product components in different root broker hierarchies cannot communicate unless trust relationships are established between the hierarchies. To allow products in different root hierarchies to communicate, you must establish trust relationships between the hierarchies, which results in multiple trust relationships. Multiple trust relationships increase the complexity of your security architecture. It can also require that you perform additional manual configuration steps each time you install a new instance of a Symantec product. You can eliminate the need for multiple trust relationships by:

- Sharing a single root broker in your enterprise
- Sharing a root broker between installations of the same product type

For more details on AT, refer to the documents at the following locations:

- AT Install Guide:<http://support.veritas.com/docs/311442>
- AT Admin Guide:<http://support.veritas.com/docs/311441>

- AT Release Notes: <http://support.veritas.com/docs/311440>

Symantec Product Authentication Service provides common authentication runtime libraries and processes that enable users to log on once to access multiple products.

Veritas Backup Reporter creates a private domain (`cc_users`) during installation. `cc_users` gives you an alternative domain to NIS and NT against which for Veritas Backup Reporter to authenticate users. (Additionally, the domains you see might be local to a particular host.)

Veritas Backup Reporter also uses several other private domains to allow various Management Server and Agent components to communicate with each other. These accounts correspond to processes and daemons and not to physical users. Various Symantec products use the private domains to interact with Symantec Product Authentication Service.

To get a list of private domains known to the Symantec Product Authentication Service, type the following command (depending on your operating system) on a Veritas Backup Reporter Management Server:

```
Solaris          /opt/VRTSat/bin/vssat showallbrokerdomains
Windows         \Program
                Files\VERITAS\Security\Authentication\bin\vssat
                showallbrokerdomains
```

To find more information about `vssat`, the Symantec Product Authentication Service command-line interface, type the following command at the command prompt:

```
vssat --help (for the list of arguments)
```

or

```
vssat command --help (for help on an individual argument).
```

## About AT configuration scenarios in Veritas Backup Reporter

You can configure AT on the VBR Management Server while fresh installation or upgrade, or modify it manually after the installation.

See “[Modifying AT configuration manually](#)” on page 143.

In PureDisk setup, you may want to move the AT Root Broker from PureDisk SPA host to the Management Server host, or vice versa.

If you want to collect data from PureDisk SPA host, review the PureDisk data collection section in addition to this section.

See “[Collecting data from PureDisk](#)” on page 223.

In Veritas Backup Reporter, you can configure AT - Root Broker (Root) and Authentication Broker (AB) - in a number of ways as per your requirements, during fresh installation or upgrade. Review this information while configuring AT during installation / upgrade.

The possible AT scenarios are described as follows:

Fresh installation of Veritas Backup Reporter 6.6	<p>You can configure AT in one of the following ways during fresh installation of VBR:</p> <ul style="list-style-type: none"><li>■ Root + AB on Veritas Backup Reporter Management Server host (local Root)</li><li>■ AB on VBR Management Server host and Root on a remote host (remote root)</li></ul>
Fresh installation of Veritas Backup Reporter 6.6 on AT host	<p>During the fresh installation of VBR on the AT host, you can configure AT in one of the following ways, depending on the existing AT configuration:</p> <ul style="list-style-type: none"><li>■ Retain the existing Root + AB configuration for Veritas Backup Reporter 6.6</li><li>■ Configure AB on the existing Root Broker host (Root &gt; Root + AB)</li><li>■ Configure Root Broker with the existing AB (AB &gt; Root + AB)</li><li>■ Retain the existing AB configuration with the existing remote Root</li><li>■ Retain the existing AB configuration with the new remote Root</li></ul>
Upgrade to Veritas Backup Reporter 6.6	<p>During the VBR upgrade, you can configure AT in one of the following ways, depending on the existing AT configuration:</p> <ul style="list-style-type: none"><li>■ Retain the existing Root + AB configuration from previous Veritas Backup Reporter version</li><li>■ Downgrade from Root + AB to AB and retain the AB configuration in Veritas Backup Reporter 6.6 using the existing remote Root</li><li>■ Downgrade from Root + AB to AB and retain the AB configuration in Veritas Backup Reporter 6.6 and point to a new remote Root</li></ul>
Clustering VBR 6.6 Management Server	<p>Configure AB on a remote AT host</p>

## Creating principal user on root broker

This section provides the detailed steps to create a principal user on the external / remote root broker host, which you want to use for Veritas Backup Reporter. You need to specify the credentials of this principal user while configuring AT in VBR, while installing / upgrading or manually modifying the AT configuration.

### To create principal user on root broker

- 1 Logon to a remote root broker machine as an administrator or a super user.
- 2 Find the root domain name of that machine by running the following command: `vssat listpd --pdrtype root`

For example, the root domain name is `root@<root IP/host name>`, where `<root IP/host name>` is referred to as root node or root broker host.

- 3 Create the authentication broker identity in the root domain with the following command: `vssat addprpl --prplname <broker identity name, for example Management Server host name>--password <broker identity password>--pdrtype root --domain <root domain name provided by running vssat listpd --pdrtype root command>--prpltype service`

The name of the root broker hash file is `root_hash`. It resides on the following location: `<AT Install location>/Authentication/bin`

- 4 Copy the root hash file to the authentication broker machine. The root hash file is a binary data. Therefore, you must copy the root hash file in the binary mode. The destination directory can be any directory on the target authentication broker machine.
- 5 Before starting the agent module configuration, find out the broker host name by executing the following command:

Windows	<code>&lt;INSTALL_DIR&gt;\VERITAS\Security\Authentication\bin\vssat showcred</code>
Solaris	<code>/&lt;INSTALL_DIR&gt;/VRTSat/bin/vssat showcred</code>

## Verifying the authentication mode for Symantec Product Authentication Service

This section provides the procedure to verify the authentication mode of Symantec Product Authentication Service AT.

### To verify the authentication mode for Symantec Product Authentication Service on Solaris

- 1 Determine if Symantec Product Authentication Service is installed on the host by running the following command:

```
pkginfo | grep VRTSat
```

- 2 Change your directory to the installation directory as follows:

```
cd /opt/VRTSat/bin/
```

- 3 If Symantec Product Authentication Service is installed, at a command prompt, enter the following:

```
./vssat showbrokermode
```

The command returns an integer value in the range of 0 to 3.

The `vssat` command can be used to verify the following:

- Appropriate trust relationship was established
- Private domains were created for the product
- Authentication principles have been created for the product

Mode 0: The broker is not configured

Mode 1: The broker is running in AB mode

Mode 2: The broker is running in Root Only mode.

Mode 3: The broker is running in Root + AB mode

### To modify the authentication mode for Symantec Product Authentication Service on Solaris

- 1 Stop the `vxatd` process by entering the following:

```
vxatd stop
```

- 2 Change your directory to the installation directory by entering the following:

```
cd /opt/VRTSat/bin
```

- 3 Run the following command to change the Symantec Product Authentication Service mode:

```
vxatd -o -a -r
```

- 4 Start the `vxatd` process by entering the following:

```
vxatd start
```

### To verify the authentication mode for Symantec Product Authentication Service on Windows

- 1 Determine if Symantec Product Authentication Service is installed on a Windows host by checking the Windows Services.
- 2 Change your directory to the installation directory by entering the following:

```
cd \Program Files\Veritas\Security\Authentication\bin
```

- 3 At the command prompt, enter the following:

```
vssat showbrokermode
```

The command returns an integer value in the range of 0 to 3.

```
Mode 0: The broker is not configured
```

```
Mode 1: The broker is running in AB mode
```

```
Mode 2: The broker is running in Root Only mode
```

```
Mode 3: The broker is running in Root + AB mode
```

### To modify the authentication mode for Symantec Product Authentication Service on Windows

- 1 Using the Windows services console, stop the Symantec Product Authentication Service.
- 2 Change your directory to the installation directory as follows:  

```
cd \Program Files\Veritas\Security\Authentication\bin
```
- 3 Run the following command to change the Symantec Product Authentication Service mode:  

```
vxatd -o -a -r
```
- 4 Using the Windows Services console, restart the Symantec Product Authentication Service.

## Installing Veritas Backup Reporter on Solaris and Windows

This section describes the procedures for fresh installation of Veritas Backup Reporter on Solaris and Windows hosts.

See [“Upgrading Veritas Backup Reporter”](#) on page 76.

You can install VBR in clustered mode.

See [“Clustering Veritas Backup Reporter”](#) on page 86.

**Table 2-8** provides steps to install Veritas Backup Reporter components. You can use this as a checklist while installing VBR.

**Table 2-8** Steps to install / upgrade / cluster Veritas Backup Reporter

Step number	Step	Reference topic
1	<p>Review the prerequisite and other hardware / software requirements for VBR Management Server and Agent hosts, carefully.</p> <p>Make sure that you satisfy the operating system requirements.</p> <p>Go through the AT configuration section to decide what is to be your AT configuration, whether the VBR Management host should be a Root Broker + AB or only AB.</p> <p>Go through the firewall settings and port number information.</p> <p>Go through the Agent deployment section.</p>	<p>See <a href="#">“Planning your Veritas Backup Reporter installation”</a> on page 35.</p>
2	<p>Go through the appropriate installation section. The installation steps vary depending on your requirement and operating system you have. There are different sections for fresh installation, upgrade, and clustering steps.</p> <p>For Push Installation steps on Windows, there is a separate section.</p> <p><b>Note:</b> After installation, verify if VBR is running properly.</p> <p>See <a href="#">“Installing Veritas Backup Reporter on Solaris”</a> on page 60.</p>	<p>See <a href="#">“Installing Veritas Backup Reporter on Windows”</a> on page 65.</p> <p>See <a href="#">“Upgrading Veritas Backup Reporter”</a> on page 76.</p> <p>See <a href="#">“Clustering Veritas Backup Reporter”</a> on page 86.</p> <p>See <a href="#">“About VBR push installation on Windows”</a> on page 71.</p>

## Installing Veritas Backup Reporter on Solaris

This section provides you with the procedure to install Veritas Backup Reporter on Solaris host.

See [“Upgrading to Veritas Backup Reporter 6.6 on Solaris”](#) on page 79.

See [“Clustering Veritas Backup Reporter on Solaris”](#) on page 100.

Use the Veritas Backup Reporter Install Script, which resides in the root directory in the product DVD, to install Veritas Backup Reporter on a Solaris host.

### To install Veritas Backup Reporter components on Solaris

- 1 Open a UNIX console and log in as `root` on the target host.
- 2 Mount the appropriate Veritas Backup Reporter 6.6 product DVD for the components you are installing.
- 3 Type the following command and press **Enter**:

```
./installvbr
```

The Install Script displays a list of Veritas Backup Reporter components available for installation.

If any components are already installed, the script lists those separately.

- 4 To add the component to the install queue, type its corresponding menu number and press **Enter**.

The label [INSTALL] appears next to each selected component to indicate that it is in the install queue.

Repeat this step for each component you want to install.

- 5 To remove a selected component from the install queue, type the component's menu number again and press **Enter**.
- 6 After adding components to the queue, type the menu number that corresponds to the Finished with selections option and press **Enter**.
- 7 Review the list of components in the install queue.
- 8 Type `y` and press **Enter** to confirm the selection and continue.
- 9 Type `n` and press **Enter** to return to the component list and revise your selection.

The next series of prompts collects configuration information for the components in the install queue.

The steps you need to complete may vary depending on which components you plan to install.

### To configure components in the install queue

- 1 Type a directory path under which to install the components and press **Enter**.
- 2 To accept the default path (`/opt`), press **Enter** without typing a directory path.

The remaining configuration steps may vary depending on which components you are installing.

- 3 If you are installing the Veritas Backup Reporter Management Server, do the following:

- Type a directory path under which to install the Veritas Backup Reporter database and press **Enter**.

The Veritas Backup Reporter database server may require up to 1 GB of temporary space at runtime. By default, temporary files will be created in the database installation directory, `/var/Veritas/ccs_data`.

To accept the default path (`/var/Veritas/ccs_data`), press **Enter** without typing a directory path.

If you specify an alternate database directory, the script creates the folder `ccs_data` below your directory.

This part of the directory path is fixed.

- Type the network address (fully qualified domain name or IP address) to which users should point their browsers to connect to the Web Engine, and then press **Enter**.

Please specify a network address for the Veritas Backup Reporter server and Web Engine. Do not use 'localhost'. This should be a fully qualified domain name or an IP address that other machines can use: `installsystem.subdomain.Veritas.com`

- Press **Enter** to accept the default port (8181) for connections to the Web Engine, or type an alternate port number, and then press **Enter**.

Please enter a port for the Symantec Web Server, or  
<Return> to accept the default port: (8181)

- Type the name or IP address of an SMTP server host to use for emailing reports and press **Enter**.

Enter the name or IP address of an SMTP server to  
use for emailing reports: (localhost) smtp.Veritas.com

#### 4 Select any of the following options to configure AT:

```
If you have an existing VxAT setup in your environment
then you can configure VBR VxAT to point to an existing root broker.
Do you want to configure VBR VxAT to point to an existing root broker?
[y,n,q] (n)
```

---

**Note:** If you are upgrading to Veritas Backup Reporter 6.6 you can choose to retain the existing AT configuration.

---

Before configuring AT, refer to the following section:

[About AT configuration in Veritas Backup Reporter](#)

- Select **n** if you want to configure Symantec Product Authentication Service (AT) server on the Veritas Backup Reporter Management Server host. The VBR Management Server host works in the Root + Authentication Broker mode.  
In this case, you do not need to enter AT server (root) host details, such as root host or root port, as these details are same as of the Management Server host.

- Enter **y** to point to the existing root broker and specify the following information.

- Root broker machine name
- Remote user name
- Domain name
- Password of the above user
- Root hash code or root hash file name as follows:

Do you want to enter Root hash directly.

No option will ask you the root hash file location [y,n,q] (y)

Enter **y** to enter root hash code.

Enter **n** to enter root hash file name

- 5 If you are installing the VBR Agent, choose whether to configure the Agent to report to a Veritas Backup Reporter Management Server host at this time by doing the following:

- Type **y** and press **Enter**.
- Type the name of the Veritas Backup Reporter Management Server host for example *VBHost.abc.com* and press **Enter**. Otherwise, type **n** and press **Enter**.

The host on which you are installing the VBR Agent must have network access to the VBR Management Server host you specify. It is best to specify the VBR Management Server host using its fully qualified domain name or IP address.

- 6 Specify the directory path where the spooler data is stored. The default location is: `/var/VERITAS/ccs_data/spooler`

---

**Note:** The spooler resides on the Agent host and can hold the backup data up to its maximum memory usage. The spooler data then sequentially transfers to the Veritas Backup Reporter Management Server.

---

- 7 Review the installation options you selected.
- 8 Type **y** and press **Enter** to confirm the selection and continue.  
Type **n** and press **Enter** to repeat the configuration steps and revise your selection.

9 Enter the installation directory. Default directory is: `/opt`

10 Enter the database dir: `/var/VERITAS/ccs_data` and DB temp dir:  
`/var/VERITAS/ccs_data`

11 Enter DB Port: 13799

The Veritas Backup Reporter Agent will report to: *VBHost.abc.com*. The Veritas Backup Reporter Server external address has been set to: *VBHost.abc.com*

Veritas Web Server port is set to: 8181

SMTP server for emailing reports is set to the specified host.

Spooler directory for this agent: `/var/VERITAS/ccs_data/spooler`

12 Is the above configuration correct? [y,n,q]

Type **y**.

The next series of prompts enable you to confirm your selections and to continue the installation after the script performs its pre-installation checks. After the script finishes installing the queued components, it prompts you to start Veritas Backup Reporter components.

#### To complete Veritas Backup Reporter component installation

- 1 After the initial system check completes, press **Enter** to continue.
- 2 Review the list of packages to be installed and press **Enter** to continue.  
The Install Script checks the system for Veritas Backup Reporter components, dependencies, and required patches. If a required patch is not found on the system, the script displays a list of the missing patches and a prompt asking whether you want to continue the installation. It is recommended that you cancel the installation and install the patches before you install Veritas Backup Reporter components.
- 3 After the installation requirements check succeeds, press **Enter** to continue.  
The Install Script installs the Veritas Backup Reporter component packages.
- 4 After all the packages are installed, press **Enter** to continue.  
If the installed components require manual configuration, the Install Script displays information on how to perform the configuration.

- 5 Press **Enter** to continue.

The Install Script performs any automatic configuration that the installed components require.

- 6 Press **Enter** to continue.

- 7 Do one of the following:

- Type **y** and press **Enter** to start Veritas Backup Reporter processes.  
In VBR 6.6 the installer creates and registers a new database server service called `dbsrv10`. VBR 6.6 uses Sybase SA 10 to store data. In all previous VBR versions, Sybase SA 9 was used.  
Along with the new database service, VBR 6.6 creates a new database engine called `VBR_ VBRhostname`  
*VBRhostname* is the name of the host where VBR Management Server is installed.

---

**Note:** The new VBR database location on Solaris: `/opt/vbrdbms`

---

- Type **n** and press **Enter** if you want to manually start the processes later.  
The Install Script displays a summary of the installation, including the location of the installation log files.

## Installing Veritas Backup Reporter on Windows

Use the Install Wizard to install Veritas Backup Reporter on a Windows host. The wizard resides at the top level of the Veritas Backup Reporter 6.6 product DVD.

---

**Note:** If you do not have version 1.1 or later of the Windows Installer on your Windows host, Veritas Backup Reporter components do not install properly.

---

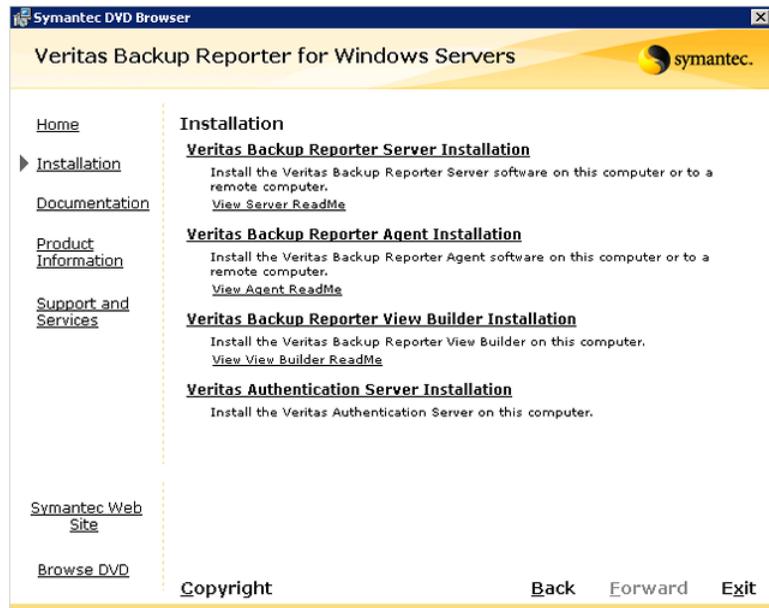
### To install the Windows installer

- 1 Exit the wizard now and install the Windows Installer.
- 2 If the Windows Installer is already installed, test its integrity by starting and stopping it from the Windows Services console.

The Windows Installer is available for download from the Microsoft Web site: <http://msdn.microsoft.com/downloads/>

### To install VBR Management Server on Windows

- 1 On a Windows host where you want to install VBR Management Server, insert the appropriate Veritas Backup Reporter 6.6 product DVD in the CD-ROM drive.
- 2
  - If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.
  - If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type '`D:\Browser.exe`' and press Enter:  
Where *D* is the CD-ROM drive.  
The Veritas Backup Reporter Installation Wizard appears as shown in the following figure.
- 3 On the Veritas Backup Reporter Installation Wizard, click the Installation link. The following screen is displayed.



- 4 Click the Veritas Backup Reporter Server Installation link to install VBR Management Server.
- 5 Read the license agreement, click 'I accept the terms of the license agreement' and click **Next**.

**6** Click any of the following options depending on your requirements:

**Install to this computer only** Select this option to install VBR Management Server on this host.

**Install to a remote computer on your network (push installation)** Select this option to install VBR Management Server using the push installation mechanism. VBR Management Server is installed on all specified computers in the network.

See [“About VBR push installation on Windows”](#) on page 71.

This option is disabled if you are running VBR 6.6 upgrade.

**Install a clustered Veritas Backup Reporter Server** Select this option to install VBR Management Server on all selected nodes, in a clustered mode.

See [“Clustering Veritas Backup Reporter on Windows”](#) on page 88.

This option is enabled if you have Veritas Cluster Server (VCS) installed.

Click **install to this computer only**.

**7** Click **Typical** to use the default settings, location, or port numbers.

---

**Note:** Click **Custom** if you want to change the default settings, locations, or port numbers.

---

Click **Next**.

**8** On the Add License Keys screen, enter your demo or permanent key that you have received with the purchase of the VBR application and click **Add**.

The license key is added to the following location: C:\Program Files\Common Files\VERITAS Shared\vrtslic\lic

**9** Click **Next**. The Authentication Settings screen is displayed.

- 10** Before configuring Symantec Authentication Service (AT), refer to the following:

[About AT configuration in Veritas Backup Reporter](#)

---

**Note:** If you are upgrading to Veritas Backup Reporter 6.6 you have an additional option to select that is Existing Configuration. Select this option to retain the existing AT configuration.

---

For fresh VBR installation, select any of the following:

**Local Root Broker** Select this option if you want to configure Symantec Product Authentication Service (AT) server on the Veritas Backup Reporter Management Server host. The VBR Management Server host works in the Root+Authentication Broker mode.

In this case, you do not need to enter AT server (root) host details, such as root host or root port, as these details are same as of the management server host.

**Remote Root Broker** Select this option if you want to configure AT Authentication Broker on the Veritas Backup Reporter Management Server host and you want to point to the AT root that is present on a different host. The management server host works in the Authentication Broker mode.

Configure the management server host for the AT root by entering the following details:

Root Host - Enter the AT root host name

Root Port - Enter the AT port number

Identity - Enter the principal user name

Password - Enter the password of the principal user account

Domain - Enter the root domain name of the AT root host.

Root Hash - Enter the root hash file name or root hash code that you have copied from the AT root. Click **Browse** to select the root hash file.

Select this check box to use root hash code instead of the root hash file.

---

**Note:** If you want to use a remote AT host, you should have this principal user created on the AT host.

You can install AT on this computer using the same VBR installer. Select the Veritas Authentication Service Installation option on the installer.

---

- 11 Click **Next**. The installer shows the summary of the settings that you have selected for installation.

- 12 Click **Install**.

The installer starts installation of VBR Management Server.

In VBR 6.6 the installer creates and registers a new database server service called `Veritas Backup Reporter Database Service`. VBR 6.6 uses Sybase SA 10 to store data. In all previous VBR versions, Sybase SA 9 was used.

Along with the new database service, VBR 6.6 creates a new database engine called `VBR_ VBRhostname`

`VBRhostname` is the name of the host where VBR Management Server is installed.

---

**Note:** The new VBR database location on Windows:

C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer

Registry key:

HKEY\_LOCAL\_MACHINE\Software\Symantec\Veritas Backup Reporter\Data\DbPath

---

- 13 After successful installation, you can view installation logs or open the README file.

- 14 Click **Finish**.

Follow this procedure to install VBR Agent.

#### To install VBR Agent

- 1 You can install the VBR Agent either on the Management Server host, product host, or a separate host. To decide where you want to install the VBR Agent, review the information on Agent deployments.

See [“About Veritas Backup Reporter Agent deployment”](#) on page 42.

On a Windows host where you want to install VBR Agent, insert the appropriate Veritas Backup Reporter 6.6 product DVD in the CD-ROM drive.

- 2 ■ If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.

- If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type '`D:\Browser.exe`' and press Enter:  
Where *D* is the CD-ROM drive.  
The Veritas Backup Reporter Installation Wizard appears.
- 3 On the Veritas Backup Reporter Installation Wizard, click the Installation link.
- 4 Click the Veritas Backup Reporter Agent Installation link to install VBR Agent.
- 5 Read the license agreement, click 'I accept the terms of the license agreement' and click **Next**.
- 6 Click **install to this computer only**.
- 7 Click **Typical** to use the default settings, location, or port numbers.

---

**Note:** Click **Custom** if you want to change the default settings, locations, or port numbers.

---

- 8 On the Agent Settings screen, enter the following information:

Host	Enter the host name where VBR Management Server is installed.
Location for Agent spooler data	Select the location to store the Agent spooler data. The spooler resides on the Agent host and can hold the backup data up to its maximum memory usage. The spooler data then sequentially transfers to the Veritas Backup Reporter Management Server.  The default directory for the spooler is: <code>C:\Program Files\Symantec\Veritas Backup Reporter\Agent\Data</code>

You can change the default location for storing spooler data and Agent logs, by clicking respective Browse buttons.

- 9 Click **Next**. The installer shows the summary of the settings that you have selected for Agent installation.
- 10 Click **Install**.  
The installer starts installation of VBR Agent.
- 11 After successful installation, you can view Agent installation logs or open the README file.
- 12 Click **Finish**.

Use the following procedure to install Java View Builder.

#### To install Java View Builder

- 1 On the VBR Management Server host, insert the appropriate Veritas Backup Reporter 6.6 product DVD in the CD-ROM drive.
- 2
  - If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.
  - If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type '`D:\Browser.exe`' and press Enter:  
Where *D* is the CD-ROM drive.  
The Veritas Backup Reporter Installation Wizard appears.
- 3 On the Veritas Backup Reporter Installation Wizard, click the Installation link.
- 4 Click the Veritas Backup Reporter View Builder Installation link to install VBR Java View Builder.
- 5 Read the license agreement, click 'I accept the terms of the license agreement' and click **Next**.
- 6 On the View Builder Features list, click **Change** if you want to change the default location for Java View Builder installation.
- 7 Select a new location and click **Next**.
- 8 The installer shows the summary of the settings that you have selected for Java View Builder installation.
- 9 Click **Install**.  
The installer starts installation of VBR Java View Builder.
- 10 After successful installation, you can view Java View Builder installation logs or open the README file.
- 11 Click **Finish**.

#### About VBR push installation on Windows

You can now install VBR Management Server and Agent using the push installation method. Using this mechanism you can install these VBR components on multiple hosts at one go.

Push installation is available only in case of fresh VBR installation, clustered or non-clustered mode. This option is disabled if you are upgrading to VBR 6.6.

If you are installing VBR in a clustered mode, you do not need to select the push installation method. The installer internally enables this option and you are

prompted to select multiple cluster nodes, where you want to install VBR from the active node.

If you have selected the 'Install to a remote computer on your network' option on the Windows installer, you can select multiple hosts in that network where you can install VBR components. You can specify to have the same installation location for all hosts. The rest of the installation steps are the same as described in the fresh installation or clustering sections.

In VBR 6.6, push installation is supported only for Windows 2003 32-bit platform.

## Resolving agent authentication failures manually on Solaris and Windows

If the Veritas Backup Reporter Agent authentication fails on Solaris or Windows, use the following procedures to manually resolving agent authentication failures.

If the Veritas Backup Reporter Agent is cannot connect to the Veritas Backup Reporter Management Server, a message such as the following may appear in the logs:

```
Authentication failed
The user or password are not valid in the given domain.
Domain = cc_users@myServer
User = admin
```

### To manually resolve agent authentication failures on a Solaris system

- ◆ Run the following command:

```
/opt/VRTSccsva/bin/agentauth -server <serverHostName>
```

### To manually resolve agent authentication failures on a Windows system

- 1 Log on to the Veritas Backup Reporter Management Server host with administrator-level privileges.
- 2 Stop the agent service using the Windows Services console (**Start > Settings > Control Panel > Administrative Tools > Services**).
- 3 Open a Windows command prompt and change to the following agent default installation directory:

```
\Program Files\Symantec\Veritas Backup Reporter\Agent\bin
```

- 4 Type the following command and press **Enter**:

```
agentauth.exe -server <serverHostName>
```

If the `agentauth.exe -server <serverHostName>` command fails, verify that the management server is online and accessible and check if the agent time lags behind the management server time.

The `agentauth.exe` command can fail for a number of reasons.

Two of the most common reasons for the `agentauth.exe` command to fail are as follows:

- The Security Dynamic Link Libraries (DLLs) are not in the PATH.  
The workaround for this is to run the following commands:
  - `cd \Program Files\Veritas\Security\Authentication\bin`
  - `"\Program Files\Symantec\Veritas Backup Reporter\Agent\bin\agentauth.exe" -server <serverHostName>`
- The management server cannot be contacted.  
Ensure that the Veritas Backup Reporter Management Server and Authentication Service are running and can be reached on ports 1556 and 2821, respectively.  
`agentauth`

- 5 Restart the agent service.

## Verifying that Veritas Backup Reporter is running properly

After installing Veritas Backup Reporter on either UNIX or Windows, perform a check to verify that Veritas Backup Reporter is running properly.

### To verify that Veritas Backup Reporter is running properly

- 1 Go to **`http://<server-host>: 8181`**.

If the Veritas Backup Reporter Login screen appears, the Veritas Backup Reporter Management Server, the Web server, and the Authentication Service are running.

The first time you login it, takes longer than usual time for the GUI to load.

- 2 Login using `admin (username) /password (password)` on the private domain:  
**`cc_users@<server name>`**
- 3 Verify that the agents and data collectors are set up correctly.
  - Go to **Settings > Global Settings > Agent Configuration**.  
The Veritas Backup Reporter Agent should appear.  
If an agent does not appear, do not click Create. Instead, troubleshoot the problem by checking that you correctly configured the ports.

## Uninstalling Veritas Backup Reporter on Solaris and Windows

This section describes uninstallation procedures for Veritas Backup Reporter on Solaris and Windows.

### Uninstalling Veritas Backup Reporter on Solaris

Use the Uninstall Script, which resides in the root directory in the product CD, to uninstall Veritas Backup Reporter on a Solaris host.

#### To uninstall Veritas Backup Reporter components on Solaris

- 1 Open a Solaris console and log in as `root` on the target host.
- 2 Change to the following directory:

```
/opt/VRTS/install
```

- 3 Type the following command and press **Enter**:

```
./uninstallvbr
```

The Uninstall Script lists all components installed on the system.

- 4 To add a component to the uninstall queue, type the number of the component and press **Enter**.

The label [UNINSTALL] appears next to the component to indicate that it is in the uninstall queue.

Repeat this step for each component you want to uninstall.

- 5 To uninstall all the components, type the number that corresponds to the Select All option and press **Enter**.
- 6 To remove a selected component from the uninstall queue, type the component's number again and press **Enter**.
- 7 When you finish adding components to the queue, type the number that corresponds to the Finished with selections option and press **Enter**.
- 8 Review the list of components in the uninstall queue.
- 9 Type `y` and press **Enter** to confirm the selection and continue.
- 10 Type `n` and press **Enter** to return to the component list and revise your selection.
- 11 If you are uninstalling the Veritas Backup Reporter Management Server, do the following:
  - Choose the data files you want to back up before uninstalling the Veritas Backup Reporter Management Server.

- To add a file type to the backup queue, type its corresponding menu number and press **Enter**.  
The label [BACKUP] appears next to the file type to indicate that it is in the backup queue.  
Data files are backed up to the directory `/var/Veritas/ccs_save`.
  - When you finish adding files to the backup queue, type the number that corresponds to the Finished with selections option and press **Enter**.
  - Review the backup options you selected.
  - Type **y** and press **Enter** to confirm the selection and continue.
  - Type **n** and press **Enter** to repeat the backup steps and revise your selection.  
The Uninstall Script backs up files in the backup queue.  
If you are backing up a large database, this may take a significant amount of time.
- 12** After the system uninstall requirements check succeeds, press **Enter** to continue.
- The Uninstall Script stops all processes and then uninstalls the component packages. When the uninstall is complete, it displays a summary of the uninstall, including the location of the uninstall log files.
- 13** Do one of the following:
- Type **y** and press **Enter** to start the uninstall process.
  - Type **n** and press **Enter** to cancel the uninstall procedure.

## Uninstalling Veritas Backup Reporter on Windows

Use the Windows Add/Remove Programs utility to uninstall Veritas Backup Reporter on a Windows host.

If you also have CommandCentral Storage components installed on the same host, and you do not want to remove them at the same time, use the Veritas Backup Reporter 6.6 product CD (original media) to remove Veritas Backup Reporter. This leaves CommandCentral Storage installed on the host.

### To uninstall Veritas Backup Reporter on Windows

- 1** Log on to the target host as a user with administrator privileges.
- 2** In the Windows Control Panel, click **Add/Remove Programs**.
- 3** Click **Veritas Backup Reporter** and click **Remove**.
- 4** In the Welcome panel of the Uninstallation Wizard, click **Next** to continue.

- 5 Review the list of components to be uninstalled.
- 6 Click **Next** to continue.
- 7 Clear the check boxes to uninstall Veritas Backup Reporter without saving its database and configuration files.  
The default is to save the database and configuration files.
- 8 Click **Change** to change the location where the database and configuration files are saved.
- 9 Click **Next** to begin uninstalling Veritas Backup Reporter components.  
When you see the Veritas Backup Reporter Uninstallation Wizard closing panel, you are finished uninstalling Veritas Backup Reporter components.
- 10 Click **Finish** to close the Veritas Backup Reporter Uninstallation Wizard.

## Upgrading Veritas Backup Reporter

This section describes procedures to upgrade to Veritas Backup reporter 6.6, on Solaris and Windows hosts.

See “[About supported upgrade paths](#)” on page 40.

---

**Note:** Veritas Backup Reporter 6.6 does not support automatic Veritas Backup Reporter Agents upgrade. When you upgrade your Veritas Backup Reporter Management Server to 6.6, you must also upgrade Veritas Backup Reporter Agents to 6.6.

---

Use the following check list prior to VBR 6.6 upgrade.

- Review the upgrade prerequisites.
- Read the database upgrade section carefully.
- Upgrade VBR components.

### About database upgrade in VBR 6.6

VBR now uses Sybase SA (SQL Anywhere) 10 to store the data, as against Sybase SA 9 in the previous versions.

Sybase updated the SA product to version 10.0. Because of this updated support, VBR updated its database from SA 9 to SA10.

VBR supports upgrade from earlier versions to VBR 6.6, by introducing the database consistency checker (DB checker) utility that runs during upgrade and ensures the consistency between SA 9 and SA 10 schemas.

During VBR upgrade, the existing VBR database should be converted to the new SA 10 format. Note the following points in case of VBR 6.6 upgrade:

- No support for Solaris 7 or any 32-bit Solaris platforms
- New port number 13799 should be used for database server communication
- The installer creates and registers a new database server service called `dbsrv10` On Solaris and `Veritas Backup Reporter Database Service` on Windows.

During VBR 6.6 upgrade, the database is upgraded to SA 10 by the `dbupgrade` utility. The consistency between the existing database schema and SA 10 schema is ensured by the DB checker utility.

The DB checker utility performs the following tasks:

- Checks if the existing database schema is consistent with the VBR 6.6 database schema.  
If the existing schema is inconsistent with the SA 10 format, it displays an alert message, specifying the modifications in the existing database that you have made in terms of customization to the stored procedures, tables, or custom SQL queries. The changes are highlighted in the `vbr-validator.log` and you cannot proceed with the database upgrade.
- Takes the backup of the original (or in other words, existing) database
- Extracts and stores custom SQL, stored procedures, VxAM data
- Deletes the VxAM, CCStorage, DRU, CCMM tables
- After the successful database upgrade to VBR 6.6 version, the stored procedures, or custom SQLs that the DB checker utility had stored will be imported to the upgraded database.

---

**Note:** After the database upgrade, only alert policies and alert recipients are retained. Alerts are not retained.

---

This completes the database upgrade.

Along with the validator logs, review the upgrade logs to ensure that VBR has been upgraded properly.

Review these logs:

Solaris	<p><i>InstallPath</i>/sunos/vbr_dbvalidator/vbr-validator.log</p> <p><i>InstallPath</i>/sunos/ccsvc-dbupgrade0.log</p> <p><b>Note:</b> On a Solaris platform, if you are installing VBR from the product DVD, you can verify the installer logs at the location which is displayed after the installation exits.</p>
Windows	<p>c:\documents and settings\administrator\local settings\temp\1\vbr_dbvalidator\vbr-validator.log</p> <p><i>InstallPath</i>\Symantec\Veritas Backup Reporter\Server\Util\ccsvc-dbupgrade0.log (this is the data migration log)</p> <p>C:\Documents and Settings\All Users\Application Data\Symantec\Veritas Backup Reporter\DB\ccsvc-dbupgrade0.log (this is the actual upgrade log)</p>

After the upgrade, the Veritas Backup Reporter configuration files and database are backed up in the following default directories:

---

**Note:** Rollback of VBR 6.6 installation is only supported on a Windows platform, in which the existing database is restored in the default location of the previous VBR version. After the rollback, you can re-install VBR 6.6.

Solaris does not support rollback mechanism. Therefore, you have to manually uninstall VBR 6.6, re-install it, and copy the saved database at the desired location.

---

Solaris	<p>The database is backed up at the <code>/var/VERITAS/ccs_save</code> location if the default path is selected for saving the database.</p> <p>The configuration files are saved at the following location after successful upgrade: <code>/var/Veritas/ccs_save</code></p>
Windows	<p>Original database is stored in the default location: <code>C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer</code>.</p> <p>Backup of the original database is saved at the location specified by the user during the upgrade process.</p> <p>The SA 10 configuration files - <code>databases.conf</code> and <code>server.conf</code> are located in the <code>C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer\conf</code> directory.</p>

## Upgrade prerequisite

This section lists the prerequisites for VBR 6.6 upgrade.

- Ensure that the disk space you have is twice the existing database size. This is because during the upgrade process, two copies of the existing database are stored on the disk. If upgrade fails, one copy is used for rollback and the other copy is used to perform upgrade on.

---

**Note:** If all VBR components are in the same location, you need 3.5x disk space or 1.5x of database size, where x is the current disk space or existing database size.

---

## Upgrading to Veritas Backup Reporter 6.6 on Solaris

On Solaris, the VBR 6.6 installer script detects the presence of previous version and guides you through the upgrade to 6.6.

### To upgrade to Veritas Backup Reporter 6.6 on Solaris

- 1 Open a UNIX console and log in as `root` on the target host.
- 2 Mount the appropriate Veritas Backup Reporter 6.6 product DVD for the components you want to upgrade.
- 3 Type the following command and press **Enter**:

```
./installvbr
```

The Veritas Backup Reporter Install Script detects if the previous VBR version is present and prompts you to confirm your choice to upgrade.

- 4 Type `y` and press **Enter**.

Veritas Backup Reporter installation files are backed up in the following default directory:

```
/var/Veritas/ccs_save
```

- 5 At this point the DB checker utility is run and it stores the existing database at the specified location. The available disk space is also checked and appropriate message is displayed.

The DB checker utility prepares the database for upgrade.

- 6 You can create a backup directory other than the default (/var/Veritas/ccs\_save) by creating a symbolic link that the Veritas Backup Reporter installer can access by typing the following commands:

```
mkdir /<path with plenty of space>/ccs_save
```

```
ln -s /<path with plenty of space>/ccs_save /var/Veritas/ccs_save
```

The /var/Veritas/ccs\_save directory may already exist from a previous upgrade.

If the /var/Veritas/ccs\_save directory already exists, move the directory by typing the following commands:

```
mv /var/Veritas/ccs_save /<path with plenty of space>
```

```
ln -s /<path with plenty of space>/ccs_save /var/Veritas/ccs_save
```

The Install Script stops Veritas Backup Reporter processes, backs up files from the previous installation, and uninstalls the previous components that you selected to upgrade.

After completing the backup and uninstall, the Install Script displays a list of Veritas Backup Reporter 6.6 components available for installation.

The label [UPGRADE] displays next to a component you are upgrading to indicate that the component is already in the install queue.

- 7 Type the number that corresponds to the **Finished with selections** option and press **Enter**.
- 8 Review the list of components in the upgrade queue.
- 9 Type **y** and press **Enter** to confirm the selection and continue.
- 10 Type **n** and press **Enter** to return to the component list and revise your selection.
- 11 After making your upgrade selections, the Install Script guides you through the same steps you follow to configure and complete a new Veritas Backup Reporter 6.6 component installation.

If you want to collect archive or Enterprise Vault data, you need to add a new license key that is valid for archive data collection, during upgrade.

Refer to the following procedures to configure and complete the upgrade:

#### [Installing Veritas Backup Reporter on Solaris](#)

The install script displays a summary of the installation, including the location of the installation log files.

- 12 Confirm that the upgrade is successful as follows:

```
Solaris          ■ Veritas Backup Reporter Management Server: #  
                  pkginfo -l VRTSccsvs | grep VERSION  
                  ■ Agent: # pkginfo -l VRTSccsva | grep VERSION  
                  ■ Java View Builder: # pkginfo -l VRTSccsvb |  
                    grep VERSION
```

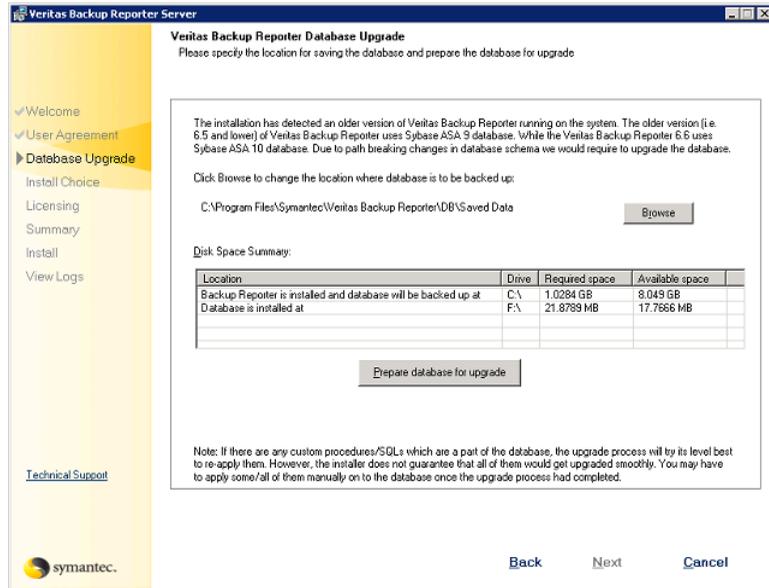
## Upgrading Veritas Backup Reporter on Windows

This section provides the procedure to upgrade VBR on Windows.

### To install VBR Management Server on Windows

- 1 On a Windows host where you want to install VBR Management Server, insert the appropriate Veritas Backup Reporter 6.6 product DVD in the CD-ROM drive.
- 2
  - If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.
  - If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type '*D*: \Browser.exe' and press Enter:  
Where *D* is the CD-ROM drive.  
The Veritas Backup Reporter Installation Wizard appears as shown in the following figure.
- 3 On the Veritas Backup Reporter Installation Wizard, click the Installation link.
- 4 Click the Veritas Backup Reporter Server Installation link to upgrade VBR Management Server.

- 5 Read the license agreement, click 'I accept the terms of the license agreement' and click **Next**. The following screen is displayed.



The screen lists the default locations for database backup, installation and available and required disk space.

If the available space is not adequate, appropriate messages are displayed, which help you decide whether to proceed with upgrade or not.

- 6 Click **Prepare Database for upgrade**. The DB checker utility checks for the consistency between the existing database schema and SA 10 format.

See "[About database upgrade in VBR 6.6](#)" on page 76.

If both schemas are consistent, it asks you to continue the upgrade process. If there is any inconsistency and database cannot be upgraded, the details displayed and you are asked to rollback the upgrade process.

The Next button is enabled once the DB is successfully prepared by the DB checker utility for upgrade.

Click **Next** to continue the database upgrade.

**7** Click any of the following options depending on your requirements:

- |  |  |
|--|--|
| Install to this computer only                      | Select this option to install VBR Management Server on this host.<br><br>The 'Install to a remote computer on your network (push installation)' option is disabled if you are running VBR 6.6 upgrade.   |
| Install a clustered Veritas Backup Reporter Server | Select this option to install VBR Management Server on all selected nodes, in a clustered mode.<br><br>See " <a href="#">Clustering Veritas Backup Reporter on Windows</a> " on page 88.<br><br>This option is enabled if you have Veritas Cluster Server (VCS) installed. |

Click **install to this computer only**.

**8** Click **Typical** to use the default settings, location, or port numbers.

---

**Note:** Click **Custom** if you want to change the default settings, locations, or port numbers.

---

Click **Next**.

**9** On the Add License Keys screen, enter your demo or permanent key that you have received with the purchase of the VBR application and click **Add**.

If you want to collect archive or Enterprise Vault data, you need to add a new license key that is valid for archive data collection, during upgrade.

The license key is added to the following location:`C:\Program Files\Common Files\VERITAS Shared\vrtslic\lic`

**10** Click **Next**. The installer shows the summary of the settings that you have selected for installation.

## 11 Click **Install**.

The installer starts upgrading of VBR Management Server.

In VBR 6.6 the installer creates and registers a new database server service called `Veritas Backup Reporter Database Service`. VBR 6.6 uses Sybase SA 10 to store data. In all previous VBR versions, Sybase SA 9 was used.

Along with the new database service, VBR 6.6 creates a new database engine called `VBR_ VBRhostname`

*VBRhostname* is the name of the host where VBR Management Server is installed.

---

**Note:** The new VBR database location on Windows:

```
C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer
```

Registry key:

```
HKEY_LOCAL_MACHINE\Software\Symantec\Veritas Backup  
Reporter\Data\DbPath
```

---

## 12 After successful upgrade, you can view installation logs or open the README file.

Upgrade logs are as follows:

Unload or database migration logs are present in

`VBR\Server\util\ccsvc-dbugarde0.log` and the Db upgrade logs in

```
C:\Documents and Settings\All Users\Application
```

```
Data\Symantec\VERITAS BACKUP REPORTER\ccsvc-dbugrade0.log
```

## 13 Click **Finish**.

## 14 Upgrade the VBR Agent.

## 15 Upgrade Java View Builder.

Follow this procedure to upgrade VBR Agent.

## Identifying the version of .jar files

While upgrading to Veritas Backup Reporter 6.6, several .jar files are replaced with new patches. However, it is difficult to identify which .jar files have been replaced with the new ones, as the file names do not contain version numbers.

### To identify version numbers of .jar files

- 1 Extract a .jar file using an archiving tool (for example, WinZIP on Windows or jar tool on Solaris).
- 2 Open `META-INF/MANIFEST.MF` file within the .jar file.

The `META-INF/MANIFEST.MF` file includes Module Vendor, Module Name, and Module Version. For example:

- Module-Vendor: Symantec Software - application vendor
- Module-Name: ccsvr-server-core - module name
- Module-Version: 6.6.16.17 - version of module deployed

## Modifying Veritas Backup Reporter on Solaris

Use the Install Script, which resides at the top level of the product CD, to modify existing Veritas Backup Reporter installations.

### To modify Veritas Backup Reporter on Solaris

- 1 Open a Solaris console and log in as `root` on the target host.
- 2 Mount the appropriate Veritas Backup Reporter 6.6 product CD for the components you want to install.
- 3 If you are installing additional Veritas Backup Reporter components, type the following command and press **Enter**:

```
./installvbr
```

- 4 If you are altering the configuration of installed Veritas Backup Reporter components, do the following:
  - Type the following command and press **Enter**:

```
./installvbr -configure
```
  - Follow the prompts presented in the install script.

## Modifying Veritas Backup Reporter on Windows

Use the Install Wizard to modify Veritas Backup Reporter installations. The wizard resides at the top level of the Veritas Backup Reporter 6.6 product DVD.

### To modify Veritas Backup Reporter on Windows

- 1 Log on to the target host as a user with administrator privileges.
- 2 Insert the appropriate Veritas Backup Reporter 6.6 product CD in the CD-ROM drive.  
  
If autorun is enabled, the Install Wizard appears and you can skip to 5.
- 3 On the Start menu, click **Run**.
- 4 In the Open text box, type the following and press **Enter**:  
**D:\Browser.exe**  
where *D* is your CD-ROM drive.
- 5 In the Welcome panel of the Install Wizard, click **Next**.
- 6 If you are installing additional Veritas Backup Reporter components, do the following:
  - Expand the branches in the component tree to display the components and utilities available to install.
  - For each component you want to install, select the component and click **This feature will be installed** from the context menu.  
The icon next to the component changes from an X to a drive icon, indicating that the component is in the install queue.
  -
- 7 If you are altering the configuration of installed Veritas Backup Reporter components, do the following:
  - 
  - Follow the prompts presented in the wizard.
- 8 Reboot your system.

## Clustering Veritas Backup Reporter

This section provides information on installing Veritas Backup Reporter (VBR) in clustered mode, on Solaris and Windows hosts. VBR supports Veritas Cluster Server (VCS) as a cluster solution.

---

**Note:** Veritas Backup Reporter is now clusterable on Windows. If you have Veritas Cluster Server (VCS) present, you can install Veritas Backup Reporter in a clustered mode, on Windows and Solaris hosts.

---

## About a Veritas Backup Reporter cluster

Clusters provide high availability of applications and data to users. In a cluster, two or more nodes are linked in a network and work collectively as a single system. Each node can access the shared disks with the help of cluster software. All nodes in a cluster are constantly aware of the status of resources on the other nodes. If a node becomes unavailable, resources running on that node migrate to an available node (this is called failover).

Veritas Backup Reporter operates in an active/passive failover configuration. VBR 6.6 must be installed on the active node.

---

**Note:** In case of Windows installer, the VBR push installer installs VBR on all nodes in the cluster.

---

When a failover occurs in a VBR cluster, VBR is shut down on the active node and starts on one of the failover nodes in the cluster. During failover, users experience only a short interruption in service. This failover provides high availability for VBR.

Veritas Backup Reporter can be clustered if you have Veritas Cluster Server (VCS) installed. You can cluster Veritas Backup Reporter Management Server and Agent.

You can cluster only VBR Management Server and Agent on Windows and Solaris hosts. Java View Builder cannot be installed in a clustered mode.

After installing Veritas Backup Reporter in clustered mode, the database is available on the shared disk, which an active node can access.

Clustering the VBR Management Server makes the Veritas Backup Reporter UI highly available.

Clustering the VBR Agent makes data collection highly available.

### Supported cluster solutions

For Veritas Backup Reporter 6.6 to be clustered, you must have Veritas Cluster Server (VCS) installed. VBR supports VCS 5.0 on both Windows and Solaris platforms.

---

**Note:** VBR 6.6 does not support Veritas Cluster Server Global Cluster Options (VCS GCO).

---

Veritas Cluster Server is a high-availability solution for cluster configurations. With Veritas Cluster Server you can monitor systems and application services, and restart services on a different system when hardware or software fails.

For more information about VCS, see the *Veritas Cluster Server User's Guide*.

## Clustering Veritas Backup Reporter on Windows

This section provides installing Veritas Backup Reporter in a clustered mode, on a Windows host.

[Table 2-9](#) provides the Windows clustering steps.

**Table 2-9** VBR clustering steps

Step	Description	Reference topic
1	Understand the limitations of a VBR cluster	See <a href="#">“Limitations of a Veritas Backup Reporter cluster”</a> on page 88.
2	<p>Make sure you have met all prerequisites.</p> <p>Prerequisites slightly vary depending on which VBR component you want to install, VBR Management Server or Agent.</p> <p>To install VBR Management Server, you need to install AT on a separate host in a standalone mode.</p> <p>To install VBR Agent, you need the Management Server already installed.</p>	See <a href="#">“Prerequisites for Windows cluster”</a> on page 89.
3	Review the Known Issues section.	See <a href="#">“Known issues”</a> on page 107.
4	Install Veritas Backup Reporter 6.6 on Windows, with the push installation mechanism, VBR installer installs VBR on all selected nodes at once, from the active node.	See <a href="#">“Installing Veritas Backup Reporter on a Windows cluster”</a> on page 91.

### Limitations of a Veritas Backup Reporter cluster

A VBR cluster has the following limitations:

- Only Veritas Backup Reporter Management Server and Agent can be clustered. Java View Builder and Symhelp (topic-search tool) cannot be clustered.

- Veritas Backup Reporter cluster cannot co-exist with any other Symantec product running in secure mode using the Symantec Product Authentication Service.
- Adding a node to a VBR cluster is not supported.
- Removing a node from a VBR cluster is not supported.
- VBR does not support clustered AT. AT installation is a prerequisite for VBR Management Server.
- Veritas Backup Reporter does not support clustered Management Server and clustered Agent to be on the same host. If both are installed on the same host, only Management Server can be clustered.

## Prerequisites for Windows cluster

This section contains information about the requirements that must be met before you install and configure VBR in a clustered mode, on a Windows host.

- Ensure that your hardware and software is supported by Veritas Cluster Server (VCS) and VBR 6.6. To know the operating system requirements for VBR, refer to the *VBR 6.6 Hardware and Software Compatibility List*. This document is also available on the Support Web site (<http://entsupport.symantec.com>). To know if your hardware or software is supported by VCS, refer to the VCS documentation.
- Set up a VCS cluster. Ensure that VCS is correctly installed and configured (VCS 5.0 is supported with VBR 6.6). VBR 6.6 can be installed on as many nodes as VCS supports.
- For a Windows cluster, verify that the cluster disk groups and dynamic volumes for VBR have been created on the shared storage. Refer to the *Veritas Storage Foundation Administrator's Guide* for details.
- Ensure that the shared drive is accessible from all the nodes of the cluster. Also ensure that the shared drive is mounted on the node from which the VBR installation is initiated.
- Ensure that the virtual IP address and virtual host name to be assigned to the VBR cluster are correctly defined and registered in the DNS. Ensure that this virtual IP address is not being used by another system.
- Ensure all VCS services are up and running on all the nodes in the cluster.
- Ensure that VBR installation is being carried out with the domain admin account.
- Ensure that the VBR-component-specific prerequisite are met:

- Before installing VBR Management Server, ensure that Symantec Authentication Service (AT) Server is installed separately in a non-clustered mode. AT may be installed in Root + AB or AB mode. This step is not required if you are installing VBR Agent.  
Make sure AT is running.  
See [“Installing Symantec Product Authentication Service on Windows”](#) on page 90.
- Before installing VBR Agent, ensure that you have installed VBR Management Server, details of which you need to specify during Agent installation.

## Installing Symantec Product Authentication Service on Windows

VBR Management Server requires that Symantec Product Authentication Service (AT) is installed on a standalone host, before it can be clustered. You can either configure AT in root + authentication broker (Root + AB) mode or authentication broker (AB) mode. Clustered Management Server will use this authentication broker. To establish a connection between AT host and VBR Management Server host, you need to create a principal user on the AT host, and use the credentials of this user while installing VBR Management Server.

To cluster a VBR Agent, you do need to install / configure AT.

All VBR cluster nodes must use the same AT. The remote AT can be configured in Root + AB or AB mode.

---

**Note:** VBR does not support clustered AT.

---

Symantec Product Authentication Service can be installed remotely in the following ways:

### To install AT on a remote host

- 1 Logon to the host where you want to install AT.

You should not cluster the AT service, as VBR does not support clustered AT.

- 2 In the product CD, navigate to the following directory:

`D:\x86\ICS\AT`

*D* is CD-ROM drive.

- 3 Execute the following file.

```
VxSSVRTSatSetup.exe
```

- 4 Create a principal user on the AT host using the following command:

```
AT_INSTALL_DIR/bin/vssat addprpl --prplname <principal name>  
--password <principal name password> --pdrtype ab --domain broker@  
<VxAT Root Host name> --prpltype service --is_broker_admin  
--is_domain_admin
```

*AT\_INSTALL\_DIR* is the directory where AT is installed.

The default location is: C:\Program

Files\VERITAS\Security\Authentication

## Installing Veritas Backup Reporter on a Windows cluster

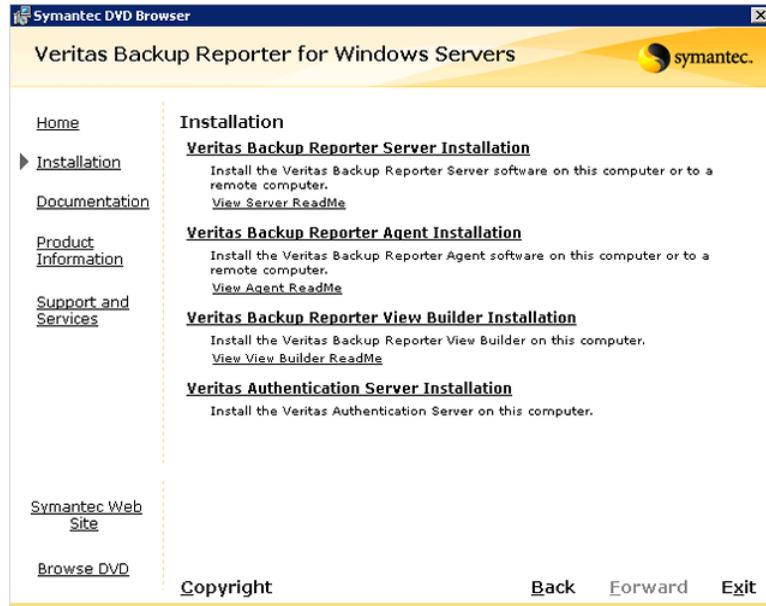
In order to cluster VBR and make it highly available, you must install and configure VBR in a clustered mode. VBR Windows installer comprises a push installation mechanism, which installs VBR on all nodes that you have specified.

You can install VBR Management Server and Agent in a clustered mode, and if they both need to be clustered, they should not be installed on the same host.

### To install VBR Management Server on a Windows cluster

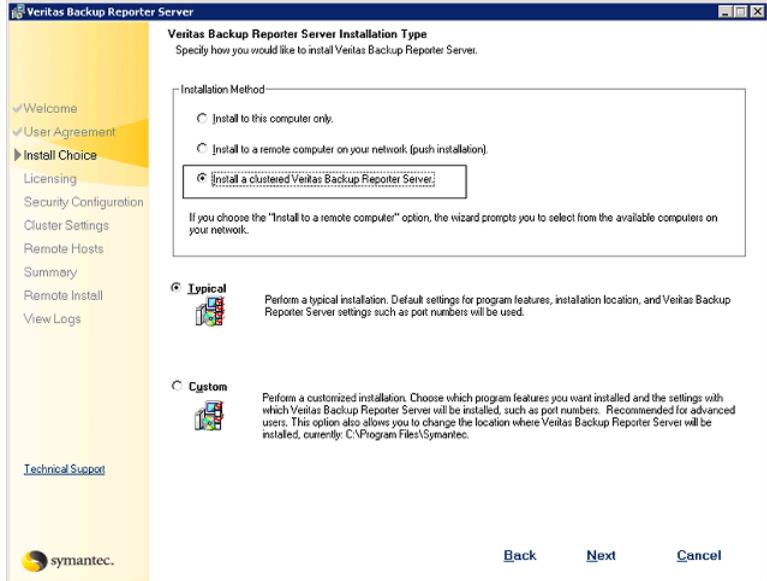
- 1 On a Windows host where you want to install VBR Management Server in a clustered mode, insert the appropriate Veritas Backup Reporter 6.6 product CD in the CD-ROM drive.
- 2
  - If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.
  - If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type '*D*:\Browser.exe' and press Enter:  
Where *D* is the CD-ROM drive.  
The Veritas Backup Reporter Installation Wizard appears as shown in the following figure.

- 3 On the Veritas Backup Reporter Installation Wizard, click the Installation link. The following screen is displayed.



- 4 Only VBR Management Server and Agent can be installed in a clustered mode. Click the Veritas Backup Reporter Server Installation link to install VBR Management Server in a clustered mode.
- 5 Read the license agreement, click 'I accept the terms of the license agreement' and click Next.

- The 'Install a clustered Veritas Backup Server' option is enabled if you have Veritas Cluster Server (VCS) installed. Click this option.



- Click **Typical** to use the default settings, location, or port numbers.

---

**Note:** Click **Custom** if you want to change the default settings, locations, or port numbers.

---

Click **Next**.

- On the Add License Keys screen, enter your demo or permanent key that you have received with the purchase of the VBR application and click **Add**.

The license key is added to the following location: C:\Program Files\Common Files\VERITAS Shared\vrtslic\lic

- Click **Next**.

- The Security Configuration screen appears. Enter the following details of a principal user to connect to the host where AT (Symantec Authentication Service) Authentication Broker (Root + AB or AB) is installed:

- Authentication Service Host Name
- Authentication Service Port Number
- Authentication Service Domain Name

- Authentication Service User Name
- Authentication Service Password

---

**Note:** You should have this principal user created on the Authentication Broker (AB) host.

See [“Installing Symantec Product Authentication Service on Windows”](#) on page 90.

---

**11** On the Cluster Settings screen, enter the following information:

Cluster Group Name	Enter the name for the VBR cluster. For example: VBR_Server
Virtual Host Name	Enter the virtual host name that is assigned to the VBR cluster. For example: VBR_Cluster-1
Virtual IP Address	Enter the IP address that assigned to the VBR cluster
Subnet Mask	Enter the Subnet Mask. For example: 255.255.252.0
Path to Shared data	Select the shared drive path that you have configured in VxVM. For example, Z:\
Public Network	Select LAN as a public network.

Click **Next**.

- 12** After specifying cluster settings, you need to select the nodes on which you want to install VBR Management Server. The VBR Windows installer installs Management Server on all these nodes using the 'Push installation' mechanism. On the Veritas Backup Reporter Server Remote Features, click **Browse** to see the available cluster nodes.
- 13** Select a node and click **Next**.

---

**Caution:** Ensure that this node does not have VBR Agent installed in a clustered mode. Because VBR does not support clustered Management Server and Agent installed on the same host.

---

**14** Enter the login credentials of this host.

Select the **Remember User Name and Password** check box if other nodes have the same login credentials, on which you want to install VBR Management Server. If you select this check box, you are not asked to enter the same information while installing VBR Management Server on the next node.

Click **Continue**.

**15** Enter the directory path where you want to install VBR Management Server on this node. For a cluster to work properly, you should install VBR Management Server at the same location on all cluster nodes.

Select the **Use this folder for subsequent systems** check box if you want to install VBR Management Server at the same location on other nodes.

Click **OK**.

**16** Click **Next**. The installer shows the summary of the settings that you have selected for installation.

**17** Click **Install**.

The installer starts installation of VBR Management Server on the active node and all nodes that you have selected, using the 'Push Installation' mechanism.

Post installation, the installer performs the following tasks on the active node:

- Creates the folder structure on the shared drive and copies the shared data to the correct locations.
- Executes the `vbrclusterutil.exe` utility which creates the cluster configuration in VCS.

**18** After successful installation, you are prompted to configure the VBR cluster.

Click **OK** to create resource group for VBR and move the VBR data to the shared path, for example: Z:\

If the cluster configuration utility fails, the appropriate message is displayed.

---

**Note:** If you want to configure the VBR cluster at a later stage, you can cancel the cluster configuration now. To configure the cluster later, you need to manually create VBR Management Server directories and move the VBR data to the shared disk.

See “[Configuring cluster manually](#)” on page 99.

---

**19** Click **Finish**.

The following procedure describes how to install VBR Agent in a clustered mode.

**To install VBR Agent on a Windows cluster**

**1** On a Windows host where you want to install VBR Agent in a clustered mode, insert the appropriate Veritas Backup Reporter 6.6 product DVD in the CD-ROM drive.

---

**Caution:** Veritas Backup Reporter does not support clustered Management Server and Agent on the same host. The Management Server and Agent should be installed on different hosts to be clustered. If both are installed on the same host, only Management Server can be clustered.

---

**2** ■ If autorun is enabled, the Veritas Backup Reporter Installation Wizard appears.

■ If autorun is not enabled, click **Start > Run**. On the Run dialog box, in the Open text box, type ‘D:\Browser.exe’ and press Enter:

Where *D* is the CD-ROM drive.

The Veritas Backup Reporter Installation Wizard appears.

**3** On the Veritas Backup Reporter Installation Wizard, click the Installation link.

**4** Click the Veritas Backup Reporter Agent Installation link to install VBR Agent in a clustered mode.

**5** Read the license agreement, click ‘I accept the terms of the license agreement’ and click Next.

- 6 The 'Install a clustered Veritas Backup Agent' option is enabled if you have Veritas Cluster Server (VCS) installed on this host. Click this option.
- 7 Click **Typical** to use the default settings, location, or port numbers.

---

**Note:** Click **Custom** if you want to change the default settings, locations, or port numbers.

---

- 8 On the VBR Agent Settings screen, enter the following information:

Host	Enter the host name where VBR Management Server is installed.
Location for Agent spooler data	Select the location to store the Agent spooler data. The spooler resides on the Agent host and can hold the backup data up to its maximum memory usage. The spooler data then sequentially transfers to the Veritas Backup Reporter Management Server.  The default directory for the spooler is: C:\Program Files\Symantec\Veritas Backup Reporter\Agent\Data

- 9 On the Cluster Settings screen, enter the following information:

Cluster Group Name	Enter the name for the VBR cluster. For example: VBR_Server
Virtual Host Name	Enter the virtual host name that is assigned to the VBR cluster. For example: VBR_Cluster-1
Virtual IP Address	Enter the IP address that assigned to the VBR cluster
Subnet Mask	Enter the Subnet Mask. For example: 255.255.252.0
Path to Shared data	Select the shared drive path that you have configured in VxVM. For example, Z:\ <b>Note:</b> The shared drive should be mounted on the node from which you are running the installer.
Public Network	Select LAN as a public network.

Click **Next**.

- 10 After specifying cluster settings, you need to select the nodes on which you want to install VBR Agent. The VBR Windows installer installs Agent on all these nodes using the 'Push installation' mechanism. On the Veritas Backup Reporter Server Remote Features, click **Browse** to see the available cluster nodes.
- 11 Select a node and click **Next**.

---

**Caution:** Ensure that VBR Management Server is not installed on this host, in a clustered mode. Because VBR does not support clustered Management Server and Agent on the same host.

---

---

**Note:** If this host already has VBR Agent installed, then you are prompted to specify whether you want it to be clustered or not.

---

- 12 Enter the login credentials of this host.  
Select the **Remember User Name and Password** check box if other nodes have the same login credentials, on which you want to install VBR Agent. If you select this check box, you are not asked to enter the same information while installing VBR Agent on the next node.  
Click **Continue**.
- 13 Enter the directory path where you want to install VBR Agent on this node. For a cluster to work properly, you should install VBR Agent at the same location on all cluster nodes.  
Select the **Use this folder for subsequent systems** check box if you want to install VBR Agent at the same location on other nodes.  
Click **OK**.
- 14 Click **Next**. The installer shows the summary of the settings that you have selected for installation.
- 15 Click **Install**.

The installer starts installation of VBR Agent on the active node and all nodes that you selected.

Post installation, the installer performs the following tasks on the active node:

- Creates the folder structure on the shared drive and copies the shared data to the correct locations.

- Executes the `vbrclusterutil.exe` utility which creates the cluster configuration in VCS.
- 16 After successful installation, you are prompted to configure the VBR cluster. Click **OK** to copy the shared data to the shared drive and execute the cluster configuration utilities, for example: Z:\

---

**Note:** If you want to configure the VBR cluster at a later stage, you can cancel the cluster configuration now. To configure the cluster later, you need to manually create VBR Agent directories on the shared disk.

See “[Configuring cluster manually](#)” on page 99.

---

- 17 Click **Finish**.

## Configuring cluster manually

This section provides the procedure to manually configuring a VBR cluster. If you cancel the cluster configuration on the Windows installer, you need to manually configure the cluster later.

### To manually configure a clustered VBR Management Server

- 1 Create the following VBR Management Server directories on the shared disk. *sharedPath* is the location on the shared disk where you want to store VBR files.
  - `sharedPath\Veritas Backup Reporter`
  - `sharedPath\Veritas Backup Reporter\Server`
  - `sharedPath\Veritas Backup Reporter\Server\DB`
  - `sharedPath\Veritas Backup Reporter\Server\DB\Conf`
  - `sharedPath\Veritas Backup Reporter\Server\DB\Data`
  - `sharedPath\Veritas Backup Reporter\Server\Web`
  - `sharedPath\Veritas Backup Reporter\Server\Web\Conf`
  - `sharedPath\Veritas Backup Reporter\Server\Web\Logs`
  - `sharedPath\Veritas Backup Reporter\Server\CorbaServer`

- `sharedPath\Veritas Backup Reporter\Server\CorbaServer\Logs`
- 2 Move the `vbr_conf.properties` from `InstallDir\Veritas Backup Reporter\Server\Conf\` to `sharedPath\Veritas Backup Reporter\Server\Web\Conf\`  
*InstallDir* is the location where VBR is installed.
- 3 Move the `ccsvc.db` from `installdir\Veritas Backup Reporter\Server\DBServer\data\` to `sharedPath\Veritas Backup Reporter\Server\DBServer\data\`
- 4 Run `InstallPath\server\bin\cluster\vbrclusterutil.exe -ci -s VBRS` for creating VBR server group on VCS.

#### To manually configure a clustered VBR Agent

- 1 Create the following VBR Agent directories :
  - `sharedPath\Veritas Backup Reporter sharedPath\Veritas Backup Reporter\Agent`
  - `sharedPath\Veritas Backup Reporter\Agent\Logs`
  - `sharedPath\Veritas Backup Reporter\Agent\Data`
  - `sharedPath\Veritas Backup Reporter\Agent\Data\evData`
- 2 Run `InstallPath\Agent\bin\cluster\vbrclusterutil.exe -ci -s VBRA` for creating VBR Agent group on VCS.

### Troubleshooting Windows cluster issues

To troubleshoot any Windows cluster issues, follow these steps:

- Check if the installer has implemented all steps  
No logging is provided by cluster configuration libraries or utilities
- Check VCS logs located at the default location `C:\Program Files\Veritas\cluster server\log`, for errors encountered during cluster configuration
- Check VBR logs: Web server logs, CORBA server logs, and Agent logs  
See “[About Veritas Backup Reporter log files](#)” on page 472.

## Clustering Veritas Backup Reporter on Solaris

This section provides information on installing VBR on Solaris host, in a clustered mode.

Only VBR Management Server and Agent can be installed in a clustered mode.

**Table 2-10** Steps to cluster VBR on Solaris

Step	Description	Reference topic
1	Make sure you have met all prerequisites.  You should have remote AT installed, to which VBR Management Server can refer to.	See <a href="#">“Prerequisites for a Solaris cluster”</a> on page 101.
2	Review the Known Issues section.	See <a href="#">“Known issues”</a> on page 107.
3	Install Veritas Backup Reporter 6.6.	See <a href="#">“Installing Veritas Backup Reporter on Solaris nodes”</a> on page 103.

## Prerequisites for a Solaris cluster

To install and configure Veritas Backup Reporter in a clustered mode, you must meet the following prerequisites:

- All participating nodes have Veritas Cluster Server (VCS) installed in non-secure mode.
- All nodes must have adequate resources to run Veritas Backup Reporter. See [“About operating system requirements”](#) on page 36.
- A shared volume or location is available to store the Veritas Backup Reporter database and security information. Locations for the Veritas Backup Reporter database and security information are stored in different paths.
- Each node requires a separate and identical install of Veritas Backup Reporter, in terms of Date and Time. All options selected during install time should be consistent node-to-node unless otherwise specified.
- All nodes must be able to mount the shared disk. You can create disk groups and volumes using VxSF.
- You should install AT (Symantec Product Authentication Service) Authentication Broker on a remote host in Root + AB or AB mode. All cluster nodes must use the same Authentication Broker. See [“Installing Symantec Product Authentication Service on Solaris”](#) on page 102.

---

**Note:** VBR does not support clustered AT.

---

- For a Solaris cluster, ensure that the shared disk is not mounted on any node in the cluster. If applicable, unmount the VBR shared mount point. Stop the volume if the mount point is on and stop the disk group for that volume on all nodes.

---

**Caution:** You should separately configure the Web settings on all Solaris cluster nodes.

---

## Installing Symantec Product Authentication Service on Solaris

VBR Management Server requires that Symantec Product Authentication Service (AT) is installed on a standalone host, before it can be clustered. You must install the version of AT Service shipped with VBR 6.6. You can either configure AT in root + authentication broker (Root + AB) mode or authentication broker (AB) mode. Clustered Management Server will use this authentication broker. To establish a connection between AT host and VBR Management Server host, you need to create a principal user on the AT host, and use the credentials of this user while installing VBR Management Server.

To cluster a VBR Agent, you do not need to install or configure AT.

---

**Note:** Symantec Product Authentication Service is installed when you install Veritas Cluster Server. You must upgrade to the version of authentication service shipped with VBR 6.6.

---

All VBR cluster nodes must use the same AT. The remote AT can be configured in Root + AB or AB mode.

---

**Note:** VBR does not support clustered AT.

---

Symantec Product Authentication Service can be installed remotely in the following ways:

### To install AT on a remote host

- 1 Logon to the host where you want to install AT.

You should not cluster the AT service, as VBR does not support clustered AT.

- 2 Using the command prompt, execute the following file in AT directory in the product DVD:

```
VxSSVRTSatSetup
```

- 3 Create a principal user on the AT host using the following command:

```
AT_INSTALL_DIR/bin/vssat addprpl --prplname <principal name>
--password <principal name password> --pdrtype ab --domain broker@
<VxAT Root Host name> --prpltype service --is_broker_admin
--is_domain_admin
```

*AT\_INSTALL\_DIR* is the directory where AT is installed.

## Installing Veritas Backup Reporter on Solaris nodes

This section describes how to install and configure Veritas Backup Reporter on Solaris, in a clustered mode.

- Network device, virtual IP and virtual name registered in DNS, netmask
- Any of the following:

Logical Volume Manager	Disk group name, volume name, file system type, mount point, and block device
------------------------	---

Physical disk	Mount point, block device, and file system type
---------------	---

Use the Veritas Backup Reporter Install Script, which resides in the root directory in the product DVD, to install Veritas Backup Reporter on a Solaris host.

The install comprises the following phases:

- Selecting components to install
- Configuring components in the install queue
- Installing the components

### To install Veritas Backup Reporter components on Solaris

- 1 Open a UNIX console and log in as `root` on the target host.
- 2 Mount the appropriate Veritas Backup Reporter 6.6 product CD for the components you are installing.

- 3** Type the following command and press **Enter**:

```
./installvbr
```

- 4** If the installer detects a cluster software, it gives you an option to install Veritas Backup Reporter in cluster mode. Select the option depending on the following scenarios:

- If the current node is not the last one in a cluster setup, select the following option:

```
Do you want to configure the cluster setup now? [y,n,q] (y)n
```

- If the current node is the last one in a new cluster setup, select the following options:

```
Do you want to configure the cluster setup now? [y,n,q] (y)y
```

```
Do you want to add this machine to an existing VBR cluster?
```

```
[y,n,q] (n)n
```

```
You have selected N, are you sure: [y,n,q] (n)y
```

- If you want to add a new node to the existing cluster, select the following option:

```
Do you want to configure the cluster setup now? [y,n,q] (y)y
```

```
Do you want to add this machine to an existing VBR cluster?
```

```
[y,n,q] (n)y
```

```
You have selected Y, are you sure: [y,n,q] (n)y
```

For further procedure, refer to 'Installing VBR on Solaris' section in this guide.

#### To add a new node to the existing Solaris cluster

- ◆ Depending on the given scenarios, run any of the following commands from the existing clustered nodes:

- If the Veritas Backup Reporter Management Server is installed on the node, run the following command:

```
Run /opt/VRTSccsvs/bin/cluster/cluster_config -s vbrs -o  
add_node -n <new_node_name>
```

- If the Veritas Backup Reporter Management Server and Agent are installed on the node, run the following command:

```
Run /opt/VRTSccsvs/bin/cluster/cluster_config -s vbrsa -o  
add_node -n <new_node_name>
```

- If the Veritas Backup Reporter Agent is installed on the node, run the following command:

```
Run /opt/VRTSccsvs/bin/cluster/cluster_config -s vbra -o  
add_node -n <new_node_name>
```

## Upgrading standalone VBR to clustered VBR on Solaris

You can upgrade standalone VBR to clustered VBR.

See “[About supported upgrade paths](#)” on page 40.

### To upgrade standalone VBR to clustered VBR on Solaris

- 1 Manually upgrade the existing database to Veritas Backup Reporter.
- 2 Install Veritas Backup Reporter in a clustered mode. Refer to the installation steps on Solaris.
- 3 Freeze the Veritas Backup Reporter service group.  
Refer to your cluster documentation for details.
- 4 Logon to the active node.
- 5 Stop database service by running the following command:  

```
/opt/VRTSccsvs/bin/vbrserver stop force
```
- 6 Copy the upgraded database to the shared location by running the following command:  

```
<SHARED_DISK>/vbr[s|sa]/vbrs/data/db
```
- 7 If there is any fault in the Veritas Backup Reporter service group, clear it.  
For details, refer to the cluster documentation.
- 8 Start the Veritas Backup Reporter services by running the following command:  

```
/opt/VRTSccsvs/bin/cluster/VBRServerStart
```
- 9 Unfreeze the Veritas Backup Reporter service group.
- 10 Delete the agents available in the Veritas Backup Reporter console on the **Settings > Global Settings > Agent Configuration** page.
- 11 Repeat the following for all agents:
  - Logon to the agent host.
  - Stop the agent process.
  - Run the following command:  

```
agentauth -server <VBR_SERVER_VIRTUAL_NAME>
```
  - Start the agent process.

## Upgrading clustered VBR to VBR 6.6 version

This section provides information on upgrading clustered VBR to 6.6 version.

### To upgrade clustered VBR to 6.6 version

- 1 Upgrade all inactive nodes to VBR 6.6. Refer to the 'Installing VBR in a clustered mode on Solaris' section.
- 2 Upgrade the active node to clustered VBR 6.6.

## Removing a Solaris node from a clustered environment

This section provides you with the procedure for removing a Solaris node from a clustered setup.

### To remove a node

- 1 Make sure the node you are trying to remove is not the active node.
- 2 Remove the node from the system list of Veritas Backup Reporter service group.  
  
Refer to your cluster documentation for details.
- 3 Uninstall Veritas Backup Reporter from the node.
- 4 Remove the Veritas Backup Reporter related entries or files from the VCS directories.

For details, refer to your cluster documentation.

## Removing VBR completely from the cluster

Use the following instructions to remove VBR completely from the cluster. This involves removing the cluster configuration and the VBR database completely.

### To remove VBR completely from Windows

- 1 Stop the VBR resource group and take it's resources offline.

```
hagrp -offline -force <VBR_Resource_Group> -any
```

where <VBR\_Resource\_Group> is the name of the VBR resource group.

- 2 Bring the mount resource online.

```
hares -online <Mount_Resource_Name>
```

- 3 Offline all the VBR resources that are online.

```
hares -offline <Resource Name>
```

where <Resource Name> is the Mount resource name if a physical disk is configured. If a shared disk is configured using VxVM, the <Resource Name> includes mount, volume, and disk-group resource names.

- 4 Set the VCS configuration file to read/write mode.  
`haconf -makerw`
- 5 Delete all the resources.  
`hares -delete <Resource Name>`
- 6 Delete the VBR resource group.  
`hatype -delete NetBackupVBRServer` or `hatype -delete NetBackupVBRAgent`  
`hagrps -delete <VBR_Resource_Group_Name>`
- 7 Delete the NetBackupVBR resource type.
- 8 Save this configuration.  
`haconf -dump -makero`  
 The option `-makero` sets the configuration to read-only.

## Known issues

[Table 2-11](#) lists issues that are related to Veritas Backup Reporter clustering.

**Table 2-11** Veritas Backup Reporter clustering issues on Windows and Solaris

Known issue and incident #	Description
Web Server Configurations are not retained on failover in clustered VBR on Solaris (1156106)	Web server settings, such as settings related to port number, SMTP server, and logging are host dependent. If you change these settings on any node, those are not reflected on other nodes in a cluster. The Web server is not clustered, therefore the failover node would not have the Web server settings same as that of the online node.  The workaround is as follows: <ul style="list-style-type: none"> <li>■ Failover to a node manually.</li> <li>■ Go to Global Settings &gt; Web Console Settings.</li> <li>■ Change the Web server settings, as you want them to be after a failover.</li> <li>■ Repeat the first three steps for each node in the cluster.</li> </ul>

**Table 2-11** Veritas Backup Reporter clustering issues on Windows and Solaris  
*(continued)*

Known issue and incident #	Description
<p>Global setting section configurations are not retained after failover (licensing, module links, server status) on Solaris (1156576)</p>	<p>Certain global settings, such as Licensing, Module Links, and Server Status (Server Log Level and Scheduler Status) are host dependent. If you change these settings on any node, those are not reflected on other nodes in a cluster. Therefore, the failover node would not have these global settings same as that of the online node. The workaround is as follows:</p> <ul style="list-style-type: none"> <li>■ Failover to a node manually.</li> <li>■ Go to Global Settings.</li> <li>■ Change the licensing, module links, and server status settings, as you want them to be after a failover.</li> <li>■ Repeat the first three steps for each node in the cluster.</li> </ul>
<p>agentErr.log file is created on local disk (1594453 )</p>	<p>After clustering VBR Agent, the agentErr.log file is created on the local host (active node). Neither agentErr.log nor other Agent log files are created on the shared disk.</p>
<p>The clustered applications are brought down while upgrading packages by VBR (1523125)</p>	<ul style="list-style-type: none"> <li>■ Create a clustered Web app on VCS.</li> <li>■ Verify that it is created in GUI. Make it online on a system</li> <li>■ Install VBR on the system, in a clustered mode.</li> </ul> <p>After VBR installation, the clustered Web application is offline</p>
<p>Solaris Cluster upgrade from 6.5 to 6.6 faults the VBR Service Group (1531453)</p>	<p>While upgrading Solaris cluster from VBR 6.5 to 6.6, VBR uninstalls packages / brings VBR processes down, which faults the resource group.</p> <p>The workaround is to upgrade to 6.5.1 before upgrading to 6.6, or follow these steps:</p> <ul style="list-style-type: none"> <li>■ Change the VBRServerStatus and VBRAgentStatus scripts before VBR 6.6 upgrade begins.</li> </ul> <p>These new scripts prevent VBR from faulting. These scripts have a support to look for a frozen file (put by installer), if it is found it returns success. Thus, the service group is not faulted during upgrade process.</p>

**Table 2-11** Veritas Backup Reporter clustering issues on Windows and Solaris  
*(continued)*

Known issue and incident #	Description
Private domain user cannot be added on clustered VBR on Windows(1590754)	<p>On Windows, while creating Private Domain User in clustered VBR, a null pointer exception is thrown.</p> <p>The workaround is as follows:</p> <p>Execute the following CLI on the AT node:</p> <pre>vssat addprpl --pdrtype ab --domain cc_users --prplname &lt;user name&gt; --password &lt;password&gt; --prpltype user</pre> <p>This CLI adds a new user in cc_users private domain.</p>
On a Windows cluster, admin password cannot be changed from GUI (1590816)	<p>This issue is seen because of a failure in CORBA connection between VBR server and AT server.</p> <p>Workaround:</p> <p>Execute the following CLI from the command line on the AT server node:</p> <pre>vssat changepasswd --pdrtype ab --domain cc_users --prplname admin --currentpasswd &lt;default password&gt; --newpasswd &lt;new password&gt; --repeatednewpasswd &lt;new password&gt;</pre>
All domains are not listed in VBR login page in clustered mode, on Windows (1591736)	<p>This issue is seen because of the CORBA connection issue between VBR Management Server and the remote AT server.</p> <p>The workaround:</p> <p>Add the required domains to the domain broker entry on the VBR Management Server host. Command: <code>vssat addbrokerdomain</code></p>
Upgrade on passive node fails, on Solaris (1591850)	<p>After upgrading the passive nodes, the VBR service group moves to faulted state, because of the Web app was restarted. This requires a manual intervention of the administrator for removing the fault, by executing cluster CLIs <code>/opt/VRTSvcs/bin/hagrp -clear vbrsa_group</code></p>

**Table 2-11** Veritas Backup Reporter clustering issues on Windows and Solaris  
(continued)

Known issue and incident #	Description
<p>On Windows, sometimes the cluster configuration is not saved in VCS. Rebooting the system cleans the configuration in VCS (1599581)</p>	<p>Any of the following resolutions will work:</p> <p>After VBR cluster configuration, save VCS configuration from the VCS Java console or by running <code>haconf -dump</code> command. This would ensure that the configuration is saved.</p> <p>OR</p> <p>If you see the VBR cluster group missing upon rebooting the VCS nodes:</p> <ul style="list-style-type: none"> <li>■ Manually bring-up the shared disk on one of the nodes.</li> <li>■ From that node, run <code>vbrclusterutil -ci -s VBRS</code> for VBR Management Server installation. Run <code>vbrclusterutil -ci -s VBRA</code> for VBR Agent installation.</li> </ul>

## Resolving agent authentication failures manually on Solaris and Windows

If the Veritas Backup Reporter Agent authentication fails on Solaris or Windows, use the following procedures to manually resolving agent authentication failures.

If the Veritas Backup Reporter Agent cannot connect to the Veritas Backup Reporter Management Server, a message such as the following may appear in the logs:

```
Authentication failed
The user or password are not valid in the given domain.
Domain = cc_users@myServer
User = admin
```

### To manually resolve agent authentication failures on a Solaris system

- ◆ Run the following command:

```
/opt/VRTSccsva/bin/agentauth -server <serverHostName>
```

### To manually resolve agent authentication failures on a Windows system

- 1 Log on to the Veritas Backup Reporter Management Server host with administrator-level privileges.
- 2 Stop the agent service using the Windows Services console (**Start > Settings > Control Panel > Administrative Tools > Services**).
- 3 Open a Windows command prompt and change to the following agent default installation directory:

```
\Program Files\Symantec\Veritas Backup Reporter\Agent\bin
```

- 4 Type the following command and press **Enter**:

```
agentauth.exe -server <serverHostName>
```

If the `agentauth.exe -server <serverHostName>` command fails, verify that the management server is online and accessible and check if the agent time lags behind the management server time.

The `agentauth.exe` command can fail for a number of reasons.

Two of the most common reasons for the `agentauth.exe` command to fail are as follows:

- The Security Dynamic Link Libraries (DLLs) are not in the PATH.  
The workaround for this is to run the following commands:
  - `cd \Program Files\Veritas\Security\Authentication\bin`
  - `"\Program Files\Symantec\Veritas Backup Reporter\Agent\bin\agentauth.exe" -server <serverHostName>`
- The management server cannot be contacted.  
Ensure that the Veritas Backup Reporter Management Server and Authentication Service are running and can be reached on ports 1556 and 2821, respectively.  
`agentauth`

- 5 Restart the agent service.

## Verifying that Veritas Backup Reporter is running properly

After installing Veritas Backup Reporter on either UNIX or Windows, perform a check to verify that Veritas Backup Reporter is running properly.

### To verify that Veritas Backup Reporter is running properly

- 1 Go to **http://<server-host>: 8181**.

If the Veritas Backup Reporter Login screen appears, the Veritas Backup Reporter Management Server, the Web server, and the Authentication Service are running.

The first time you login it, takes longer than usual time for the GUI to load.

- 2 Login using admin (username) /password (password) on the private domain:  
**cc\_users@<server name>**
- 3 Verify that the agents and data collectors are set up correctly.
  - Go to **Settings > Global Settings > Agent Configuration**.  
The Veritas Backup Reporter Agent should appear.  
If an agent does not appear, do not click Create. Instead, troubleshoot the problem by checking that you correctly configured the ports.

## Stopping and starting Veritas Backup Reporter services

This section talks about the Veritas Backup Reporter services. It provides the procedures to stop and start VBR services on Solaris and Windows hosts.

### About Veritas Backup Reporter services

This section lists the Veritas Backup Reporter (VBR) services.

- Veritas Backup Reporter Management Server  
See [“Stopping and restarting the Veritas Backup Reporter Management Server”](#) on page 113.
- On Windows - Veritas Backup Reporter Database  
On Solaris - dbsrv10  
VBR 6.6 uses Sybase SA 10 database management system to store the data.
- Veritas Backup Reporter Agent  
See [“Stopping and starting the Veritas Backup Reporter Agent ”](#) on page 115.
- Veritas Backup Reporter CORBA server  
CORBA service is dependant on VBR database service. If you stop the database service, the CORBA service also stops. However, you need to start the CORBA server service separately.
- Veritas Backup Reporter Help (or Symhelp)

This is a search / help tool, using which you can search a specific VBR topic. the section called “Using the Symhelp search tool”

---

**Caution:** Symhelp may not be updated. For the most recent information about *Veritas Backup Reporter 6.6 Guide*.

---

- Symantec Product Authentication Service
- Symantec Web server
- Symantec Private Branch Exchange (PBX)

---

**Note:** For more details on the VBR and shared components, refer to the following section:

the section called “About Veritas Backup Reporter components”

---

## Stopping and restarting the Veritas Backup Reporter Management Server

By default, the Veritas Backup Reporter Management Server starts whenever you boot your Veritas Backup Reporter Management Server host. However, you can manually stop and restart the Veritas Backup Reporter Management Server service.

### Stopping and restarting the Management Server on Solaris

This section provides the procedure required to stop and restart VBR Management Server on a Windows machine.

#### To stop and restart the VBR Management Server on Solaris

- 1 Open a Solaris console, and log on to the Veritas Backup Reporter Management Server host as `root`.
- 2 In the console, change to the Veritas Backup Reporter Management Server directory.

By default, this directory is: `/opt/VRTSccsvs/bin`

For example:

```
cd /opt/VRTSccsvs/bin
```

Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation.

- 3 Add `/opt/vrts/bin` to your host's `PATH` environment variable to access the Veritas Backup Reporter scripts and commands from any directory on the host.
- 4 Shut down the Veritas Backup Reporter Management Server by running the following command:

```
./vbrserver stop force
```

The `vbrserver stop force` command stops the Veritas Backup Reporter Management Server and its shared components, such as Symantec Product Authentication Service, Veritas Backup Reporter Database, CORBA server, Symantec Private Branch Exchange, and Symhelp (Veritas Backup Reporter Help).

- 5 To stop the Veritas Backup Reporter Management Server but not the components that are shared among products, use the `vbrserver stop` command.

After stopping the Veritas Backup Reporter Management Server, wait about 30 seconds before starting it again. This gives the operating system time to free up logical ports and other resources that the Veritas Backup Reporter Management Server may need upon restart.

This command neither starts nor stops the Veritas Backup Reporter Agent.

- 6 Restart the Veritas Backup Reporter Management Server from the same directory by typing the following command:

```
./vbrserver start
```

The `start` command starts the Veritas Backup Reporter Management Server and its components, including components shared with other Symantec products.

By default, the Veritas Backup Reporter Management Server starts whenever you boot its host.

The command `vbrserver start` starts the Veritas Backup Reporter Management Server, its services, such as Symantec Product Authentication Service, Veritas Backup Reporter Database (dbsrv10), CORBA server, Symantec Private Branch Exchange, and Veritas Backup Reporter Help (or Symhelp).

## Stopping and restarting the Management Server on Windows

This section provides the procedure required to stop and restart VBR Management Server on a Windows machine.

### To stop and restart the Veritas Backup Reporter Management Server on Windows

- 1 Log on to the Veritas Backup Reporter Management Server host as an administrator or a user in the Administrators group.
- 2 Using the Windows Service Control Manager (SCM), to stop the following Veritas services in the order listed, right-click the service and click **Stop**.

```
Veritas Backup Reporter Database  
Symantec Private Branch Exchange  
Symantec Product Authentication Service  
Symantec Web Server  
Veritas Backup Reporter Management Server  
Veritas Backup Reporter Agent
```

After stopping the Veritas Backup Reporter Management Server, wait about 30 seconds before starting it again. This gives the operating system time to free up logical ports and other resources that the Veritas Backup Reporter Management Server may need upon restart.

- 3 Alternatively, you can also use the following command to automatically stop VBR services:

```
cd <INSTALLDIR>\Tools cscript vx_services_stop.vbs
```

- 4 To restart the following Veritas services in the order listed, right-click the service, and click **Start**.

```
Veritas Backup Reporter Management Server  
Symantec Web Server  
Symantec Product Authentication Service  
Symantec Private Branch Exchange  
Veritas Backup Reporter Database  
Veritas Backup Reporter CORBA server  
Veritas Backup Reporter Help
```

- 5 Alternatively, you can also use the following command to automatically start the Veritas services.

```
cd <INSTALLDIR>\Tools cscript vx_services_start.vbs
```

- 6 Close the Windows Service Control Manager.

## Stopping and starting the Veritas Backup Reporter Agent

By default, the Veritas Backup Reporter Agent starts whenever you boot your Agent host. However, you can manually stop or start the VBR Agent service.

## Stopping and restarting Agent on Solaris

This section provides the procedure to stop and restart the Veritas Backup Reporter Agent service on a Solaris host.

To stop or start the Agent on a Solaris host, you can also use the startup and shutdown script, `vbragent`.

`vbragent`

### To stop and restart the Veritas Backup Reporter Agent on Solaris

- 1 Open a UNIX console, and log on to the Agent host as `root`.
- 2 In the console, change to the agent directory.

By default, this directory is: `/opt/VRTSccsva/bin`

For example:

```
cd /opt/VRTSccsva/bin
```

Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation.

- 3 Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the Veritas Backup Reporter scripts and commands from any directory on the host.
- 4 Shut down the agent by typing the following command:

```
./vbragent stop
```

After stopping the agent, wait about 30 seconds before starting it again. This gives the operating system time to free up logical ports and other resources that the agent may need upon restart.

- 5 Restart the agent from the same directory by typing the following command:

```
./vbragent start
```

## Stopping and restarting Agent on Windows

If you have administrator-level rights on your Windows hosts, use the Windows Services application to stop or start the Veritas Backup Reporter Agent.

### To stop and start the Veritas Backup Reporter Agent on Windows

- 1 Log on to the Windows agent host as an administrator or a user in the Administrator's group.
- 2 Open the Windows Service Control Manager (SCM) by clicking **Start > Program Files > Administrative Tools > Component Services**.

- 3** In the Services list, locate the Veritas Backup Reporter Agent service, right-click the service and click **Stop**.

After stopping the agent, wait about 30 seconds before starting it again. This gives the operating system time to free up logical ports and other resources that the agent may need upon restart.

- 4** Right-click the service and click **Start**.
- 5** Close the Windows Service Control Manager.



# Introducing the Veritas Backup Reporter console

This chapter includes the following topics:

- [Logging on to Veritas Backup Reporter console](#)
- [About the Veritas Backup Reporter console](#)
- [Accessing product Help](#)
- [Using the Symhelp search tool](#)
- [Accessing NetBackup Operations Manager host](#)

## Logging on to Veritas Backup Reporter console

Veritas™ Backup Reporter (VBR) is a Web-based software application that helps organizations by providing visibility into their data protection environment.

If you are using a Web browser that is supported by Veritas Backup Reporter and you have all prerequisites met, you can log on and connect to a VBR Management Server host.

For more information about Web browser and Operating Systems requirements, refer to *Veritas Backup Reporter Hardware and Software Compatibility List*.

### To log on to Veritas Backup Reporter console

- 1 On a VBR Management Server host or a client host that is connected to the Management Server, open a Web browser.

---

**Note:** You must configure the Web browser to accept cookies. If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the VBR Management Server. In addition to this, you must enable JavaScript.

---

- 2 In the browser's address field, type the following URL:

`https://VBRServerHostName:portNumber/vbr`

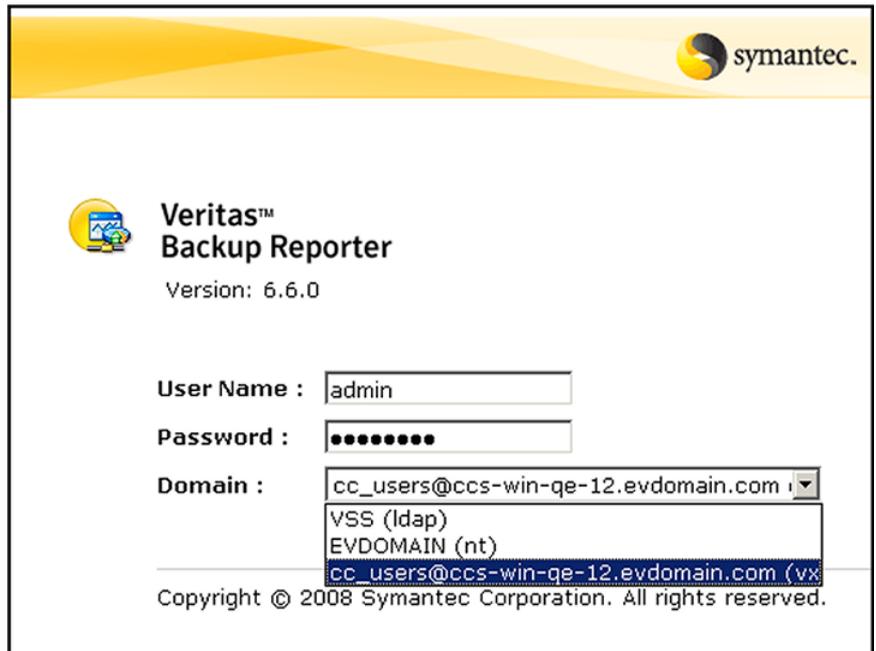
where *VBRServerHostName* is the name, IP address, or fully qualified domain name of the VBR Management Server host. *portNumber* is the port number through which you are connected to the VBR Management Server. The default port number is '8443'.

For example: `https://myhost.example.com:8443/vbr`

You can access any VBR Management Server host to which you have the IP connectivity and the required user credentials.

On Windows clients, you can create a shortcut using this URL to facilitate launching of the console from the Windows Start menu.

- 3 Press **Enter**. The login page is displayed as shown in the following figure:



**Veritas™  
Backup Reporter**  
Version: 6.6.0

User Name :

Password :

Domain :  ▼  
VSS (ldap)  
EVDOMAIN (nt)  
cc\_users@ccs-win-qe-12.evdomain.com (vx)

Copyright © 2008 Symantec Corporation. All rights reserved.

- 4 On the login page, enter the following user information:

---

**Note:** Symantec Authentication Service (AT) authenticates the VBR user information.

See [“About the Symantec Product Authentication Service”](#) on page 25.

---

User Name

Enter the user name.

**Note:** Veritas Backup Reporter is shipped with the default user name and password of admin user created in the ‘cc\_users’ domain. The default user credentials are as follows: ‘admin’ and ‘password’. You can use these credentials at the time of the first login.

For security reasons, it is best to change these credentials as soon as possible.

Password

Enter the password of your user account.

**Domain**

Select the domain to which your user account belongs.

If you are logging in with the default admin user account, use the 'cc\_users@hostname (vx)' domain.

*hostname* is the name of the VBR Management Server host.

See “[Managing user accounts](#)” on page 163.

**Caution:** If the Domain drop-down list is empty, it is likely that the VBR Management Server host is not configured properly.

the section called “About troubleshooting Veritas Backup Reporter console issues ”

- Click **Login**.

## About the Veritas Backup Reporter console

The Veritas Backup Reporter console is displayed in a Web browser and consists of a header, a set of tabs, a task pane, and the main content pane.

After successfully logging on to VBR console, the Home page is displayed as shown in the following figure:

See “[Logging on to Veritas Backup Reporter console](#)” on page 119.



The following sections describe the VBR Web UI (User Interface) elements in detail.

- [About the Veritas Backup Reporter console header](#)

- [About the Veritas Backup Reporter console tabs](#)
- [About the Veritas Backup Reporter console task pane](#)
- [About the Veritas Backup Reporter console content pane](#)

---

**Note:** At the bottom, the VBR console displays name of the user who has currently logged in, for example [admin]. It also displays the date and time when you logged on to the VBR Management Server host.

---

## About the Veritas Backup Reporter console header

The VBR console header located at the top consists of the following functions:

About	Click to view Veritas Backup Reporter product details, such as current version or copyright information.
Logout	Click to logout from the VBR console
Help	Click to access Veritas Backup Reporter Help
Search	Access Veritas Backup Reporter help search tool, called Symhelp See <a href="#">“Using the Symhelp search tool”</a> on page 126.
NetBackup	Click to access NetBackup Operations Manager, another Symantec product See <a href="#">“Accessing NetBackup Operations Manager host”</a> on page 127.

---

**Note:** The Veritas Backup Reporter console header does not display the name of the Management Server to which you are connected. To connect to another Management Server, log out and then connect.

See [“Logging on to Veritas Backup Reporter console”](#) on page 119.

---

## About the Veritas Backup Reporter console tabs

The VBR console header consists of the following tabs that provide access to various Veritas Backup Reporter functions.

Home	Use this tab to display the home page
------	---------------------------------------

Reports	<p>Use this tab to generate and view reports about backup and archive resources</p> <p>See <a href="#">“About backup and recovery reports”</a> on page 333.</p> <p>See <a href="#">“Reporting on archive data”</a> on page 405.</p> <p>In VBR 6.6, you can also generate archive reports based on Enterprise Vault data.</p> <p>The Reports tab consists of the following sub-tabs:</p> <ul style="list-style-type: none"><li>■ My Reports</li><li>■ Backups</li><li>■ Archives</li><li>■ Explorers</li><li>■ Costs</li><li>■ Customs</li></ul>
Alerts	<p>Use this tab to generate alerts depending on various alert conditions / policy types</p> <p>See <a href="#">“About alerts and the Alert Manager”</a> on page 295.</p> <p><b>Note:</b> Prior to VBR 6.6, the Alerts section was part of the Monitors section. In VBR 6.6, the reports and Knowledge Base available in the Monitors section have been moved under the Reports section.</p> <p>Click <b>Reports &gt; Explorers</b> to access Knowledge Base and reports that were previously in the Monitors section.</p> <p>See <a href="#">“About alerts and the Alert Manager”</a> on page 295.</p>
Costs	<p>Use this tab to define chargeback rates and formulas to establish and monitor IT costs for different levels of the organization</p> <p>See <a href="#">“Generating a cost report”</a> on page 460.</p>
Views	<p>Use this tab to display information about IT assets</p> <p>See <a href="#">“Creating views in Java View Builder”</a> on page 281.</p>
Settings	<p>Use this tab to customize the Veritas Backup Reporter Management Server, configure data collectors, define and manage user accounts</p> <p>The Settings tab consists of the following sub-tabs:</p> <ul style="list-style-type: none"><li>■ User Settings</li><li>■ Global Settings</li></ul>

## About the Veritas Backup Reporter console task pane

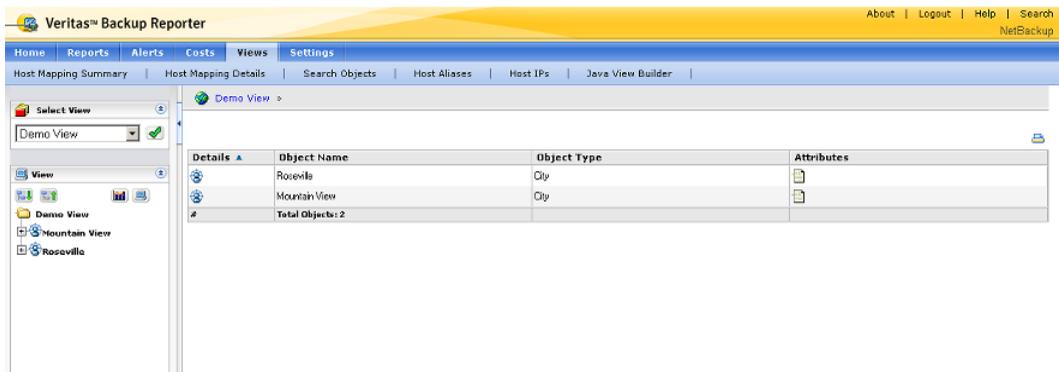
In most sections of the Veritas Backup Reporter console, a task pane on the left side of the console window serves as a navigation area, giving you quick access to specific tasks. The following figure shows the task pane for Global Settings.



## About the Veritas Backup Reporter console content pane

The main display area at the right-hand side or content pane displays information in a variety of tabular and graphical formats. The information displayed in the content pane is context-sensitive to current selections in the tabs and the task pane.

The following figure shows the content pane for the Views section.



## Accessing product Help

Veritas Backup Reporter offers a cross-platform, browser-based online help system.

---

**Caution:** VBR online Help may not be updated. For the most recent information about Veritas Backup Reporter, refer to the PDF (Portable Document Format) documents.

See [“About Veritas Backup Reporter documentation”](#) on page 31.

---

On UNIX computers, you can use manual pages to find reference and usage information about product-specific commands. When you install Veritas Backup Reporter, the `pkgadd` command installs the nroff-tagged manual pages in the appropriate directories under `/opt/VRTS/man`.

See [“Command and configuration file locator”](#) on page 519.

To ensure that new manual pages display correctly, update the following:

- `MANPATH` environment variable to point to `/opt/VRTS/man`

### To access VBR online Help

- ◆ Click **Help** in console header. This opens the help viewer in a new window. Use the Contents, Index, or Search tab to search for particular information related to Veritas Backup Reporter.

## Using the Symhelp search tool

Veritas Backup Reporter provides a next generation context-sensitive help search tool called Symhelp that you can use to search for a particular Veritas Backup Reporter topic.

---

**Caution:** Symhelp may not be updated. For the most recent information about Veritas Backup Reporter, refer to the PDF (Portable Document Format) documents.

See [“About Veritas Backup Reporter documentation”](#) on page 31.

---

### To use the Symhelp search tool

- 1 Click **Search** in the upper-right corner of the VBR console. This opens a new Symhelp search window.
- 2 Type text or phrase that you want to search for, in the text box. You can also type in a query regarding VBR. For example, ‘About agent’, ‘configuring a NetBackup data collector’, or simply ‘management server’.

**3** Click Search.

Alternatively, click a link in the Browse Help pane. This will populate the Topics pane with the related topics. Click any of the listed topics to view the information in the right pane.

**4** Use the options available in the right pane as follows:

Print	Click to print the topic.
Left arrow (<)	Click to go to the previous topic, if you have displayed multiple topics.
Right arrow (>)	Click to go to the next topic, if you have displayed multiple topics.

## Accessing NetBackup Operations Manager host

You can switch to another Symantec product, such as NetBackup Operations Manager (NOM) installed on a different host.

**To access NetBackup Operations Manager host from the VBR console**

- 1** In the VBR console, click **NetBackup** from the header.
- 2** Depending on whether you have configured the module links required for accessing other Symantec products, the steps vary explained as follows:
  - If you have already configured module links for accessing NOM, clicking the 'NetBackup' link launches NOM in the same window.
    - Enter the valid credentials and select the appropriate domain to logon to NOM.  
For more details on NOM, refer to the NOM documentation.
  - If you have not configured the module links before, clicking the 'NetBackup' link opens the Edit Module Link page.
    - Provide the required information to access NOM.

Protocol	Select 'http' or 'https'.
Host	Enter the NOM host name that you want to access. For example, 'NOMServer1'
Port	Enter the port number. Enter 8443 if you have selected the 'https'. This is the default port. Or enter 8181 if you have selected the 'http' protocol.

- Click **OK**. The Edit Module Link page is closed.
- On the VBR console, click **NetBackup** from the header. NOM is launched in the same window.
- Enter the valid credentials and select the appropriate domain to logon to NOM.  
For more details on NOM, refer to the NOM documentation.

# Configuring Veritas Backup Reporter Management Server

This chapter includes the following topics:

- [Editing links to Symantec products](#)
- [Configuring the data retention period](#)
- [Disabling demo database purging](#)
- [About changing the database password](#)
- [Backing up the Veritas Backup Reporter database](#)
- [Restoring the Veritas Backup Reporter database](#)
- [Configuring SMTP server using global system settings](#)
- [Defining view-level aliases](#)
- [Copying user-defined content](#)
- [Configuring Web server settings](#)
- [Modifying AT configuration manually](#)
- [About creating and importing views in XML](#)
- [Modifying the default export directory for scheduled reports](#)
- [Cleaning temporary files generated with reports](#)
- [Setting up trust relationships between Veritas Backup Reporter on hosts](#)

- [Managing Veritas Backup Reporter Management Server SSL certificates](#)
- [Managing licenses](#)
- [Managing user accounts](#)
- [Merging objects](#)

## Editing links to Symantec products

You can use the Veritas Backup Reporter console to perform various Management Server configuration tasks.

You can use the links in the Veritas Backup Reporter console header to navigate to other Symantec products, for example NetBackup Operations Manager (NOM). If all Symantec products are installed on the same host, you do not need to manually configure the links. However, if any of the products is installed on a different host, or if the default port for the product changes, you need to configure the URL. If the port or host changes after the initial configuration, you need to modify the URL settings.

### To edit links to Symantec products

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Module Links**.
- 4 On the Modify Module Links page, click the Edit icon to edit URL settings for a Symantec product.
- 5 From the Protocol drop-down list box, select one of the following:
  - `http`
  - `https (secure)`
- 6 In the Host text box, type a valid host name, fully qualified host name, or host IP address of the server, to which you want to connect using the module link.  
  
If you do not specify a host name, the system automatically clears the host and the port text boxes.

- 7 In the Port text box, type the port number to connect to the product server host.  
  
The default port number to connect to NOM Server host is '8443' for `https` protocol.  
  
If you do not specify port or protocol, the system uses the values in the URL that is in the address field of the Web browser.
- 8 Click **OK**.

## Configuring the data retention period

You can configure the Veritas Backup Reporter Management Server retention periods for data types that are logged, such as Job, Policy, and Skipped Files.

### To configure data retention period on the Veritas Backup Reporter Management Server

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Data Retention**.
- 4 In the Data Retention dialog box, type the number of days to retain the data in the Veritas Backup Reporter database.
- 5 Click **Save** to finish.

## Disabling demo database purging

The sample data that is shipped with Veritas Backup Reporter has database purging enabled. This means that when the management server starts, all media data is purged.

The Solaris sample database swap script prompts you to run the timeshift tool after the database is swapped, but before the management server restarts. You can enable or disable database purging at any time through the console.

---

**Warning:** Do not use this feature while connected to the Veritas Backup Reporter database in a production environment or else it can result in loss of important data.

---

### To disable demo database purging

- 1 Log on to a Veritas Backup Reporter management server on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings**.
- 3 Click **Data Retention**.
- 4 On the Data Retention Policies page, select the **Disable Purging** check box.
- 5 Click **Save**.

## About changing the database password

Using the `changedbpassword` utility, you can change password of the Veritas Backup Reporter database.

Veritas Backup Reporter uses the Sybase SA (Server Anywhere) database to store backup data. You require a user name and a password to access the data stored in the database.

Veritas Backup Reporter provides the following three database user accounts, which you can use to access the database:

guest	A read-only account with "guest" as a password. The guest account is not used by the management server.
ccsvc	An account used by the management server to access the database. This account owns all database tables of Veritas Backup Reporter.
dba	The database administrator account. The "dba" account is required by the database queries that are used to update the database schema, upgrade to a new release, and so on.

The location of the `changedbpassword` utility is as follows:

Windows	<code>&lt;serverInstallDir&gt;\util</code>
Solaris	<code>/opt/VRTSccsvs/bin/</code>

For more information on the `changedbpassword` utility, refer to:

.

## About changes in the `vbr_conf.properties` file

After changing the database password, the following new configuration property entries are added to the `vbr_conf.properties` file:

- `database.password.obfuscated.dba`
- `database.password.obfuscated.ccsvc`

These parameters store the obfuscated (encrypted) versions of the database passwords for the database administrator (DBA) and members of the `ccsvc_user` account.

If the `database.password.obfuscated.ccsvc` parameter is set in the `vbr_conf.properties` file, the server reads the obfuscated value, determines the password, and then uses the password for connecting to the database instead of using the default password.

---

**Note:** If the `vbr_conf.properties` file is missing or corrupt, or the database password for the DBA is missing from the file, the default database password for the DBA is used for changing the passwords. If the default password does not work, the `changedbpassword` utility prompts the user to specify the current database password of the DBA.

---

## About changes in the `support.exe` file

The Veritas Technical Support team uses the script in the `support.exe` file for collecting data required for troubleshooting purposes.

If the `changedbpassword` utility is run, `support` includes the updated `vbr_conf.properties` file when gathering information about the management server.

## Backing up the Veritas Backup Reporter database

Veritas Backup Reporter is shipped with a database backup script that performs backup of the database without interrupting its operations, which is referred to as hot backup. On Solaris as well as Windows platforms, the script overwrites existing database (db) files before backing up or restoring the database. The db files are as follows: `ccsvc.db` and `ccsvc.log`. The script backs up or restores the `ccsvc.log` file (if it exists).

---

**Note:** Regular filesystem backups are not sufficient for backing up the Veritas Backup Reporter database. You must schedule periodic hot backups for the Veritas Backup Reporter database to avoid losing any important data.

---

### To back up the Veritas Backup Reporter database

- 1 Log on to the Veritas Backup Reporter database server host in one of the following ways:

Solaris                      root

Windows                    As an administrator or user in the Administrator group

- 2 Open the Solaris console or Windows command prompt.
- 3 Run the backup script that is appropriate for your platform. Specify one of the following backup directories depending on your platform:

Solaris                      /opt/VRTSccsvs/bin/dbbackup /my\_db\_backup\_dir

Windows                    C:\Program Files\Symantec\Veritas Backup  
Reporter\Server\util\DbBackup.bat  
C:\MyDbBackupFolder

The backup script creates `ccsvc.db` and `ccsvc.log` (if it exists) in the backup directory that you specified.

## Restoring the Veritas Backup Reporter database

After you backup the database, you can restore it. On Solaris hosts, the restore operation automatically stops the database, restores the backup database files, and restarts the database. On Windows hosts, you issue a series of commands that stop the database, restore individual backup database files, and restart the database. On Solaris as well as Windows platforms, the script overwrites existing database (db) files before backing up or restoring the database. The db files are as follows: `ccsvc.db` and `ccsvc.log`. The script backs up or restores the `ccsvc.log` file (if it exists).

### To restore a backed up Veritas Backup Reporter database

- 1 On the management server whose backup data you want to restore, open a UNIX console or a Windows command prompt and log in as `root` (on UNIX) or as an administrator or user in the Administrators group (on Windows).

Solaris                    Open a Solaris console and then log in as `root`.

Windows                  Open a Windows command prompt and log in as an administrator or user in the Administrators group.

All the paths shown in the steps that follow are the default database install paths. These paths may differ for your site if the database was installed anywhere other than the default location.

- 2 To stop all Veritas Backup Reporter processes, do one of the following:

Solaris                    Type the following command and press **Enter**.

```
/opt/VRTS/bin/vbrserver stop force
```

Windows                  Use the Windows Service Control Manager (SCM) to stop all Veritas Backup Reporter services.

Alternatively, you can also use the following commands to automatically stop all Veritas Backup Reporter processes:

```
<INSTALDIR>\Tools
```

```
cscript vx_services_stop.vbs
```

**3** To restore the backed up database, do one of the following:

Solaris                   Type the following command and press **Enter**.  
  
                          `/opt/VRTSccsvs/bin/dbbackup <backupDir> -restore  
                          <restoreDir>`

Windows                 Type the following command and press **Enter**.  
  
                          `C:\Program Files\Symantec\Veritas Backup  
                          Reporter\Server\util\DbBackup.bat <backupDir>  
                          -restore <restoreDir>`

where *backupDir* is the directory where the backed up database resides, and  
<restoreDir> is the location of the current Veritas Backup Reporter database.

*restoreDir* is optional.

If not used, `vxcc_db_backup` and `DbBackup.bat` restores to the default  
database directory:

Solaris                   `/var/VERITAS/ccs_data`

Windows                 `C:\Program Files\Symantec\Veritas Backup  
                          Reporter\DB\Data`

If you specified a non-default directory location, you must specify the  
*restoreDir* option.

The script prompts you with a message similar to the following:

```
WARNING: this operation will overwrite the active  
Veritas Backup Reporter data on this host.  
Do you wish to continue ? [y/n] (n)
```

- 4 To continue with the restore, type **y**.  
`vx_ccdb_backup` and `DbBackup.bat` automatically stops and restarts the database.
- 5 To restart all Veritas Backup Reporter processes, do one of the following:

Solaris Type the following command and press **Enter**.

```
/opt/VRTS/bin/vbrserver
```

Windows Use the Windows Service Control Manager (SCM) to start all Veritas Backup Reporter services.

Alternatively, you can also use the following commands to automatically start all Veritas Backup Reporter processes:

```
<INSTALLDIR>\Tools
```

```
cscript vx_services_start.vbs
```

## Configuring SMTP server using global system settings

You can configure your own settings for the Veritas Backup Reporter console and apply them globally for all users.

### To configure global system settings for the Veritas Backup Reporter console

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **System Settings**.

The SMTP server details that you see on this page have already been entered while installing VBR. You can modify these settings using this section.

VBR uses these global server settings to send email notifications using the SMTP Server that you specify here, with anonymous access.

4 Edit the following default information:

System Name	Change the title that you want to appear on the title bar of the Veritas Backup Reporter UI.
SMTP Server Name	Change the SMTP (Simple Mail Transfer Protocol) Server host name that you have entered while installing the Veritas Backup Reporter application.  Notifications of alerts generated in Veritas Backup Reporter are sent using this SMTP server.  See <a href="#">“About alerts and the Alert Manager”</a> on page 295.
Email Address	Modify the default email ID (no-reply@symantec.com). The email notifications are sent with this email ID as the sender email ID. For example, enter alerts@symantec.com
Email Address Name	Modify the name associated with the email ID. For example, Backup Reporting Department

5 Click **Save**.

## Defining view-level aliases

You can specify aliases of various levels of an object view’s tree structure. The aliases replace the default labels, such as Level 1 and Level 2 that appear in the Custom Report Wizard.

### To define view-level aliases

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Alias View Levels**.
- 4 Select an object view from the View Name drop-down list.
- 5 Type an alias for a level of the object view.
- 6 Click **Save**.

## Copying user-defined content

Most user-definable content, such as reports, folders, tables, schedules, cost variables, and cost formulas, is accessible only by the user who has created it.

Using the copy user profile functionality, you can copy information from one user account to another.

---

**Note:** You must have administrator privileges to copy reports that are not based on views. To run view-based reports you need to have at least administrator (read-only) privileges.

---

#### To copy user-definable content

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Copy User Profile**.
- 4 Select the source user account from the From drop-down list box.
- 5 Select the target user account from the To drop-down list box.
- 6 Select the Process in background check box to copy the user profile in the background. This option lets you work on other tasks in the console while user profile is being copied in the background.
- 7 Type the email address in the Notification Email Address text box. After all user information is copied to the target user account in the background, the notification is sent to the specified email address.
- 8 In the Copy Items window, do one of the following:
  - Select the items you want to copy, for example reports or cost rates and formulas.
  - Click **Select All** to select all items at once.
- 9 Click **Next**.
- 10 Click **Save** to finish.

## Configuring Web server settings

This section provides procedures to configure the following Web server settings.

### Configuring the SMTP server

This section provides the procedure to change the SMTP server configuration using the Web server console.

---

**Note:** However, VBR uses the SMTP server configured in the **Global Settings > System Settings** section, to send email notifications.

See [“Configuring SMTP server using global system settings”](#) on page 137.

---

#### To configure the SMTP server

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Web Console Configuration**.
- 4 In the Symantec Web server console, click **Configure SMTP Server**.

The details that you see on this page have already been entered while installing VBR. You can modify these SMTP server settings. However, email notifications are sent through the SMTP server specified in the **Global Settings > System Settings** section.

See [“Configuring SMTP server using global system settings”](#) on page 137.

- 5 Type the necessary information in the following fields:

SMTP server	Type the name of the SMTP server.
Domain	Type the domain to which the SMTP server belongs.
Username and password	Enter the user account information (user name and password), using which you can connect to the SMTP server.

- 6 Click **OK**.

## Changing the Web server port

You may need to change the default port that is, the Symantec Web server port or Web server port used by the Veritas Backup Reporter Management Server to communicate with the Veritas Backup Reporter console.

---

**Note:** Before deleting an old port, you must add a new port.

---

---

**Note:** The Veritas Backup Reporter Agent and a few other Veritas Backup Reporter components use a port other than the Symantec Web server port to communicate with the Veritas Backup Reporter Management Server.

---

#### To add a new port

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Web Console Configuration**.
- 4 In the Symantec Web Server console, click **Add Port**.
- 5 Enter the following information:

Port Number	Type the Web server port number that will be used by the Veritas Backup Reporter Management Server.  See <a href="#">“About configuring Veritas Backup Reporter firewall”</a> on page 46.
Protocol	Select one of the following: <ul style="list-style-type: none"><li>■ http (unsecured)</li><li>■ https (secure)</li></ul>
IP Address	Type the IP address of the Web server.
Domain	Type the domain to which the Web server belongs.
User and Password	Enter the user account information (user name and password), using which you can connect to the server.

- 6 Click **OK**.

#### To delete an old port

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Web Console Configuration**.
- 4 In the Symantec Web Server console, click **Delete Port**

5 Type the following information:

Port Number	Type the port number that you want to delete. You cannot delete the port being used to access the Web page. See <a href="#">“About configuring Veritas Backup Reporter firewall ”</a> on page 46.
IP Address	Type the IP address that is bound to the port.
Domain	Type the domain to which the Web server belongs.
User and Password	Enter the user account information (user name and password), using which you can connect to the Web server.

6 Click **OK**.

## Configuring Veritas Backup Reporter Management Server logging

You can change Veritas Backup Reporter Management Server logging by using the Veritas Backup Reporter console.

### To configure Veritas Backup Reporter Management Server logging

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Web Console Configuration**.
- 4 In the Veritas Web Server console, click **Configure Logging**.
- 5 In the Web Applications drop-down list, select one of the following log levels:
  - Fine
  - Finer
  - Finest
  - Config
  - Info
  - Warning
  - Severe

Set the level to a lower value to generate more logs. Finest is the lowest level while Severe is the highest level.

6 Click **OK**.

## Modifying AT configuration manually

In Veritas Backup Reporter (VBR), you can configure Symantec Product Authentication Service (AT) during installation or modify the configuration later.

See [“About AT configuration in Veritas Backup Reporter”](#) on page 54.

The AT Root broker can be present on the VBR Management Server host or an external host.

This section describes how you can modify the AT configuration after installing Veritas Backup Reporter, to communicate with product hosts. You need to modify the AT configuration in the following scenarios:

Upgrading VBR Management Server from AB > Root + AB mode

In certain scenarios, you may want to upgrade the AT configuration of VBR Management Server. For example:

- You have installed the VBR Management Server in AB (Authentication Broker) mode pointing to the AT Root configured on an external host for example, PureDisk SPA
- You want to change this AT configuration from external to local Root Broker for VBR Management Server.

In this case, you should upgrade VBR Management Server from AB > Root + AB mode.

See [“Upgrading VBR Management Server from AB > Root + AB”](#) on page 144.

This implies that you need to downgrade the PureDisk SPA from Root + AB mode to AB, pointing the Root configured on VBR Management Server.

If you are moving the Root Broker of PureDisk SPA to the VBR Management Server or any other external / remote host, create Principal user on the this remote or Management Server host and modify the AT configuration on the PureDisk SPA host.

See [“Moving the Root Broker from PureDisk SPA host to VBR Management Server”](#) on page 230.

**Note:** For the most recent information on modifying the AT configuration in PureDisk, refer to the PureDisk documentation.

Downgrading VBR Management Server from Root + AB > AB mode

In certain scenarios, you may want to downgrade the AT configuration of VBR Management Server. For example:

- You have installed the VBR Management Server in Root + AB mode
- You want to collect data from PureDisk SPA (Storage Pool Authority)
- PureDisk SPA is in Root + AB mode
- You want to point VBR Management Server to the Root Broker on PureDisk SPA

In this case, you should downgrade VBR Management Server from Root + AB > AB mode.

See [“Downgrading VBR Management Server from AB > Root + AB or moving the remote Root”](#) on page 146.

Changing the remote Root of VBR Management Server

In certain scenarios, you may want to change the remote Root of the VBR Management Server. For example:

- VBR Management Server is installed in AB mode pointing to the Root that is configured on a host called ‘Server1’.
- You want to change the remote Root and point the VBR Management Server to the root that is configured on a host called ‘Server2’.

See [“Downgrading VBR Management Server from AB > Root + AB or moving the remote Root”](#) on page 146.

## Upgrading VBR Management Server from AB > Root + AB

This section describes how to upgrade the VBR Management Server from AB > Root + AB mode.

**To upgrade VBR Management Server from AB > Root + AB**

- 1 Logon to the VBR Management Server host and run the following command from the command prompt:

Windows `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Server\Util\configure_external_rootbroker.bat local`

Solaris `<INSTALL_DIR>/VRTSccsvs/bin/configure_external_rootbroker.sh local`

To change the Root of PureDisk and point it to Root Broker configured on the VBR Management Server host, you need to add a Principal user on the Management Server host and specify its credentials on the PureDisk SPA host. For more details on changing the AT configuration of PureDisk SPA, refer to the PureDisk documentation.

- 2 Delete the directory containing the certificate pointing to the old root broker by running the following command on all agent hosts configured for the current management server:

Windows `rd /s /q [INSTALL_DIR]\Symantec\Veritas Backup Reporter\EmbeddedAT\4.4.110.4\data`

Solaris `rm -rf /opt/VRTSbrat/data`

- 3 Start all services by running the following commands:

Windows

- `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Tools\net start vbrserver`
- `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Tools\net start vbrcorbaserver`
- `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Tools\net start vbragent`

Solaris

- `/<INSTALL_DIR>/VRTSccsvs/bin/vbrserver start`
- `/<INSTALL_DIR>/VRTSccsva/bin/vbragent start`

- 4 After changing the AT configuration on the VBR Management Server host, you need to update the Authentication Broker information on all the Agent hosts that are connected to this Management Server host.

Run the following command on the VBR Agent host to update the Authentication Broker information:

```
Agentauth -server ABHostName
```

Where *ABHostName* is the host name where authentication broker is configured, in this case it is the VBR Management Server host name.

- 5 To verify the execution of the script run the following command:

```
Windows vssat showcred
```

```
Solaris /<INSTALL_DIR>/VRTSat/bin/vssat showcred
```

This command shows at least five users.

## Downgrading VBR Management Server from AB > Root + AB or moving the remote Root

This section describes how to downgrade VBR Management Server from Root + AB > AB, when you want the Management Server to point to a Root Broker installed on a remote host. You can use the same procedure if you want to move the remote Root Broker of VBR Management Server to a new host. In both these scenarios, you need to create a principal user on the remote Root Broker host. The VBR Management Server AB will point to this Root Broker, using the credentials of this principal user.

### To downgrade VBR Management Server from AB > Root + AB or move the remote Root to a new host

- 1 Logon to the remote Root Broker host as an administrator or a super user, which you want the VBR Management Server to point to.
- 2 Open the command prompt and run the following command:

```
Windows <INSTALL_DIR>\VERITAS\Security\Authentication\bin\vssat showcred
```

```
Solaris /<INSTALL_DIR>/VRTSat/bin/vssat showcred
```

- 3 Find the root domain name of the remote Root Broker host by running the following command: `vssat listpd --pdrtypes root`

For example, the root domain name is `root@root IP/host name`, where `root IP/host name` is referred to as root node or root broker host.

Example output:

```
Domain(s) Found 1
Domain Name root@PDServer1.myline.com
Expiry Interval 0
```

If the Root Broker is not configured on this host, this command does not return any output.

- 4 Create the authentication broker identity in the root domain with the following command: `vssat addprpl --prplname <broker identity name, for example Management Server host name>--password <broker identity password>--pdrtypes root --domain <root domain name provided by running vssat listpd --pdrtypes root command>--prpltype service`

For example:

```
vssat addprpl --prplname VBRServer1--password myPassword--pdrtypes
root --domain PDServer1.myline.com--prpltype service
```

The name of the Root Broker hash file is `root_hash`. It resides at the following location on the remote Root Broker host:

```
<INSTALL_DIR>\VERITAS\Security\Authentication\bin
```

- 5 Copy the root hash file from the remote Root Broker host to the Management Server host. The root hash file is a binary data. Therefore, you should copy the root hash file in the binary mode. The destination directory can be any directory on the target Management Server host.

Do not overwrite the existing `root_hash`, copy it in an alternate location

## 6 Run the following command:

Windows	<pre>&lt;INSTALL_DIR&gt;\Symantec\Veritas Backup Reporter\Server\Util\configure_external_rootbroker.bat -identity &lt;broker_identity_name&gt; -password &lt;broker_identity_password&gt; -rootbrokerhost &lt;broker_host_name&gt; -roothashfile &lt;root_broker_hashfile_location&gt;</pre>
Solaris	<pre>&lt;INSTALL_DIR&gt;/VRTSccsvs/bin/configure_external_rootbroker.sh -identity &lt;broker_identity_name&gt; -password &lt;broker_identity_password&gt; -rootbrokerhost &lt;broker_host_name&gt; -roothashfile &lt;root_broker_hashfile_location&gt;</pre>

**For example:** `configure_external_rootbroker.bat -identity vbrroot -password Symantec -rootbrokerhost PureDiskServer1 -roothashfile C:\root_hash`

## 7 Delete the directory containing the certificate pointing to the old root broker by running the following command on all agent hosts configured for the current management server:

Windows	<pre>rd /s /q [INSTALL_DIR]\Symantec\Veritas Backup Reporter\EmbeddedAT\4.4.110.4\data</pre>
Solaris	<pre>rm -rf /opt/VRTSbrat/data</pre>

## 8 Start all services by running the following command:

Windows	<ul style="list-style-type: none"><li>■ <code>&lt;INSTALL_DIR&gt;\Symantec\Veritas Backup Reporter\Tools\net start vbrserver</code></li><li>■ <code>&lt;INSTALL_DIR&gt;\Symantec\Veritas Backup Reporter\Tools\net start vbrcorbaserver</code></li><li>■ <code>&lt;INSTALL_DIR&gt;\Symantec\Veritas Backup Reporter\Tools\net start vbragent</code></li></ul>
Solaris	<ul style="list-style-type: none"><li>■ <code>/&lt;INSTALL_DIR&gt;/VRTSccsvs/bin/vbrserver start</code></li><li>■ <code>/&lt;INSTALL_DIR&gt;/VRTSccsva/bin/vbragent start</code></li></ul>

- 9** After changing the AT configuration on the VBR Management Server host, you need to update the Authentication Broker information on all the Agent hosts that are connected to this Management Server host.

Run the following commands on the VBR Agent host to update the Authentication Broker information:

- Windows `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Tools\net stop vbragent`
- Solaris `/<INSTALL_DIR>/VRTSccsva/bin/vbragent stop`

- `Agentauth -server ABHostName`

Where *ABHostName* is the host name where authentication broker is configured, in this case it is the VBR Management Server host name.

- Windows `<INSTALL_DIR>\Symantec\Veritas Backup Reporter\Tools\net start vbragent`
- Solaris `/<INSTALL_DIR>/VRTSccsva/bin/vbragent start`

- 10** To verify the execution of the script run the following command:

- Windows `vssat showcred`
- Solaris `/<INSTALL_DIR>/VRTSat/bin/vssat showcred`

This command shows at least five users.

- 11** Before starting the data collector configuration, find out the broker host name by executing the following command:

- Windows `<INSTALL_DIR>\VERITAS\Security\Authentication\bin\vssat showcred`
- Solaris `/<INSTALL_DIR>/VRTSat/bin/vssat showcred`

## About creating and importing views in XML

You can use the Veritas Backup Reporter console to create views, but you may find it faster and more convenient to create XML files that describe the views you want to create. You can then import the XML into Veritas Backup Reporter.

Veritas Backup Reporter provides an XML utility to import and export your XML files.

This utility resides in the following locations on the Veritas Backup Reporter Management Server host:

Solaris	<code>&lt;serverInstallDir&gt;/bin/xml.sh</code>
Windows	<code>&lt;serverInstallDir&gt;\util\xml.bat</code>

Run the utility with no arguments to view a command usage summary.

## Modifying the default export directory for scheduled reports

The `exportDirectoryPrefix` setting in the `vbr_conf.properties` file controls the default export path (Directory Prefix) that Veritas Backup Reporter console users see when they attempt to save scheduled reports (**Settings > Email/Export Reports > Edit**).

See [“Exporting reports”](#) on page 443.

The export reports option allows Veritas Backup Reporter administrators to confine users to a specific export directory, preventing them from exporting the reports to any arbitrary and potentially harmful system directory. If `exportDirectoryPrefix` is not defined, Veritas Backup Reporter defaults to whatever is defined in `web.xml`, or in one of the following Veritas Backup Reporter Management Server directories.

- On Solaris: `/opt/VRTSccsvs/web/vbr/temp`
- On Windows: `\Program Files\Symantec\Veritas Backup Reporter\Server\web\vbr\temp`

If the specified prefix directory is not present on the host, the Veritas Backup Reporter Management Server creates it.

**To modify the default export directory for scheduled reports**

- 1 On the Veritas Backup Reporter Management Server on which you want to change the default export path, do one of the following:

Solaris                    Open a Solaris console and log in as `root`

Windows                 Open a Windows command prompt and log in as an administrator or a user in the Administrators group.

- 2 Using a text editor, open `vbr_conf.properties` in the following default location for your platform:

Solaris                    `/opt/VRTSccsvs/conf`

Windows                 `\Program Files\Symantec\Veritas Backup Reporter\Server\conf`

- 3 Using a text editor, search for the following string:

`exportDirectoryPrefix=`

If the string is not present, add it.

- 4 Type a valid path that exists on the Veritas Backup Reporter Management Server.

For example on Solaris:

`exportDirectoryPrefix=/var/reports`

For example on Windows:

`exportDirectoryPrefix=C:\Shared\Reports`

On Windows systems, you must insert an extra backslash since the configuration information is stored in a Java properties file.

- 5 Save your changes and close `vbr_conf.properties`.
- 6 When you modify `vbr_conf.properties` file, you must restart the Veritas Backup Reporter Management Server to commit your changes, as follows:

Solaris                    Type one of the following commands:

- `/opt/VRTSccsvs/bin/vbrserver stop`
- `/opt/VRTSccsvs/bin/vbrserver start`

Windows                 Use the Services application to restart the Veritas Backup Reporter Management Server.

## Cleaning temporary files generated with reports

While generating a report, the system creates other related information, such as report images and html files. These temporary files are stored in the following locations on the Veritas Backup Reporter Management Server host:

Solaris                    <serverInstallDir>/web/vbr/temp/reports

Windows                <serverInstallDir>\server\web\vbr\temp\reports

With each new report, the size of the `reports` directory increases. Veritas Backup Reporter provides a means to periodically delete the temporary files and clean the `reports` directory. The Report Clean Up Schedule, which is shipped with default settings, which runs internally and deletes all temporary files that are generated in the `reports` directory.

The `application.properties` file contains the location of the `reports` directory.

---

**Note:** Only temporary files that are older than a day are deleted.

---

The administrator can edit the Report Clean Up Schedule.

### To clean temporary files

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings**.
- 3 On the Settings tab, click **Schedules**.
- 4 Select the check box in front of the Report Clean Up Schedule.
- 5 Click the Edit icon.
- 6 Edit schedule or recurrence pattern as required.

---

**Note:** Do not delete the Report Clean Up Schedule.

---

- 7 Click **Save**.

# Setting up trust relationships between Veritas Backup Reporter on hosts

If you have installed the Web servers of multiple Symantec products on different hosts, you must configure the Symantec Product Authentication Service to allow the authentication brokers to exchange information. Configuring these authentication broker trusts allows cross-product linking in the Veritas Backup Reporter console without additional user logins.

Using the Symantec Product Authentication Service command-line interface, `vssat`, you can set up trust relationships between each pair of hosts.

**Note:** You must perform this procedure for each pair of hosts. For example, if you have Veritas Backup Reporter installed on host A, NetBackup Operations Manager (NOM) installed on host B, and Command Central Storage installed on host C, perform this procedure three times, once for the A-B pair, again for the B-C pair, and a third time for the C-A pair.

[Table 4-1](#) lists the Veritas product component for which you must set up trusts.

**Table 4-1** Symantec product component hosts that require trust relationship

Symantec product	Product component host on which to establish trust
NetBackup Operations Manager	NOM Management Server
Veritas Backup Reporter	Veritas Backup Reporter Management Server
CommandCentral Storage	CommandCentral Storage Web Engine

## To set up trust relationships

- 1 On the Veritas product host on which you want to set up a trust relationship (see [Table 4-1](#)), do one of the following:

Solaris                      Open a Solaris console and log in as `root`

Windows                    Open a Windows command prompt and log in as an administrator or a user in the Administrators group .

- 2 Change to the Symantec Product Authentication Service CLI (`vssat`) directory. The default is one of the following:

- On Solaris: `/opt/VRTSat/bin`

- **On Windows:** \Program Files\Veritas\Security\Authentication\bin

**3** Type the following command, and then press **Enter**:

```
vssat setuptrust -broker remoteHost:2821 -securitylevel low
```

where <remoteHost> is either a host name, qualified domain host name, or host IP address of the remote host with which you are establishing the trust.

The entry 2821 is the registered port number for Symantec Product Authentication Service.

**4** Repeat steps 1–3 for the second host.

#### To view a list of hosts trusted by the local host

- ◆ On the appropriate Symantec product host on which you have administrator privileges, type the command appropriate for the operating system, and then press **Enter**:

Solaris                    /opt/VRTSat/bin/vssat showalltrustedcreds

Windows                 \Program  
                          Files\Veritas\Security\Authentication\bin\vssat  
                          showalltrustedcreds

After removing a trust, restart Symantec Product Authentication Service before the changes take effect.

#### To remove trust relationships

**1** On the Veritas product host (see earlier table) on which you want to remove a trust relationship,

Solaris                    Open a Solaris console and log in as `root`

Windows                 Open a Windows command prompt and log in as an administrator or as a user in the Administrators group.

**2** Change to the Symantec Product Authentication Service CLI (`vssat`) directory.

The default is one of the following:

- **On Solaris:** /opt/VRTSat/bin

- **On Windows:** \Program Files\Veritas\Security\Authentication\bin

- 3 Type the following command, and then press **Enter**:

```
vssat removetrust -broker remoteHost:2821
```

where <remoteHost> is either a host name, qualified domain host name, or host IP address of the remote host with which you are establishing the trust.

The entry 2821 is the registered port number for Symantec Product Authentication Service.

- 4 Repeat steps 1-3 for the second host.
- 5 Restart the Veritas Backup Reporter Management Server on the hosts on which you removed the trusts:

Solaris                    /opt/VRTSccsvs/bin/vbrweb restart

Windows                Using the Windows Services application, restart the Veritas Backup Reporter Management Server.

## Managing Veritas Backup Reporter Management Server SSL certificates

The Veritas Backup Reporter Management Server uses Secure Sockets Layer (SSL) to communicate with Web browser clients. The keystore certificate with which the Web Engine ships causes your Web browser to display a security alert. You can delete this certificate and generate one appropriate for your site.

When serving content over the secure port, the Veritas Backup Reporter Management Server presents a self-signed SSL certificate (issued by Veritas) to the browser. Unless you generate a new certificate, your Web browser displays a security alert.

---

**Note:** Certificate management commands are available only via the command-line interface. Commands that modify the certificate require a Server restart.

---

### Viewing SSL certificate information

You can view SSL certificate information.

### To view information about the configured SSL certificate

- ◆ Run the following command on the computer where the Veritas Backup Reporter Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui cert display
```

where the default locations for %VRTSWEB\_HOME% are as follows:

Solaris            /opt/VRTSweb

Windows         C:\Program Files\VERITAS\VRTSweb

## Creating a self-signed SSL certificate

You can create a custom self-signed SSL certificate for Veritas Backup Reporter Management Server and the CommandCentral Storage Web Engine.

### To create a self-signed SSL certificate

- ◆ Run the following command on the system where the Veritas Backup Reporter Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui cert create
```

The command guides you through the process of creating a new certificate.

Please answer the following questions to create a self-signed certificate.

This is required to enable the HTTPS protocol for the web server.

+++++

With what hostname/IP will you access this web server?

[thor106]:**thor106**

What is the name of your organizational unit?

[Unknown]:**Engineering**

What is the name of your organization? [Unknown]:**Your Company**

What is the name of your City or Locality? [Unknown]: **Mountain View**

What is the name of your State or Province? [Unknown]:**California**

What is the two-letter country code for this unit? [Unknown]:**US**

Is CN=thor106, OU=Engineering, O=Your Company, L=Mountain View, ST=California, C=US correct? [no]:**yes**

Certificate created successfully

You must restart the server for the new certificate to take effect.

## Exporting an SSL certificate to a file

You can export the public key associated with an SSL certificate to a file. This key can then be imported into other applications that trust the Veritas Backup Reporter Management Server instance. If the Veritas Backup Reporter Management Server SSL certificate does not exist, the command prompts you to create one. If you specify the RFC option, the key output is encoded in a printable format, defined by the Internet RFC 1421 standard.

### To export an SSL certificate to a file

- ◆ Run the following command on the system where the Veritas Backup Reporter Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui cert export<cert_file>[rfc]
```

For example:

```
%VRTSWEB_HOME%\bin> webgui cert export C:\myapp\vrtsweb.cer rfc
```

## Configuring a CA-signed SSL certificate

By default, Veritas Backup Reporter Management Server presents a self-signed SSL certificate every time you access Veritas Backup Reporter Management Server over the SSL port. You can install a certificate signed by a Certificate Authority (CA) like Verisign.com or Thawte.com.

### To configure a CA-signed SSL certificate

- 1 If you do not have a self-signed certificate with information that can be verified by the CA, create one by running the following command:

```
%VRTSWEB_HOME%\bin>webgui cert create
```

See [“Creating a self-signed SSL certificate”](#) on page 156.

- 2 Generate a Certificate Signing Request (CSR) for the certificate by running the following command on the system where Veritas Backup Reporter Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui cert certreq <certreq_file>
```

where <certreq\_file> specifies the file to which the CSR is written. The file is written using the Public-Key Cryptography Standard PKCS#10.

For example:

```
%VRTSWEB_HOME%\bin> webgui cert certreq c:\myapp\vrtsweb.csr
```

- 3 Submit the CSR to a certification authority, which then issues a CA-signed certificate.

- 4 Import the CA-issued certificate to Veritas Backup Reporter Management Server by running the following command on the system where Veritas Backup Reporter Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui import <ca_cert_file>
```

where <ca\_cert\_file> represents the certificate issued to you by the certification authority.

For example:

```
%VRTSWEB_HOME%\bin>webgui cert import c:\myapp\vrtsweb.cer
```

Note that the import command fails if the CA root certificate is not a part of the trust store associated with the Veritas Backup Reporter Management Server. If the command fails, add the CA root certificate to Veritas Backup Reporter Management Server trust store by running the following command:

```
%VRTSWEB_HOME%\bin>webgui cert trust ca_root_cert_file
```

For example:

```
%VRTSWEB_HOME%\bin>webgui cert trust c:\myapp\caroot.cer
```

Once the certificate used to sign the CSR is added to the Veritas Backup Reporter Management Server trust store, you can import the CA-assigned certificate into Veritas Backup Reporter Management Server.

- 5 Restart the Veritas Backup Reporter Management Server by running the following command:

```
%VRTSWEB_HOME%\bin>webgui restart
```

## About cloning SSL certificates

You can clone the Veritas Backup Reporter Management Server SSL keypair into a keystore and use the cloned Veritas Backup Reporter Management Server and the Web Engine certificate for another application or Web server. Visit <http://java.sun.com> for more information about keystores.

```
%VRTSWEB_HOME%\bin> webgui cert clone <keystore> <storepass> <alias>  
<keypass>
```

If a clone keystore exists, the command renames it to keystore.old. If the Veritas Backup Reporter Management Server SSL certificate does not exist, the command prompts you to create one.

For example:

```
%VRTSWEB_HOME%\bin>webgui cert clone  
c:\myapp\myserv.keystoremystorepass myalias mykeypass
```

# Managing licenses

This section describes procedures to manage license keys from the Veritas Backup Reporter UI.

## About licensing model

In Veritas Backup Reporter 6.6, the licensing model is modified to accommodate the new Enterprise Vault support.

---

**Note:** If you want to collect archive or Enterprise Vault data, you need to add a new license key that is valid for archive data collection, during upgrade.

---

Earlier, the licenses were charged depending on the number of backup clients that Veritas Backup Reporter was to report on. In Veritas Backup Reporter 6.6, one more component has been added in the licensing model, that is the number of mailboxes that you want VBR to report on.

For example: You have a VBR - NetBackup set up with 100 backup clients and VBR - Enterprise Vault set up with 500 mailboxes to report on. You need to purchase a license that enables you to report on 100 backup clients and 500 mailboxes.

While installing Veritas Backup Reporter, if you install Symantec Enterprise Vault enabled licensing key, a new license option called Symantec Enterprise Vault is added. This is visible in the Veritas Backup Reporter console, on the **Settings > Global Settings > Licensing** page as shown in the following figure:

If you have a license for 1000 mailboxes, it is added as 'Archived Mailboxes 1000' as shown in the figure.

Settings > Global Settings > Licensing

Add new License Key:

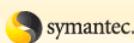
Licenses currently installed on the system:

Key	Type	Expiration Date
<input type="checkbox"/> A2C9-GNRO-CMPT-4B42-FEP6-3WOT-4C6N-FECC-PNY	DEMO	Mon Mar 16 00:00:00 IST 2009

License Option	Licensed	Current
Hide Tabs	false	
Settings	true	
Costs	true	
Monitoring	true	
Reporting	true	
Views	true	
Backup Clients	1000	✔ Total : 0
Archived Mailboxes	1000	✔ Total : 0
IBM Tivoli Storage Manager	true	
CommVault Galley	true	
EMC NetWorker	true	
Backup	true	
Symantec Backup Exec	true	
Veritas PureDisk	true	
Symantec Enterprise Vault	true	
Veritas NetBackup	true	

These two entries show that the license to collect archive data of 1000 mailboxes from Enterprise Vault is installed.

If the number of mailboxes that you have configured exceeds the license limit, the following message is displayed when you try to logon to the Veritas Backup Reporter console.



**Number of backup clients (8) exceeds the license limit (4) and number of archived mail boxes (5) exceeds the license limit (1)  
 You have been successfully logged out**

 **Veritas™ Backup Reporter**  
 Version: 6.6

User Name :   
 Password :   
 Domain :

Copyright © 2008 Symantec Corporation. All rights reserved.

## Adding license keys

An administrator can install Veritas Backup Reporter license keys to activate additional product features or delete license keys that are no longer needed.

You can add one or more Veritas Backup Reporter license keys to the VBR Management Server to which you are connected as an administrator.

### To add Veritas Backup Reporter license keys

- 1 In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings**.
- 3 Click **Licensing**.
- 4 In the Add new License Key text box, type a valid Veritas Backup Reporter license key.  
For more information, click **Help**.
- 5 Click **Add Key**.

## Viewing license keys

You can view license keys installed on the VBR Management Server host, on which you are connected.

### To view Veritas Backup Reporter license keys

- 1 In the VBR console, log on to the VBR Management Server host, on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings**.
- 3 Click **Licensing**.

## Deleting license keys

You can remove one or more Veritas Backup Reporter license keys from the VBR Management Server, on which you are connected as an administrator.

### To delete Veritas Backup Reporter license keys

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Licensing**.
- 4 Select the check box next to the license key you want to delete.
- 5 Click **Delete**.
- 6 A confirmation message appears. On the confirmation message box, select one of the following:
  - Click **OK** to confirm the delete operation.
  - Click **Cancel** to stop the delete operation.

## Managing user accounts

After you install Veritas Backup Reporter, you need to create user accounts. The Symantec Product Authentication Service validates credentials of Veritas Backup Reporter users based on NT, NIS, or private domains.

You can either add existing users present in various domains to Veritas Backup Reporter or create users in the private cc\_users domain.

---

**Note:** You should immediately create one or more administrator accounts to replace the default administrator account that is shipped with Veritas Backup Reporter.

---

### Adding existing domain users to Veritas Backup Reporter

You can add users that are already in various domains, to Veritas Backup Reporter.

#### To add an existing user to Veritas Backup Reporter

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click **Add User**.

- 5 In the New User Details page, type information of a user, such as first name, last name, domain name, access level, email, department, cost center, and contact details in the corresponding fields.

Most fields are optional; however, the following fields are mandatory:

Login	Enter the login name of a user.
Domain Name	Select a domain name from the drop-down list, such as <code>root@hostame (vx)</code> , <code>cc_users@hostname (vx)</code> , or <code>VSS (ldap)</code> where <i>hostname</i> is the name of the VBR Management Server.
Access Level	Select User, Administrator (Read Only), or Administrator.  Administrator has read and write privileges on all Veritas Backup Reporter functions.  Administrator (Read Only) has read privileges on all functions of Veritas Backup Reporter.  User has read and write privileges on limited functions of Veritas Backup Reporter.

- 6 Click **Save**.

## Creating a private domain user account

After installing Veritas Backup Reporter, you need to create user accounts. The Symantec Product Authentication Service validates user credentials in Veritas Backup Reporter based on NT, NIS, or private domains.

---

**Caution:** Creating private domain user accounts is not recommended. You should use existing systems, such as AD, LDAP, NT or NIS.

---

If you are implementing a private domain, create Veritas Backup Reporter users with the Create Private Domain User option. If you are authenticating users based on an existing NT, NIS, or localhost domain, use the Add User option.

---

**Note:** You should immediately create one or more administrator accounts to replace the default administrator account that is shipped with Veritas Backup Reporter.

---

### To create a private domain user account

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click **Create Private Domain User**.
- 5 In the New User Details window, type information (such as first name and last name) for the new user in the corresponding fields.

Most fields are optional; however, the following fields require values:

Login	Enter any alphanumeric or special character (maximum length 255)
Domain Name	Select a domain from the drop-down list.
Access Level	Select User, Administrator (Read Only), or Administrator, to set the access level or privileges for the user.  Administrator has read and write privileges on all Veritas Backup Reporter functions.  Administrator (Read Only) has read privileges on all functions of Veritas Backup Reporter.  User has read and write privileges on limited functions of Veritas Backup Reporter.

- 6 Click **Save** to create a new private domain user account.

## Viewing Veritas Backup Reporter user account information

You can view a list of the Veritas Backup Reporter users and their details such as, name, user name, access level, authentication domain, and so on. The used details are arranged in a tabular format. You can sort the table by user details.

### To view Veritas Backup Reporter user account information

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click **Report**.

## Editing Veritas Backup Reporter user accounts

You can modify the password, permission level, and user information for the user accounts you already created.

### To edit a Veritas Backup Reporter user account

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click the **Edit** link next to the user account that you want to edit.
- 5 In the User Information window, make the necessary changes to the user account information.
- 6 Click **Save** to save the changes made to the user account.

## Deleting Veritas Backup Reporter user accounts

You can delete user accounts that do not need to be maintained.

---

**Warning:** Do not inadvertently delete all your administrator accounts.

---

### To delete a Veritas Backup Reporter user account

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Check the user account you want to delete.
- 5 Click **Delete**.
- 6 Select one of the following:
  - Click **OK** to confirm the delete operation.
  - Click **Cancel** to stop the delete operation.

## Creating Veritas Backup Reporter user groups

If you want to give the same privileges to multiple users, add them to a single user group. This user group then can be assigned read and write privileges on Veritas Backup Reporter views, as required. The same access rights are attributed to all users in the user group.

### To create a Veritas Backup Reporter user group

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click the Groups tab.
- 5 On the Groups tab, click **Add Group**.
- 6 In the New Group Details window, type the group name, and click **Save**. You now can go to the Users tab and add user accounts to the group.

## Adding users to Veritas Backup Reporter user groups

You can add user accounts to user groups.

### To add a user account to a Veritas Backup Reporter user group

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Select one or more users you want to add to a group.
- 5 Click **Add Users to Group**.
- 6 In the new window, select one or more user groups to which you want to add the selected users.
- 7 Click **Add**.

## Editing user groups

You can modify an existing user group.

### To edit a Veritas Backup Reporter user group

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 Click the Groups tab.
- 5 On the Groups tab, next to the user account that you want to edit, click **Edit**.

- 6 In the Group Information window, make the necessary changes to the user group.
- 7 Click **Rename Group** to save changes.

## Deleting Veritas Backup Reporter user groups

You can delete a user group that you no longer need.

### To delete a Veritas Backup Reporter user group

- 1 Log on to the VBR Management Server host with administrator privileges.
- 2 In the VBR console, click **Settings > Global Settings**.
- 3 Click **Users/Groups Management**.
- 4 On the Groups tab, select one or more user groups that you want to delete.
- 5 Click **Delete**.
- 6 On the confirmation message box, select one of the following:
  - Click **OK** to confirm the delete operation. This displays a dialog box stating that the user group has been deleted.
  - Click **Cancel** to stop the delete operation.

## Merging objects

Veritas Backup Reporter provides a facility to merge objects that represent the same backup client, but registered as separate objects. Using the Veritas Backup Reporter UI, you can merge only one object into other, at a time.

To merge multiple objects simultaneously, use the command-line utility called `xml.bat`.

See [“About the XML API”](#) on page 559.

In VBR Java View Builder, you can merge multiple objects simultaneously by using the Merge Objects option.

For more details, refer to *Java View Builder Online Help*.

In Veritas Backup Reporter, you can merge objects representing the same backup client and data of which is collected by the same Veritas Backup Reporter Agent. To accomplish this, you can use the `forcemerge` option available for the `xml` command-line utility.

**To merge two objects**

- 1 Log on to the Veritas Backup Reporter Management Server host with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 3 Click **Object Merger**.
- 4 On the Object Merger screen, from the Object getting merged list, select an object name.
- 5 From the Resultant object list, select another object name, which represents the same object that you have selected from another list.

After merging the two objects successfully, the object selected from the Object getting merged list is deleted and the object selected from the Resultant object list is retained.

- 6 Click **Next**.
- 7 On the Update fields before merging objects screen, modify the fields of the resultant object if you want.

All object details are appropriately mapped.

- 8 Click **Save**.



# Understanding data collection

This chapter includes the following topics:

- [About data collection in Veritas Backup Reporter](#)
- [Modifying Veritas Backup Reporter Agent configuration](#)
- [Changing Management Server host for an Agent](#)
- [Viewing agent status](#)
- [Removing agent configurations from the management server](#)
- [Viewing agent alerts](#)
- [About data collectors](#)
- [About products and their versions supported by Veritas Backup Reporter](#)
- [Managing data collectors](#)
- [Collecting NetBackup data](#)
- [Collecting data from Backup Exec](#)
- [Collecting data from PureDisk](#)
- [Collecting data from Legato Networker](#)
- [Collecting data from IBM Tivoli Storage Manager](#)
- [Collecting data from CommVault](#)
- [Collecting data from Enterprise Vault](#)

## About data collection in Veritas Backup Reporter

Veritas Backup Reporter (VBR) provides extensive reporting on the data received from backup / archiving products. Veritas Backup Reporter Agent consists of product-specific data collectors that collect data from the backup / archiving products and return it to the Veritas Backup Reporter Management Server.

See [“About Veritas Backup Reporter components”](#) on page 22.

---

**Note:** Only one Agent can be installed on a single host.

---

VBR Agent consists of data collectors that can collect data from the following backup / archiving products:

- Symantec Enterprise Vault (Windows only)

---

**Note:** Apart from the backup products, Veritas Backup Reporter can now collect data from Symantec Enterprise Vault, an archiving product. In VBR 6.6, you can configure the Enterprise Vault data collector to collect archive data and generate reports to monitor your archiving environment.

See [“Reporting on archive data”](#) on page 405.

To collect Enterprise Vault / archive data, you need to install the VBR Agent on a Windows host.

---

- Veritas NetBackup
- Veritas NetBackup PureDisk
- Symantec Backup Exec (Windows only)

---

**Note:** To collect data from Backup Exec Server host, you need to install the VBR Agent on a Windows host.

---

- EMC Legato Networker
- IBM Tivoli Storage Manager (TSM)
- CommVault Galaxy Backup & Recovery

---

**Note:** You must install Veritas Backup Reporter Management Server and Agent of the same versions. For example, Agent 6.2 MP3 works only with Management Server 6.2 MP3 or Management Server 6.5 is compatible only with Agent 6.5.

---

When you install the Agent, data collectors for all backup / archiving products are automatically installed. However, you need to configure and run a data collector to be able to collect data from the respective product.

---

**Note:** The **Create** link on the **Settings > Global Settings > Agent Configuration** page guides you on where to look in the VBR documentation to install an Agent or change the VBR Management Server host for the existing Agent.

the section called “Installing Veritas Backup Reporter on Solaris and Windows”  
See [“Changing Management Server host for an Agent”](#) on page 176.

In VBR 6.6, you cannot create an Agent using the VBR console. However, you can modify the Agent that you have installed through VBR installation wizard.

See [“Modifying Veritas Backup Reporter Agent configuration”](#) on page 174.

---

## About data collection checklist

This section describes what all you need to take care of before collecting data from a product host.

- Make sure if the appropriate ports are open required for communication between VBR Agent, Management Server, and product host.  
the section called “About configuring Veritas Backup Reporter firewall”
- Review the following section to understand the VBR Agent deployment scenarios.  
[About Veritas Backup Reporter Agent deployment](#)
- Make sure you have installed and configured the VBR Agent appropriately.  
[About Veritas Backup Reporter Agent deployment](#)
- Review the following section to understand the functionality of the data collectors.  
[About data collectors](#)
- Check if any prerequisites are to be met, before collecting the data. These prerequisites vary depending on which product host you want to collect the data.  
Configure data collector appropriately as described in the data collection sections. Refer to the product specific checklists, if any, included in the following sections.
  - [Collecting NetBackup data](#)
  - [Collecting data from PureDisk](#)
  - [Collecting data from Backup Exec](#)

- [Collecting data from IBM Tivoli Storage Manager](#)
- [Collecting data from CommVault](#)
- [Collecting data from Legato Networker](#)
- [Collecting data from Enterprise Vault](#)

## Modifying Veritas Backup Reporter Agent configuration

You can modify the Agent configuration using the VBR console.

### To modify the Agent configuration

- 1 Log on to the Agent host with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 In the Agents tab, click the Agent link to modify its configuration settings. This displays the Agent/Server Information page.
- 4 The Agent/Server Information page shows the Agent Host, and Spooled Data Directory that you have entered while installing the Agent.

Maximum Data Spool Size on Disk (MB) is the maximum allowable size of the spooler. If the spooler has reached its maximum limit (500 MB), the data collection cannot proceed.

---

**Note:** The spooler resides on the Agent host and can hold the backup data up to its maximum memory usage. The spooler temporarily stores the collected data and transfers it sequentially to the VBR Management Server.

---

You can modify the following Agent configuration settings on the Agent/Server Information page:

Agent Host CORBA Port	You can modify the default Agent host CORBA Port, which is 7806. The Agent uses this port for CORBA communication.
-----------------------	--

See [“About configuring Veritas Backup Reporter firewall ”](#) on page 46.

Backup Reporter Server Host Name	<p>Enter the name of the VBR Management Server host, to which you want to connect the Agent. To connect to this new Management Server host, you need to carry out a few steps as described in the following section.</p> <p>See <a href="#">“Changing Management Server host for an Agent”</a> on page 176.</p>
Level	<p>From the drop-down list, select the granularity level for Agent log information. The log levels are as follows:</p> <ul style="list-style-type: none"> <li>■ Off</li> <li>■ Severe</li> <li>■ Warning</li> <li>■ Info</li> <li>■ Config</li> <li>■ Debug-Fine</li> <li>■ Debug-Finer</li> <li>■ Debug-Finest</li> <li>■ All</li> </ul> <p>Select 'Off' to disable collection of Agent error logs. If you set the log level to 'All', every bit of the core Agent information will be logged. When you set the logging to a particular level, the log information for all levels previous to that level is also stored. For example, if you set the log level to 'Warning', all warnings and errors / exceptions (log information pertaining to the 'Severe' log level) are logged. In Debug type of logs, all CLIs that were fired during data collection are stored, along with the information pertaining to previous log levels.</p>
Max Size (MB)	<p>Enter the maximum size in MB that you want to set for the Agent log file. For example, enter 5, if you want the Agent log file to grow up to 5 MB before it rolls over to the next log file. The number of log files created depends on the Rollover Count that you specify.</p>

#### Rollover Count

Enter the rollover count for the Agent log files. For example: If you specified the Max Size of the core Agent log file as 5 MB and Rollover Count as 4, a log file (say core-0.log) can grow up to 5 MB. When the size reaches 5 MB, the log information is pushed to the next log file (say core-1.log) and the latest log information is stored in the first log file (that is core-0.log). Thus, when four log files are full and log information is still increasing, the oldest log information that is in 3.log file is deleted. Thus, at any given time the number of log files is less than or equal to 4 and the latest log information is available in the core-0.log file.

the section called “About Veritas Backup Reporter log files”

#### 5 Click **Save**.

After configuring the Agent, you need to configure the data collectors to collect data from the backup / archiving products.

See “[Viewing agent status](#)” on page 177.

#### 6 See “[Configuring a data collector](#)” on page 189.

## Changing Management Server host for an Agent

In certain situations, you may need to change the Management Server host that you have specified while installing VBR Agent. For example: You have an Agent A1 configured, which connects to VBR Management Server named VBR1. You want to change the Management Server host of A1 to the new one named VBR2. You can either modify the Management Server host name using the **Settings > Global Settings > Agent Configuration** section and then carry out the following steps, or you can directly carry out the following steps without modifying the Management Server host name.

#### To change the VBR Management Server host for an Agent

- 1 Log on to the old VBR Management Server console (for example, VBR1) with administrator-level privileges.
- 2 Delete the Agent to be moved (for example, A1). Go to **Settings > Global Settings > Agent Configuration**, in the Agents tab, select a checkbox and click **Delete**.
- 3 Log on the VBR Agent host (for example, A1).
- 4 Stop the Agent service.

5 In the command prompt, run the following command:

Solaris `/opt/VRTSccsva/bin/agentauth -server new VBR  
Management Server host name`

For example, VBR2

Windows `\Program Files\Symantec\Veritas Backup  
Reporter\Agent\bin\agentauth.exe -server new  
VBR Management Server host name`

For example, VBR2

6 Start the Agent Service.

See “[Stopping and starting the Veritas Backup Reporter Agent](#)” on page 115.

The `agentauth` command may fail. To resolve these issues, refer to the following section:

See “[Resolving agent authentication failures manually on Solaris and Windows](#)” on page 110.

## Viewing agent status

Veritas Backup Reporter provides you with the detailed view of the current status of configured agents. By looking at the agent status page, you can know the status of the events that are configured for each data collector.

The agent status page displays the following agent details:

- Name of the agent host
- Version of the agent
- Number of configured data collectors
- agent version
- Memory usage of the agent

---

**Note:** The agent’s memory usage comprises three parameters. If the agent memory usage appears as 1M / 2M of 253M, it signifies that the agent is using 1 MB of memory out of 2 MB of the allocated memory and the maximum heap size is set to 253 MB.

---

### To view agent status

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, in the Configured Agents table, click the **Show Details** link to view the status of the respective agent.

Use the **Show Problems Only**, **Show Agent Summary**, **Show Agent Data Transmission Problems**, and **See Alerts** links to view failed events, event status summary, data transmission status, and alert details, respectively.

See “[Viewing status of configured data collectors](#)” on page 179.

## Viewing all agents status summary

Apart from viewing the status for the selected agent, Veritas Backup Reporter lets you view status summary of all configured agents. The All Agents Summary page displays the event status for all configured agents.

The All Agents Summary displays the following details:

Agent Host	Name or IP address of the agent host
Ready	Number of events that are in the Ready state
Running	Number of events that are running
Completed	Number of events that are completed
Failed	Number of events that are failed
Files In Spooler	Size of data residing in the spooler
DiskSpace Used By Spooler (MB)	Disk space of the spooler in MB
Spooler Lag	The lag between reception of data by the spooler and the transmission of that data by the spooler to the management server
Memory Usage	Memory usage by the agent
Last Heartbeat	The time of the recent heartbeat sent by the agent to the management server. With the heartbeats, the agent indicates that it is running. The heartbeat reports to the agent whenever there are any changes in the agent configurations on the management server.

### To view the agent status summary

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the **Show All Agents Status** link to view the status summary of all agents.

## Viewing status of configured data collectors

The Configured Data Collector Status page displays the following details, such as type of the data collector and name of the management server host.

Product	Name of the backup/archiving product, for example Veritas NetBackup
Product Host	Name of the product host from which the data collector is collecting data
Host Qualify Option	The option by which the backup product host is qualified, for example Via DNS
Status	The status of the data collector, for example enabled or disabled
Data Type	Name of the data type to be collected, such as Job, Image, Policy, Media, Skipped File or Error in a NetBackup setup
Server Last Successful Data Load	The recent date and time when the management server received data collected from a backup product
Agent Last Successful Data Load	The recent date and time when the agent received data from the data collector collected from a backup product
Last Run Time	The date and time when this data type was collected last
Collection Status	Status of the event queue, for example Not Queued, Ready, Running, Completed, or Failed
Last Exception Message	The code and description of the exception that recently occurred while collecting data
Records Collected	Record count or number of records collected against the event

Force Poll This option enables you to collect backup data, irrespective of the predefined schedule, against each event. Click **Poll** to start collecting data. For a few events, you can also specify the time interval for data collection. Use the From Last drop-down list to specify the time interval in hours, days, months, or years.

See “[Collecting data by the force poll method](#)” on page 196.

**To view the data collector status**

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the configured agent that you want to view the data collector status for.
- 4 On the Agent/Sever Information page, in the Configured Data Collectors table, click the **Show Details** link to view the status of the respective data collector.

## About data collection status

The data collection has various stages, from not queued to completed. Veritas Backup Reporter uses color coding to represent these collection states, which let you clearly distinguish these states from each other.

Table 5-1 describes the various stages of data collection.

**Table 5-1** Collection status

Collection status (color code)	Description
Not queued (Grey)	The event is not yet queued for data collection. It is queued at the scheduled time. Since the event is not ready and data is not yet collected, the Server and Agent Last Successful Data Load, and Event Last Run Time are unknown and are indicated as Never Reported and Not Run, respectively.
Ready (Yellow)	The event is ready for data collection. Since the data collector has not yet collected the data, the Server and Agent Last Successful Data Load are unknown and hence indicated as Never Reported. Initially, the Event Last Run Time is indicated as Not Run, which is later updated as the event runs.

**Table 5-1** Collection status (*continued*)

Collection status (color code)	Description
Running (Blue)	The event is running and the data collector is collecting data. As the management server does not immediately receive data from the agent, the Server Last Successful Data Load time is initially shown as In Progress, which is indicated by the color orange. This time is later updated as the management server receives data. The Agent Last Successful Data and Event Last Run Time are updated as the event runs.
Completed (Green)	The event is completed as the data collector has collected data. The Server Last Successful Data Load, Agent Last Successful Data and Event Last Run Time are updated as the event runs. Initially, The Server Last Successful Data Load time is shown in the color orange. This state indicates that the management server is still receiving data from the spooler; however, the agent has already received data from the data collector.
Failed (Red)	The event is failed because of some external reasons. In this case, the data collector cannot pass data to the agent and consequently to the management server. The Server Last Successful Data Load and Agent Last Successful Data time are shown as Never Reported in case of initial data load. The Event Last Run Time is updated as the event runs.
Paused (Color of the state when the event was paused – Grey, Red or Green)	The event is paused. You can interrupt the event when it is not yet queued, failed, or completed. However, the event continues to collect data when it is in the Ready or Running state, even if it is paused. The Server Last Successful Data Load, Agent Last Successful Data Load, and Event Last Run Time are updated as per the status of the event (Not Queued, Failed, or Completed) when it was paused.

## Viewing the complete agent status summary

You can view the status summary of the selected agent. Agent status summary is presented in the following ways:

- [About agent summary by data collector type](#)
- [About agent summary by data type](#)
- [About Data collectors summary](#)

### To view complete agent status summary

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the **Show All Agents Status** link.
- 4 On the All Agents Summary page click the agent host name, for which you want to view the status summary.
- 5 On the complete agent status page, click the **Show Agent Summary** link.

### About agent summary by data collector type

This section shows details of all data collectors for the selected agent.

Product	Name of the backup or archiving product, for example Veritas NetBackup
Target Host	Name of the product host, from which the agent is collecting data
Ready	Number of data types scheduled for each data collector that are in the Ready state
Running	Number of data types scheduled for each data collector that are in the Running state
Completed	Number of data types scheduled for each data collector that are in the Completed state
Failed	Number of data types scheduled for each data collector that are in the Failed state
Files in Spooler	Number of records that are in spooler
Disk Space Used by Spooler (MB)	Disk space in MB
Spooler Lag	The time taken by the spooler to send the backup data to the management server, since the time it received that data from the agent

### About agent summary by data type

This section shows total number of events with the specified status that are scheduled for the selected agent.

Data Type	Name of the data type to be collected, such as job or media in case of NetBackup setup
Ready	Total number of data types of the specified type that are scheduled for all data collectors and that are in the Ready state
Running	Total number of data types of the specified type that are scheduled for all data collectors and that are in the Running state
Completed	Total number of data types of the specified type that are scheduled for all data collectors and that are in the Completed state
Failed	Total number of data types of the specified type that are scheduled for all data collectors and that are in the Failed state
Files in Spooler	Number of records that are in spooler
Disk Space Used by Spooler (MB)	Disk space in MB
Spooler Lag	The time taken by the spooler to send the backup data to the VBR Management Server, since the time it received that data from the VBR Agent

## About Data collectors summary

The data collectors summary provides details of each event scheduled for each data collector, such as status and record count.

Product	Name of the backup or archiving product, for example Veritas NetBackup
Target Host	Name of the product host, from which the agent is collecting data
Policy and Schedule	The status of the event that collects policy data and the record count
Tape Drive Usage	The status of the event that collects tape drive usage data and the record count
Media	The status of the event that collects media data and the record count

Job	The status of the event that collects job data and the record count  Error and Skipped File data is also collected as part of Job data
Image	The status of the event that collects image data and the record count

## Viewing agent data transmission errors

You can view errors occurred during data transmission between agent and management server.

Product	Name of the backup or archiving product, for example Veritas NetBackup
Data Type	The name of the data type
Last Exception Message	The code and description of the exception that has recently occurred while transmitting data to management server
Force Load	The force load option enables you to transmit backup data to management server irrespective of the predefined schedule. Click <b>Force Load</b> to start transmitting data.

### To view agent data transmission errors

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the **Show All Agents Status** link.
- 4 On the All Agents Summary page click the agent host name, for which you want to view the status summary.
- 5 On the complete agent status page, click **Show Agent Data Transmission Problems** link.

## Removing agent configurations from the management server

You can remove an agent configuration from the management server.

### To remove agent configurations from the management server

- 1 Log on to the Veritas Backup Reporter Management Server with the administrator privileges, from which you want to remove one or more agents.
- 2 In the console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Agents Settings page, in the Settings table, select agents that you want to remove from the management server by selecting check boxes in front of them.
- 4 Click **Delete**.
- 5 On the confirmation dialog box, click **OK**.

## Viewing agent alerts

You can use the console to view agent alerts for a particular data collector.

### To view agent alerts for a data collector

- 1 Log on to the Veritas Backup Reporter Management Server on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Agent Settings page, click the link for the agent for which you want to view agent alerts.
- 4 On the Agent/Server Information Configuration page, in the Settings table, select the data collector for which you want to view agent alerts.
- 5 Click **Show Agent Status** at the bottom of the screen.
- 6 On the Complete Agent Status page, click **Alerts**.

See [“About alerts and the Alert Manager”](#) on page 295.

## About data collectors

Agent Module has been renamed as 'Data Collector' in VBR 6.6.

The VBR data collectors, as the name suggests, collect data from backup/archiving product hosts. Each data collector collect data from a single product host. You can configure multiple data collectors for a single VBR Agent.

---

**Note:** Agent Module has been renamed as 'Data Collector' in VBR 6.6.

---

You can create data collectors to communicate with the various products, such as NetBackup, BackupExec, or Enterprise Vault. These data collectors collect the specified data type as specified in the configuration. You can specify to collect all or some of the data types for that product. For example, NetBackup data collector can collect Tape Drive Usage, Media, Policy and Schedule, Job, Error, Skipped File, or Image.

You can enable or disable a data collector.

[Table 5-2](#) lists the data collectors that you can configure in Veritas Backup Reporter.

**Table 5-2** Data collector types

Data Collector type	Description
NetBackup Data Collector	Create this data collector to collect data from NetBackup. See <a href="#">“Collecting NetBackup data ”</a> on page 198.
NetBackup PureDisk Data Collector	Create this data collector to collect data from NetBackup PureDisk. See <a href="#">“Collecting data from PureDisk ”</a> on page 223.
BackupExec Data Collector (Windows only)	Create this data collector to collect data from BackupExec. See <a href="#">“Collecting data from Backup Exec”</a> on page 221.
TSM Data Collector	Create this data collector to collect data from TSM. See <a href="#">“Collecting data from IBM Tivoli Storage Manager ”</a> on page 235.
Legato Networker Data Collector	Create this data collector to collect data from Legato Networker. See <a href="#">“Collecting data from Legato Networker”</a> on page 234.
CommVault Galaxy Backup & Recovery Data Collector	Create this data collector to collect data from CommVault Galaxy Backup & Recovery. See <a href="#">“Collecting data from CommVault”</a> on page 236.
Enterprise Vault Data Collector (Windows only)	Create this data collector to archive collect data from Symantec Enterprise Vault database See <a href="#">“Collecting data from Enterprise Vault ”</a> on page 237. <b>Note:</b> Support for Enterprise Vault has been added in VBR 6.6.

[Table 5-3](#) lists data types collected by VBR data collectors from various products.

**Table 5-3** Data types collected

Backup product	Data type collected by Veritas Backup Reporter
Veritas NetBackup	Tape Drive Information, Media, Policy and Schedule, Job, Error, Skipped File, Image
Veritas NetBackup PureDisk	Policy and Schedule, Job
Symantec Backup Exec	Tape Drive Information, Media, Policy and Schedule, Job, Error, Skipped File <b>Note:</b> Support for data collection of Skipped File and Media data is added in VBR 6.6
Tivoli Storage Manager	Tape Drive Information, Media, Policy and Schedule, Job, Error, Skipped File
EMC Legato Networker	Tape Drive Information, Media, Policy and Schedule, Job, Error, Skipped File
CommVault Galaxy Backup & Recovery	Tape Drive Information, Media, Policy and Schedule, Job, Error, Skipped File, Image
Symantec Enterprise Vault	Archive Policy, Vault Store, Target, Archive <b>Note:</b> Support for Enterprise Vault is added in VBR 6.6.

## About products and their versions supported by Veritas Backup Reporter

This section lists the backup products and their versions that are supported by Veritas Backup Reporter.

[Table 2-4](#) lists backup products supported by Veritas Backup Reporter.

**Table 5-4** Backup products supported by Veritas Backup Reporter

Backup product	Versions	Support level
Veritas NetBackup	3.4, 3.4.1, 4.5, 5.0, 5.1, 6.0, 6.0 MPx, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4	All supported NetBackup platforms via remote agent  Native agent for Windows 2000, 2003 and Solaris 8, 9, and 10

**Table 5-4** Backup products supported by Veritas Backup Reporter (*continued*)

Backup product	Versions	Support level
Veritas NetBackup PureDisk	6.2, 6.2.1, 6.2.2, 6.5, 6.5.0.1, 6.5.1	PureDisk supported platform (PDOS) via remote agent
Symantec Backup Exec	10.0, 10d, 11d, 12, 12.5 <b>Note:</b> Symantec Backup Exec running on NetWare is not supported by Veritas Backup Reporter.	All supported Symantec Backup Exec platforms via remote agent Native agent on backup servers on Windows 2000, 2003 <b>Note:</b> VBR 6.6 does not support data collection from Backup Exec 9.x version. You need to create a data collector to collect data from Backup Exec 10d and later versions. However, you can run the reports on the Backup Exec 9.x data.
EMC Legato NetWorker	6.x, 7.x	Native agent on backup servers on Windows 2000, 2003 and Solaris 8, 9, and 10
IBM Tivoli Storage Manager (TSM)	5.1, 5.2, 5.3, 5.4, 5.5	All supported TSM platforms via remote agent Native agent for backup server on Windows 2000, 2003 and Solaris 8, 9, and 10
CommVault Galaxy Backup & Recovery	5.9 SP3	All supported CommVault platforms via remote agent
Symantec Enterprise Vault	2007 SP3, 2008	All supported Symantec Enterprise Vault platforms via remote agent Native agent on Microsoft SQL Server 2005 or 2008 (where Enterprise Vault database resides) on Windows 2000 and 2003

## Managing data collectors

VBR data collectors let you collect data from the respective backup / archiving products. You can configure multiple data collectors for a single agent, to collect

data from each product host. Before configuring data collectors, you need to configure agent.

The agent contains data collectors that you can enable and configure for the following Symantec and third-party backup / archiving applications:

- Veritas NetBackup
- Veritas NetBackup PureDisk
- Symantec BackupExec (Windows only)
- EMC Legato Networker
- IBM Tivoli Storage Manager (TSM)
- CommVault Galaxy Backup & Recovery
- Symantec Enterprise Vault (Windows only)

## Configuring a data collector

Veritas Backup Reporter is designed to provide extensive reporting on the data received from backup / archiving products. Veritas Backup Reporter consists of a management server, an agent, and a console. The agent contains product-specific data collectors collecting data from the products and returning it to the management server. You can generate various business reports on this backup / archiving data.

When you install the agent, all data collectors are automatically installed. After you configure the agent, configure the data collectors.

### To configure a data collector

- 1 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 2 On the Settings page, click the agent for which you want to configure a data collector.
- 3 On the Agent/Server Information Configuration page, click **Create**.

**4** On the Create Agent Data Collector Configuration page, enter the following information:

Product	<p>Select the name of the product from which you want to collect data. For example, Veritas NetBackup.</p> <p>The options in the Product drop-down list box comprise the product name and the operating system on which the VBR Agent is running. Select the appropriate option from the list box. For example: You have a NetBackup Master Server running on a Solaris host and the VBR Agent running on a Windows host. To collect data from the NetBackup Master Server (running on Solaris), select Veritas 'NetBackUp - Windows' from the Product drop-down list.</p> <p>This will create a data collector of type NetBackup.</p> <p>For Enterprise Vault and Backup Exec, only Windows option is available, as these products support only Windows operation system.</p>
Target Host Name	<p>Enter the name of the NetBackup Master Server or Media Server host name from which you want to collect the backup / archiving data.</p>

**5** Click **Next**.

On the Data Collector Details page, the Target Details, Configuration Settings, Log Settings, And Discovered Hosts details are displayed.

**6** Check / enter the following Target Details:

Product	<p>Displays the name of the product that you have specified on the Create Data Collector Configuration page.</p>
Target Host Name	<p>Displays the name of the target host that you have specified on the Create Data Collector Configuration page.</p>
Data Collector Status	<p>By default, the data collector status is Enabled. You can disable the data collection by changing the status.</p>

- 7** Enter the data collector configuration settings. These settings vary depending on the data collector type that you are configuring. For product specific configuration settings, refer to the respective data collection settings.
- See [“Collecting NetBackup data ”](#) on page 198.
- See [“Collecting data from PureDisk ”](#) on page 223.
- See [“Collecting data from Backup Exec”](#) on page 221.
- See [“Collecting data from CommVault”](#) on page 236.
- See [“Collecting data from IBM Tivoli Storage Manager ”](#) on page 235.
- See [“Collecting data from Legato Networker”](#) on page 234.
- See [“Collecting data from Enterprise Vault ”](#) on page 237.
- 8** Enter the following Log Settings:

Level	<p>From the drop-down list, select the granularity level for log information. The log levels are as follows:</p> <ul style="list-style-type: none"> <li>■ Off</li> <li>■ Severe</li> <li>■ Warning</li> <li>■ Info</li> <li>■ Config</li> <li>■ Debug-Fine</li> <li>■ Debug-Finer</li> <li>■ Debug-Finest</li> <li>■ All</li> </ul> <p>If you set the log level to ‘Off’, no logs will be stored for this log level and if you set it to ‘All’, every bit of the data collector information will be logged. When you set the logging to a particular level, the log information for all levels previous to that level is also stored. For example, if you set the log level to ‘Warning’, all warnings and errors / exceptions (log information pertaining to the ‘Severe’ log level) are logged.</p> <p>In Debug type of logs, all CLIs that were fired during data collection are stored, along with the information pertaining to previous log levels.</p>
Max Size (MB)	<p>Enter the maximum size in MB that you want to set for a data collector log file. For example, enter 5, if you want a data collector log file to grow up to 5 MB before it rolls over to the next log file. The number of log files created depends on the Rollover Count that you specify.</p>

### Rollover Count

Enter the rollover count for the data collector log files.

For example: If you specified the Max Size of a log file as 5 MB and Rollover Count as 4, a log file (say 0.log) can grow up to 5 MB. When the size reaches 5 MB, the log information is pushed to the next log file (say 1.log) and the latest log information is stored in the first log file (that is 0.log). Thus, when four log files are full and log information is still increasing, the oldest log information that is in 3.log file is deleted. Thus, at any given time the number of log files is less than or equal to 4 and the latest log information is available in the 0.log file.

Example of the log file name:

```
module-002-enterprisevault-server1-0.log
```

**9** Enter the following Discovered Hosts - Name Qualification Options:

With these options, you can specify the way you want to refer to the Enterprise Vault hosts in Veritas Backup Reporter context.

- |                                    |  |
|------------------------------------|--|
| Append Domain                      | <p>Select this option and add text in the @ text box to append this text to all product host names.</p> <p>For example: Veritas Backup Reporter has discovered a host name, say 'NetBackup1' from NetBackup database. Veritas Backup Reporter may not be able to refer to 'NetBackup1' using the same host name, while requesting backup data. In this case, select the Append Domain option and add domain name say 'DomainName', which will be appended to the host name, that is NetBackup1@DomainName</p> <p>This is useful if different product servers refer to physically different clients by the same name.</p> |
| Via DNS (not recommended for DHCP) | <p>This is a default option. This option enables the Veritas Backup Reporter Agent to perform DNS lookup on the product host names to get the associated IP addresses. Use this option only if you have a common DNS environment for product hosts and Veritas Backup Reporter Agent.</p> <p><b>Caution:</b> Do not use this setting if the hosts in backup environment use DHCP, because there may be conflicts with the same IP addresses being used by the different servers at different times.</p>  |
| Do Not Qualify                     | <p>Select this option if you do not want to Veritas Backup Reporter Agent to modify the host names discovered from backup product.</p> <p><b>Caution:</b> Do not use this option if you do not have unique host names across the backup environment. Because HostA from one product server will now match against a HostA discovered from another server and you cannot identify them in reports.</p>  |

**10** Enter the following information regarding data types to be collected:

Configuration Status	Select this check box to collect the associated data type.
Collectable Data Type	Lists the data types that can be collected from a product host. The data types vary depending on the product that you are collecting data from.  the section called “About data collectors”
Collection Interval (sec)	Enter the collection interval in seconds, minutes, hours, and days. This is the time interval that you want to set between the two consecutive data collections.  For example: You have set the Collection Interval to 15 Minutes. The first data collection starts at say 9 AM and continues until all archive records are collected and ends at 11 AM. The next data collection will start at 11.15 AM.
Blackout Period Start Time	Select the start time of a blackout period. The data is not collected for the time specified in Blackout Period Duration, since Blackout Period Start Time.
Blackout Period Duration (hr)	Select the blackout duration in hours, for which the data is not collected since the time specified for the Blackout Period Start Time field.  For example: You have set the Blackout Period Start Time as 1:00 PM and the Blackout Period Duration as 2 hours. No data is collected between 1 PM to 3 PM.
Last Successful Data Load	States whether last data load was successful or not.  See “ <a href="#">Viewing agent status</a> ” on page 177.
Collection Status	Displays the status of data collection. You can either resume or pause the data collection.

**Fetch Size** Select the number of records of the data type that you want to fetch at a time.

For example:

If the Fetch Size is set 500, the Veritas Backup Reporter Agent can at a time send maximum of 500 Archive records to the Management Server. If the Agent has collected 600 Archive records from the Enterprise Vault database, it can send them to the Management Server in two chunks, 1st chunk of 500 records and 2nd one of 100.

Symantec recommends that you set the fetch size to 5000 for the Archive data type because of the following reason:

There can be thousands of records of the Archive data type that Agent collects from the Enterprise Vault database, in a given time interval. The Agent sends these records to the Management Server, as soon as it receives them from the Enterprise Vault database. If you set the fetch size of the Archive data type to a value lesser than 5000, the data collection and data transmission by the Agent will not be in sync and the Agent performance will drop.

## 11 Click **Save**.

# Modifying data collector configurations

You can use the Veritas Backup Reporter console to modify configuration of a data collector.

### To modify data collector configurations

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the agent to modify its data collector configuration.
- 4 On the Agent/Server Information page, in the Configured Data Collectors table, click the data collector you want to modify.
- 5 On the Data Collector Details page, do the following:
  - From the Status drop-down list, select Enabled or Disabled.
  - Modify the Log Settings fields, such as level of information in the log file, maximum log file size in bytes, and rollover file count.

For example: If you specified the Max Size of a log file as 5242880 bytes and Rollover Count as 4, log files with maximum size of 5242880 bytes are created. When four log files are full and log information is still increasing, the oldest file is deleted. Thus, at any given time the number of log files is less than or equal to 4.

- 6 Modify data collector variables.
- 7 Modify host name qualification options.
- 8 Modify data type configurations, such as configuration status, collection interval, blackout period, collection status, or fetch size. The fetch size is the number of records you want the data collector to pass to the agent at one go.  
You cannot modify the collection status of the disabled data types.
- 9 Click **Save**.

## Collecting data by the force poll method

The force poll option lets you collect data against each data type, irrespective of the predefined schedule. For a few data types, you can also specify the time interval for data collection. The NetBackup data types, such as media, policy, and tape drive usage do not have the time interval option, because this data is not updated very often.

---

**Warning:** If you want to run a force poll, the management server must communicate with the agent on the agent CORBA port. The default port is 7806. If this port is changed, force polls do not work.

---

### To collect data by force poll method

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Settings page, click the agent to run the force poll on its data type.
- 4 On the Agent/Server Information page, in the Configured Data Collectors table, click **Show Details** to open the corresponding Data Collector status.

- 5 For the data types such as, error, image, job, and skipped file, you can select the time interval in hours, days, months, or years from the From Last drop-down list.
- 6 Click the **Poll** button corresponding to the data type, for which you want to execute the force poll.

The Poll button is disabled if you have disabled the data collector.

## Copying data collector configurations

You can use the console to copy a data collector configuration on the agent. In this way, you can quickly duplicate data collector settings for various agent hosts.

### To copy data collector configurations on agents

- 1 Log on to the Veritas Backup Reporter Management Server on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings > Agent Configuration**.
- 3 In the Agent Settings page, click the agent for which you want to copy one or more data collector configurations.
- 4 In the Agent/Server Information page, in the Configured Data Collectors table, select the data collectors you want to copy.
- 5 From the drop-down list, click **Copy Items**, and then click **Go**.
- 6 On the alert message box, click **OK**.
- 7 Specify the host name of the target data collector.

## Deleting data collectors

Use the VBR console to delete a data collector.

### To delete a data collector on a VBR Agent

- 1 Log on to the Veritas Backup Reporter Management Server on which you have administrator-level privileges.
- 2 In the console, click **Settings > Global Settings > Agent Configuration**.
- 3 On the Agent Settings page, click the agent from which you want to delete a data collector.
- 4 In the Agent/Server Information panel, in the Configured Data Collectors table, select the data collector you want to delete.
- 5 From the drop-down list, click **Delete**, and then click **Go**.
- 6 On the alert message box, click **OK**.

## Collecting NetBackup data

This section provides information on collecting data from NetBackup and configuring NetBackup data collector.

For other tasks related to data collector, refer to the following sections.

See [“Modifying data collector configurations”](#) on page 195.

See [“Collecting data by the force poll method”](#) on page 196.

See [“Copying data collector configurations”](#) on page 197.

See [“Deleting data collectors”](#) on page 197.

## About Policy and Scheduled Jobs data collected in VBR 6.6

Veritas Backup Reporter (VBR) 6.6 collects additional information about NetBackup Policies, Schedules, and Jobs, using which you can generate a set of new reports.

VBR can now collect the following Policy, Schedule, and Job information from NetBackup.

**Policy** VBR 6.6 collects additional policy information / attributes, for example Policy Type, Data Classification, Policy Volume Pool, or Policy Storage Unit .

**Note:** VBR 6.6 NetBackup data collector collects new attributes of policies as part of ‘Policy and Schedule’ data type.

The policy attributes are collected using the `bppllist` CLI (Command-line Interface).

You can generate custom reports using the new policy attributes.

**Schedule** VBR 6.6 collects additional schedule information / attributes, for example Schedule Type, Type of Backup, Schedule Retention, and Schedule Frequency.

**Note:** VBR 6.6 NetBackup data collector collects new attributes of schedules as part of ‘Policy and Schedule’ data type.

The configuration data of all schedules is collected using the `bppllist` CLI.

You can generate custom reports using the new schedule attributes.

**Job** VBR 6.6 collects Scheduled Jobs information as part of 'Job' data type.

See [“About Policy and Scheduled Jobs data collected in VBR 6.6”](#) on page 198.

Scheduled Jobs information is collected using the `nbpemreq` CLI (Command-line Interface).

VBR 6.6 collects Job Execution Type as part of 'Job' data type, using `bpdbjobs` CLI. In NetBackup, jobs are executed according to their Job Execution Types, namely Manual and Scheduled.

VBR 6.6 provides a set of new canned reports called 'Scheduled Jobs' to view Scheduled Jobs information, for example Schedule Time of jobs.

See [“Reporting on scheduled jobs data”](#) on page 390.

Depending on the execution type and status, the jobs collected from NetBackup are categorized in Veritas Backup Reporter as follows:

Scheduled Jobs	Jobs that are scheduled to run at specific time in future are referred to as Scheduled Jobs in VBR context. Each Scheduled Job is associated with a client, policy, schedule, and schedule time. VBR retains this information historically, to compare the schedule time of a job with the actual job start time.
Actual Jobs	Jobs that have already been run  These include all jobs that were run, either of execution type 'Scheduled' or 'Manual'.
Manual Jobs	Some jobs are initiated by NetBackup administrator / user at his or her discretion. They are executed as soon as they are initiated. These jobs are called 'Manual Jobs'.

Prior to VBR 6.6, you could view only those jobs, which were already run and their corresponding Job Start Time. You could not collect schedule time of jobs. Therefore, you could not compare actual Job Start Time with its schedule time.

VBR 6.6 collects Scheduled Job information using the `nbpemreq` CLI.

Scheduled Job information comprises the following data in that order:

- Client Name
- Policy Name
- Schedule Name
- Next Schedule Time for this Job

Following are the examples of Scheduled Job information:

VBRServer1 FullBackup Daily 2009-03-19 18:00:00

VBRServer1 IncrementalBackup Weekly 2009-03-19 18:00:00

VBRServer2 FullBackup Daily 2009-03-23 00:20:00

Veritas Backup Reporter 6.6 provides a new set of reports called 'Scheduled Jobs' that is available in the Backups > Activity Planning report category.

See ["Reporting on scheduled jobs data"](#) on page 390.

The Scheduled Jobs reports help you answer the following questions:

- Which and how many Scheduled Jobs have already been run?  
These are the jobs for which both schedule time and Job Start Time are available
- Did jobs run at the schedule time or the actual Job Start Time was different than the Schedule Time?  
You can determine this by comparing the Schedule Time and Job Start Time of each Scheduled Job
- Which Scheduled Jobs did not actually run?  
These are the Scheduled Jobs which do not have corresponding Job Start Time
- What was the actual Job Start Time of a Scheduled Job?  
The actual Job Start Time of a job that was run is available in VBR
- How many jobs that have already been run, are manual and how many of them are of type 'Scheduled'?  
Job execution type is collected in VBR 6.6.

## About the restrictions in collecting scheduled jobs data

The following are a few restrictions you may come across while collecting the schedule data or generate the related reports:

- In VBR 6.6, NetBackup data collector can collect additional policy and schedule data only from NetBackup 6.0 or later versions. If you have NetBackup version older than 6.0, you cannot view the reports based on additional policy and schedule data.
- In VBR 6.6, NetBackup data collector can collect Schedule Jobs information only from NetBackup 6.5 or later versions. If you have NetBackup version older than 6.5, you cannot view the reports based on jobs that have schedule associated with them.
- If you have NBAC enabled NetBackup, you can collect schedule information only in case of local data collection setup and on Solaris platform. This particular setup does not support collection of schedule information from a

Windows platform. It does not support collection of schedule information also from a Solaris platform in case of remote data collection.

- All new policy and schedule attributes collected in VBR 6.6 are available while generating custom reports and not in canned reports. A set of canned reports is available only for Scheduled Jobs information. See [“Reporting on scheduled jobs data”](#) on page 390.
- You require credentials of the NetBackup Administrator to collect Scheduled Jobs data from a remote NetBackup Master Server with version prior to 6.5.4. Specify these admin user credentials while creating NetBackup data collector. See [“Configuring NetBackup data collector”](#) on page 201.
- Jobs for which schedule information is not available, are excluded from Scheduled Jobs reports, from actual job count and scheduled job count.
- If you have upgraded VBR from an older version to 6.6, Scheduled Jobs reports will not show jobs that have already been executed in NetBackup Master Server with version prior to 6.5.4. Only jobs that are scheduled to run in future will be shown as Scheduled Jobs.
- After the initial data load (the very first data collection after a fresh VBR installation), if you run a Scheduled Jobs report for the job schedule time older than the initial data load time, the Scheduled Jobs count may not be displayed accurately. This is because the `nbpemreq` CLI receives schedule time only for the jobs that are scheduled to run in future. The schedule time of jobs that have already been run is not available. However, all actual jobs are collected.

## Configuring NetBackup data collector

This section provides the procedure to configure the NetBackup data collector using the Veritas Backup Reporter console.

### To configure NetBackup data collector

- 1 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 2 On the Settings page, click the agent for which you want to configure an NetBackup data collector.
- 3 On the Agent/Server Information Configuration page, click **Create**.

**4** On the Create Agent Data Collector Configuration page, enter the following information:

**Product** Select the name of the product from which you want to collect data. Select Veritas NetBackup.

The options in the Product drop-down list box comprise the product name and the operating system on which the VBR Agent is running. Select the appropriate option from the list box. For example: You have a NetBackup Master Server running on a Solaris host and the VBR Agent running on a Windows host. To collect data from the NetBackup Master Server (running on Solaris), select Veritas 'NetBackUp - Windows' from the Product drop-down list.

This will create a data collector of type NetBackup.

For Enterprise Vault and Backup Exec, only Windows option is available, as these products support only Windows operation system.

**Target Host Name** Enter the name of the NetBackup Master Server or Media Server host name from which you want to collect the backup / archiving data.

**5** Click **Next**.

On the Data Collector Details page, the Target Details, Configuration Settings, Log Settings, And Discovered Hosts details are displayed.

**6** Check / enter the following Target Details:

**Product** Displays the name of the product as Veritas NetBackup. You have specified this product name on the Create Data Collector Configuration page.

**Target Host Name** Displays the name of the NetBackup Master Server or Media Server host name that you have specified on the Create Data Collector Configuration page.

**Data Collector Status** By default, the data collector status is Enabled. You can disable the data collection by changing the status.

**7** Enter the following Configuration Settings:

Collection Method	<p>The method using which VBR collects data from NetBackup, that is CLI (command-line interface)</p> <p>The CLI method uses the <code>bpd jobs</code> command to gather job data.</p>
Home Directory	<p>The directory path on the VBR Agent host where the NetBackup application is installed. In case of remote data collection, this is the directory path on the VBR Agent host where RAC (Remote Admin Console) is installed.</p> <p>Example of home directory path on a Windows machine:  <code>C:\Program Files\VERITAS\NetBackup</code></p> <p>Example of home directory path on a Solaris machine:  <code>/usr/opensv/netbackup</code></p>
Volume Manager Home	<p>The directory path on the VBR Agent host where the Volume Manager is installed.</p> <p>Example of Volume Manager location on a Windows machine:  <code>C:\Program Files\VERITAS\Volmgr</code></p> <p>Example of Volume Manager Home location on a Solaris machine: <code>/usr/opensv/volmgr</code></p>
Future Scheduled Jobs	<p>Set this option to Enable, if you want to collect the Scheduled Jobs from NetBackup.</p> <p>The Scheduled Jobs data is collected using the <code>nbpemreq</code> CLI.</p> <p>In case of remote data collection, to collect Scheduled Jobs, you need to specify valid NetBackup user credentials.</p> <p><b>Note:</b> This configuration setting has been added in VBR 6.6. You can now generate reports to view jobs that are scheduled to run in future.</p> <p>See <a href="#">“Reporting on scheduled jobs data”</a> on page 390.</p>
Breakup Jobs	<p>Set this option to Enable, if you want to break up a job (using data from the NetBackup's catalog) so that the size and backup file count have finer granularity.</p> <p>Enabling this option increases the load on the VBR Agent, the load on the master server, and the time it takes to gather and load data. This feature is most effective if you explicitly list multiple paths in your policy include lists in NetBackup.</p> <p>the section called “About Breakup Jobs option”</p>

Role	<p>Set the role to Master or Media to specify that the target host from which NetBackup data collector will collect is a Master Server or a Media Server respectively.</p> <p>If the target host is both a Master Server and a Media Server, then set the role to Master.</p> <p>If you set the role to Master, media and tape drive data for all associated Media Servers will be collected.</p> <p>If you have set the role to Media, media and tape drive data for this particular Media Server will be collected.</p>
Days Per Image Fetch	<p>This configuration setting is relevant for initial data load (data collected for the very first time after a fresh VBR installation). In case of the initial data load, the image size that needs to be collected is huge. By using the Days Per Image Fetch option, you can collect this huge data in chunks.</p> <p>For example:</p> <p>If NetBackup has 15 years of image data that needs to be collected and you have selected 1800 days (5 years) as Days Per Image Fetch, the <code>bpimagelist</code> CLI will be fired for three times to collect 5 years of data each time.</p> <ul style="list-style-type: none"><li>■ The first call to <code>bpimagelist</code> collects data for this period: 15 years ago - 10 years ago</li><li>■ The second call to <code>bpimagelist</code> collects data for this period: 10 years ago - 5 years ago</li><li>■ The third call to <code>bpimagelist</code> collects data for this period: 5 years ago - today</li></ul> <p>In most of the environments, a default value of 1800 days (five years) works fine. However, in case of larger setups where <code>bpimagelist</code> does not successfully return the default, you can set this option to a lower value.</p> <p>The Days Per Image Fetch drop-down list consists of the following values:</p> <ul style="list-style-type: none"><li>■ 1800 days</li><li>■ 360 days</li><li>■ 180 days</li><li>■ 90 days</li><li>■ 30 days</li><li>■ 7 days</li></ul>
Library Capacity	<p>Set this option to Enable if you want to collect the slot count information, which is required for calculating the tape library capacity.</p>

Skip Errors for Tape Drive and Media Usage	<p>Ignore this configuration setting if the role is set to Media.</p> <p>If the role is set to Master, do any of the following:</p> <ul style="list-style-type: none"> <li>■ Select the Skip Errors for Non-configured Media Server option to skip errors that occur while collecting data only from a non-configured media server associated with the target host and continue collecting data.</li> <li>■ Select the Skip Errors for All Media Servers option to skip errors that occur while collecting data from any of the Media Servers associated with the target host and continue collecting data.</li> <li>■ Select the Do Not Skip Errors option if you do not want to skip errors for any Media Server. This terminates the data collection.</li> </ul> <p>Configured Media Server -</p> <p>Non-configured Media Server -</p>
EMM Server Host	Enter the name of the Enterprise Media Manager host associated with this target host.
Date Time Format	Enter the date time format as per the target host locale. The CLIs use this date time format while collecting data.
NetBackup Username	<p>Ignore this configuration setting in the following scenarios:</p> <ul style="list-style-type: none"> <li>■ If you have set the Future Scheduled Jobs option to Disable</li> <li>■ If you want to collect the Scheduled Jobs data from a local NetBackup host.</li> </ul> <p>If you want to collect the Scheduled Jobs data remotely, using the <code>nbpemreq</code> CLI, set the Future Scheduled Jobs option to Enable, and specify valid NetBackup admin credentials.</p> <p>Enter the NetBackup user name.</p>
NetBackup Password	Enter the password of a NetBackup user account.

**8** Enter the following Log Settings:

See [“About NetBackup data collector log files”](#) on page 209.

Level	<p>From the drop-down list, select the granularity level for log information. The log levels are as follows:</p> <ul style="list-style-type: none"><li>■ Off</li><li>■ Severe</li><li>■ Warning</li><li>■ Info</li><li>■ Config</li><li>■ Debug-Fine</li><li>■ Debug-Finer</li><li>■ Debug-Finest</li><li>■ All</li></ul> <p>If you set the log level to 'Off', no logs will be stored for this log level and if you set it to 'All', every bit of the data collector information will be logged. When you set the logging to a particular level, the log information for all levels previous to that level is also stored. For example, if you set the log level to 'Warning', all warnings and errors / exceptions (log information pertaining to the 'Severe' log level) are logged.</p> <p>In Debug type of logs, all CLIs that were fired during data collection are stored, along with the information pertaining to previous log levels.</p>
Max Size (MB)	<p>Enter the maximum size in MB that you want to set for a data collector log file. For example, enter 5, if you want a data collector log file to grow up to 5 MB before it rolls over to the next log file. The number of log files created depends on the Rollover Count that you specify.</p>
Rollover Count	<p>Enter the rollover count for the data collector log files.</p> <p>For example: If you specified the Max Size of a log file as 5 MB and Rollover Count as 4, a log file (say 0.log) can grow up to 5 MB. When the size reaches 5 MB, the log information is pushed to the next log file (say 1.log) and the latest log information is stored in the first log file (that is 0.log). Thus, when four log files are full and log information is still increasing, the oldest log information that is in 3.log file is deleted. Thus, at any given time the number of log files is less than or equal to 4 and the latest log information is available in the 0.log file.</p> <p>Example of the log file name: module-002-enterprisevault-server1-0.log</p>

**9** Enter the following Discovered Hosts - Name Qualification Options:

With these options, you can specify the way you want to refer to the Enterprise Vault hosts in Veritas Backup Reporter context.

- |                                    |   |
|------------------------------------|---|
| Append Domain                      | <p>Select this option and add text in the @ text box to append this text to all NetBackup host names.</p> <p>For example: Veritas Backup Reporter has discovered a host name, say 'NetBackup1' from NetBackup database. Veritas Backup Reporter may not be able to refer to 'NetBackup1' using the same host name, while requesting backup data. In this case, select the Append Domain option and add domain name say 'DomainName', which will be appended to the host name, that is NetBackup1@DomainName</p> <p>This is useful if different Master Servers refer to physically different clients by the same name.</p> |
| Via DNS (not recommended for DHCP) | <p>This is a default option. This option enables the Veritas Backup Reporter Agent to perform DNS lookup on the NetBackup host names to get the associated IP addresses. Use this option only if you have a common DNS environment for NetBackup hosts and Veritas Backup Reporter Agent.</p> <p><b>Caution:</b> Do not use this setting if the hosts in NetBackup environment use DHCP, because there may be conflicts with the same IP addresses being used by the different servers at different times.</p>  |
| Do Not Qualify                     | <p>Select this option if you do not want to Veritas Backup Reporter Agent to modify the host names discovered from NetBackup.</p> <p><b>Caution:</b> Do not use this option if you do not have unique host names across NetBackup environment. Because HostA from one Netbackup Master Server will now match against a HostA discovered from another Master Server and you cannot identify them in reports.</p>   |

**10** Enter the following information regarding data types to be collected:

- |                      |  |
|----------------------|--|
| Configuration Status | Select this check box to collect the associated data type. |
|----------------------|--|

Collectable Data Type	<p>Lists the data types that the NetBackup data collector collects from NetBackup as follows:</p> <ul style="list-style-type: none"><li>■ Tape Drive Information</li><li>■ Media</li><li>■ Policy and Schedule - This data type includes new information pertaining to Policy and Schedule that is collected in VBR 6.6.</li><li>■ Job</li><li>■ Error</li><li>■ Skipped File</li><li>■ Image</li></ul>
Collection Interval (sec)	<p>Enter the collection interval in seconds, minutes, hours, and days. This is the time interval that you want to set between the two consecutive data collections.</p> <p>For example: You have set the Collection Interval to 15 Minutes. The first data collection starts at say 9 AM and continues until all archive records are collected and ends at 11 AM. The next data collection will start at 11.15 AM.</p>
Blackout Period Start Time	<p>Select the start time of a blackout period. The data is not collected for the time specified in Blackout Period Duration, since Blackout Period Start Time.</p>
Blackout Period Duration (hr)	<p>Select the blackout duration in hours, for which the data is not collected since the time specified for the Blackout Period Start Time field.</p> <p>For example: You have set the Blackout Period Start Time as 1:00 PM and the Blackout Period Duration as 2 hours. No data is collected between 1 PM to 3 PM.</p>
Last Successful Data Load	<p>States whether last data load was successful or not.</p> <p>See "<a href="#">Viewing agent status</a>" on page 177.</p>
Collection Status	<p>Displays the status of data collection. You can either resume or pause the data collection.</p>

**Fetch Size** Select the number of records of the data type that you want to fetch at a time.

For example:

If the Fetch Size is set 500, the Veritas Backup Reporter Agent can at a time send maximum of 500 Archive records to the Management Server. If the Agent has collected 600 Archive records from the Enterprise Vault database, it can send them to the Management Server in two chunks, 1st chunk of 500 records and 2nd one of 100.

Symantec recommends that you set the fetch size to 5000 for the Archive data type because of the following reason:

There can be thousands of records of the Archive data type that Agent collects from the Enterprise Vault database, in a given time interval. The Agent sends these records to the Management Server, as soon as it receives them from the Enterprise Vault database. If you set the fetch size of the Archive data type to a value lesser than 5000, the data collection and data transmission by the Agent will not be in sync and the Agent performance will drop.

## 11 Click Save.

### About NetBackup data collector log files

Use the NetBackup data collector log files while troubleshooting any issues related to NetBackup data collector configuration and data collection. The logs are stored at the following location:

```
Install Path\Symantec\Veritas Backup Reporter\Agent\Logs\module-moduleNumberAsCreated-netbackup-agenthostname-0.log
```

Where *Install Path* is the location where you have installed the Veritas Backup Reporter application. By default *Install Path* is: C:\Program Files

Where *moduleNumberAsCreated* can vary depending on the number of data collectors that you have configured for the Agent and the sequence in which they have configured.

Where *agenthostname* is the name of the Agent host where you have configured the NetBackup data collector.

Example of the NetBackup data collector log file name:

```
module-002-netbackup-server1-0.log or module-002-netbackup-server1-1.log
```

## About Breakup Jobs option

This section describes the NetBackup specific Breakup Jobs option that you can set while configuring Netbackup data collector. You can either enable or disable breaking up the NetBackup jobs.

See “[Configuring NetBackup data collector](#)” on page 201.

If you do not want to display backup job status at the file system level, disable the breakup jobs option on the data collector configuration page for the NetBackup master server host. With Breakup Jobs enabled, you must place a separate object for each file system when you construct a view using the View Builder. On the other hand, with Breakup Jobs disabled, you must place only one file system object (named `Other`) into your view.

---

**Note:** Do not enable the Breakup Jobs option if Oracle RMAN backup policies are in use in the environment. The use of Breakup Jobs with Oracle RMAN results in one file system object per RMAN backup that affects the performance.

---

To demonstrate the effect of Breakup Jobs, a job for HostA and path C:\ reference the following:

- With breakup jobs enabled, host HostA and file system C:\
- With breakup jobs disabled, host HostA and file system Other

### About the effects of enabling the Breakup Jobs option

[Table 5-5](#) shows some NetBackup policy configurations and the resulting ways in which data is collected with Breakup Jobs enabled. (With Breakup Jobs disabled, every job references the file system object named `Other`.)

---

**Note:** Multistream policies generally create breakup jobs with only one path.

---

**Table 5-5** Resultant paths with Breakup Jobs option enabled

Multistream	File systems included	Number of NetBackup jobs	Paths shown in NetBackup	Paths shown in Veritas Backup Reporter views
No	C:\ D:\ [OR] C:\ NEW_STREAM D:\ [OR] NEW_STREAM C:\ NEW_STREAM D:\	1	C:\ D:\	C:\ D:\ Other
No	C:\	1	C:\	C:\
No	ALL_LOCAL_DRIVES	1	ALL_LOCAL_DRIVES	ALL_LOCAL_DRIVES
Yes	C:\ D:\	1+2	C:\ D:\ <hr/> [Detail file-list format] BACKUP C:\ USING * BACKUP D:\ USING *	C:\ D:\ Other
Yes	C:\	1+1	C:\ <hr/> [Detail file-list format] BACKUP C:\ USING *	C:\ Other

**Table 5-5** Resultant paths with Breakup Jobs option enabled (*continued*)

Multistream	File systems included	Number of NetBackup jobs	Paths shown in NetBackup	Paths shown in Veritas Backup Reporter views
Yes	C:\ NEW_STREAM D:\	1+2	C:\ NEW_STREAM D:  ----- [Detail file-list format] BACKUP C:\ USING * BACKUP D:\ USING *	C:\ D:\ Other
Yes	ALL_LOCAL_DRIVES	1+Number of drives	ALL_LOCAL_DRIVES Shadow Copy Components:\	C:\ D:\ ALL_LOCAL_DRIVES Shadow Copy Components:\
Yes	NEW_STREAM C:\ NEW_STREAM D:\	1+2	NEW_STREAM C:\ NEW_STREAM D:\  ----- [Detail file-list format] BACKUP C:\ USING * BACKUP D:\ USING *	C:\ D:\ Other

“Other” file system objects can occur when the Breakup Jobs option is enabled. Whether the option is enabled or not, VBR collects sum of sizes of each file system. The sum when the option is enabled may not be equal to the sum when the option is not enabled. If the sums are not equal, VBR create Other file system to make up the difference.

## Collecting data from NBAC enabled NetBackup Master Server

Veritas Backup Reporter can collect data from a NetBackup Master Server that is NBAC (NetBackup Access Control) enabled. This requires a few steps to be carried out before actually collecting the NetBackup data.

---

**Caution:** This section provides steps pertaining only to Solaris platform.

---

### To collect data from NBAC enabled NetBackup Master Server

- 1 In NBAC, create “NBU\_Reporter” group with Read permission on all objects.
- 2 Run the following command on NetBackup Master Server:

```
bash-3.00$ /usr/opensv/netbackup/bin/goodies/nbac_cron -setupCron  
  
This application will generate a VERITAS private domain identity  
that can be used in order to run unattended cron and/or at jobs.  
User name to create account for (e.g. root, JSmith etc.):  
vbrmonitor  
  
Password:  
  
Password  
  
Access control group to add this account to [NBU_Admin]:  
NBU_Reporter  
  
Do you wish to register this account locally for root(Y/N)? y
```

#### The following message is displayed:

```
In order to use the account created please login as the OS  
identity that will run the at or cron jobs. Then run nbac_cron  
-setupcron or nbac_cron -setupat. When nbac_cron -setupcron or  
nbac_cron -setupat is run the user name, password and  
authentication broker will need to be supplied. Please make note  
of the user name, password, and authentication broker. You may  
rerun this command at a later date to change the password for an  
account.
```

```
Operation completed successfully.
```

**3 Run the following command on NetBackup Master Server:**

```
bash-3.00# /usr/opensv/netbackup/bin/admincmd/bpnbaz/bpnbaz  
-AddUser NBU_Reporter
```

The following message is displayed:

```
This application will now create your cron and/or at identity.  
Authentication Broker: NBUMaster.veritas.com Name: vbrmonitor
```

Password:

```
<same password>
```

```
Created cron and/or at account information. To use this account  
in your own cron or at jobs make sure that the environment  
variable VXSS_CREDENTIAL_PATH is set to  
"/usr/opensv/home/.vxss/credentials.crat"
```

Operation completed successfully.

**4 Check if the vbrmonitor user is added to the required group or not, by running the following command:**

```
bash-3.00# /usr/opensv/netbackup/bin/admincmd/bpnbaz  
-ListGroupMembers NBU_Reporter
```

If the user is not added to the NBU\_Reporter group, you have to manually add it to the group as follows:

■ Run the following command on NetBackup Master Server:

```
bash-3.00# /usr/opensv/netbackup/bin/admincmd/bpnbaz/bpnbaz  
-AddUser NBU_Reporter  
vx:CronAtUsers@nbuserver.xxx.veritas.com:CronAt_vbrmonitor
```

The following message is displayed:

Operation completed successfully.

**5 In Netbackup's bp.conf add the following entry:**

```
AUTHENTICATION_DOMAIN = CronAtUsers "VBR Cron User" VXP  
nbuserver.xxx.veritas.com 0
```

**6 Look for "start\_ccsvagent()" after "export EAT\_HOME\_DIR" text in the /opt/VRTSccsva/bin/vbragent file and insert the following lines:**

```
VXSS_CREDENTIAL_PATH=<Path to cert file created in step 3>  
export VXSS_CREDENTIAL_PATH
```

**7 Save the vbragent file and restart the Agent.**

## To collect data from NBAC enabled NetBackup Master Server

### 1 Log on to the NetBackup Master Server as 'root'.

Run the following command on NetBackup Master Server:

```
bpnbat -login
```

Enter the following information or press Enter to specify the default values.

```
Authentication Broker [swsx16.vxindia.veritas.com is default]:
```

```
Authentication port [0 is default]:
```

```
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd) [unixpwd is default]:
```

```
Domain [swsx16.vxindia.veritas.com is default]:
```

```
Login Name [root is default]:
```

```
Password:
```

The following message is displayed:

```
Operation completed successfully.
```

### 2 Create 'NBU\_Reporter' group with Read permission on all objects.

### 3 Run the following command:

```
/usr/openv/netbackup/bin/goodies/nbac_cron -addat
```

The following message is displayed:

```
This application will generate a Symantec private domain identity that can be used in order to run unattended cron and/or at jobs.
```

```
User name to create account for (e.g. root, JSmith etc.):
```

```
vbrmonitor
```

```
Password:
```

```
Password:
```

```
Access control group to add this account to [NBU_Admin]:
```

```
NBU_Reporter
```

```
Failed to add user "CronAt_vbrmonitor" to NetBackup access control group "NBU_Reporter" Optional VxSS libraries not initialized.
```

**4** Run the following command:

```
vssat listpdprincipals --pdrtype ab --domain CronAtUsers  
listpdprincipals  
-----  
-----  
Principal Count: 2  
Principal Name: admin  
Principal Type: Unknown  
Principal Name: CronAt_vbrmonitor  
Principal Type: User  
-----
```

Make sure the user is created under NBU\_Reporter group, if not then add the user with `bpnbaz -adduser`.

**5** Run the following command:

```
/usr/opensv/netbackup/bin/admincmd/bpnbaz -ListGroupMembers  
NBU_Reporter
```

The following message is displayed:

```
Operation completed successfully.
```

**6** Run the following command:

```
/usr/opensv/netbackup/bin/admincmd/bpnbaz -AddUser NBU_Reporter  
vx:CrontAtUsers@swsx16.vxindia.veritas.com:CrontAt_vbrmonitor
```

The following message is displayed:

```
Operation completed successfully.
```

**7 Run the following command:**

```
/usr/opensv/netbackup/bin/admincmd/bpnbaz -ListGroupMembers  
NBU_Reporter
```

```
=====
```

Enter the following information:

Type: **User**

Domain Type: **vx**

Domain: **CrontAtUsers@swsx16.vxindia.veritas.com**

Name: **CrontAt\_vbrmonitor**

The following message is displayed:

```
Operation completed successfully.
```

**8 Run the following commands:**

```
export EAT_HOME_DIR=/opt/VRTSbrat
```

**9 export EAT\_DATA\_DIR=/opt/VRTSbrat/data****10 /usr/opensv/netbackup/bin/goodies/nbac\_cron -setupat**

Run the following command:

```
This application will now create your cron and/or at identity.
```

Enter the following information:

Authentication Broker: **swsx16.vxindia.veritas.com**

Name: **vbrmonitor**

Password:

The following message is displayed:

```
You do not currently trust the server: swsx16.vxindia.veritas.com,  
do you wish to trust it? (Y/N):
```

Enter **y**

```
Created cron and/or at account information. To use this account  
in your own cron or at jobs make sure that the environment  
variable VXSS_CREDENTIAL_PATH is set to "//.vxss/credentials.crat"  
Operation completed successfully.
```

**11 Run the following command:**

```
cp /.vxss/credentials.crat /opt/VRTScsva/
```

**12** Run the following command:

```
Edit /opt/VRTSccsva/bin/vbragent  
  
start_ccsvcagent()  
  
.....  
  
VXSS_CREDENTIAL_PATH=/opt/VRTSccsva/credentials.crat  
  
export VXSS_CREDENTIAL_PATH
```

**13** Add following to `/usr/opensv/netbackup/bp.conf`

```
AUTHENTICATION_DOMAIN = CronAtUsers "VBR Cron User" VXPDP  
swsx16.vxindia.veritas.com 0
```

**14** Restart NetBackup services

**15** Restart VBR Agent

See [“Stopping and starting the Veritas Backup Reporter Agent”](#) on page 115.

## About the Library Capacity option

A NetBackup data collector can collect tape library capacity data or slot count information from all NetBackup Media Servers.

To collect library capacity data, the VBR agent must communicate with the host where NetBackup volume database resides. The NetBackup volume database can be on a separate media server host or on a master server host acting as a media server.

By using the Library Capacity option on the NetBackup data collector configuration page, you can either enable or disable the collection of slot count information. The slot count is required for calculating the tape library capacity.

See [“Configuring NetBackup data collector”](#) on page 201.

The NetBackup data collector collects the library capacity from all media servers connected to a master server. If the number of media servers is high, a significant drop in the performance of Veritas Backup Reporter can occur. To avoid this drop, disable the collection of slot count information. However, if you have never collected the slot count, reports do not show the correct tape library capacity data because the tape library capacity depends on the slot count. To get the exact total library capacity without dropping the performance, you can set the Library Capacity option to Enable for the first time, collect the slot count information, and then disable the Library Capacity option.

To collect the library capacity data, the VBR Agent must be authorized to connect to the master server along with all media servers. If it is not authorized, it results into the following:

- Data cannot be collected from the tape drives attached to the media server.
- The tape drive usage collection event fails.

---

**Note:** You can collect the library capacity locally as well as remotely.

---

The NetBackup master server or media server is connected to a backup device, for example, a tape drive or a tape library.

## NetBackup data collection checklist

Ensure the following before you start collecting data from NetBackup:

- The Veritas Backup Reporter Agent is deployed on an appropriate host. See [“About Veritas Backup Reporter Agent deployment”](#) on page 42.
- The Agent service is running. Restart the Agent service, if it has stopped. See [“Stopping and starting the Veritas Backup Reporter Agent ”](#) on page 115.
- NetBackup services are running.
- NetBackup data collector is configured properly. See [“Configuring NetBackup data collector”](#) on page 201.
  - The Data Collector Status is set to Enabled.
  - The configuration settings are appropriate.
  - The data types to be collected from the NetBackup Master Server are selected.
  - The Collection Interval and Blackout Period are set appropriately.
- If you want to collect data from the NetBackup Master Server that is NBAC enabled, carry out the procedure described in the following section: See [“Collecting data from NBAC enabled NetBackup Master Server ”](#) on page 213. Collecting data from NBAC enabled NetBackup Master Server

In case of remote data collection - VBR Agent and NetBackup Master Server are installed on different hosts - ensure the following points in addition to the checklist points mentioned earlier.

- Verify the link between the Agent host and the target NetBackup host is established by running the following command from the Agent host:

```
Solaris          /usr/opensv/netbackup/bin/admincmd/bpdbjobs  
                -report -all_columns -M localhost
```

```
Windows         C:\Program  
                Files\Veritas\NetBackup\bin\admincmd\bpdbjobs  
                -report -m NBUserServer
```

If the command returns NetBackup data from the NetBackup server, then the link is functioning correctly.

- Make sure that the remote Agent host has Remote Admin Console (RAC) or Master or Media Server installed, to collect data from the Master Server that you want to monitor / report on.

You can find the RAC installation option at the following location: **NetBackup Installation Wizard > Master Server option > Remote Admin Console.**

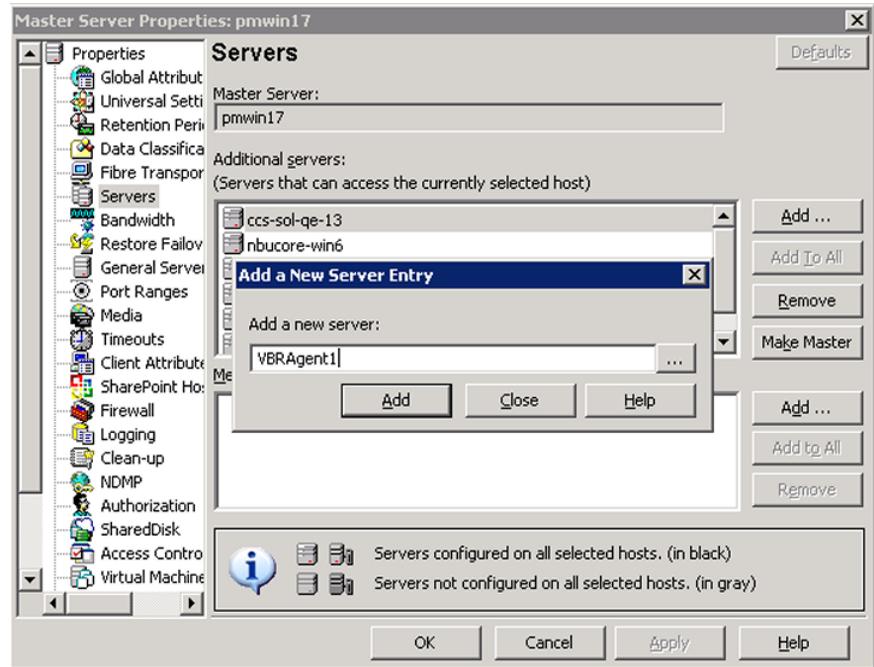
Solaris host does not support RAC.

Make sure that NetBackup binaries are installed in the default location on the target NetBackup server:

```
Solaris          /usr/opensv/netbackup
```

```
Windows         C:\Program Files\Veritas\NetBackup
```

- Make sure you have added the remote VBR Agent host entry in the NetBackup Master Server host properties. Restart the NetBackup Master Server.
  - On Solaris host, add the Agent host entry in the NetBackup Mater Server `bp.conf` file, as `SERVER=VBRAgentHostName`.
  - On Windows host add the Agent host enter as shown in the following figure:



## Collecting data from Backup Exec

This section describes data collection from Backup Exec.

In VBR 6.6, Skipped File and Media data can also be collected from Backup Exec.

---

**Note:** VBR 6.6 does not support data collection from Backup Exec 9.x version. You need to create a data collector to collect data from Backup Exec 10d and later versions. However, you can run the reports on the Backup Exec 9.x data.

---

For other tasks related to data collector, refer to the following sections:

See [“Modifying data collector configurations”](#) on page 195.

See [“Collecting data by the force poll method”](#) on page 196.

See [“Copying data collector configurations”](#) on page 197.

See [“Deleting data collectors”](#) on page 197.

---

**Caution:** The Backup Exec data collector requires the following component to be installed on the VBR Agent host, to collect data properly.

Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) that is vcredist\_x86.exe

VC Redistributable Package is available at:

[http://www.microsoft.com/downloads/details.aspx?](http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en)

[familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en)

Once you install this component on the Agent host, configure the Backup Exec data collector as described in the following section.

---

### To configure Backup Exec data collector

- 1 Click **Settings > Global Settings > Agent Configuration**.
- 2 On the Agents page, click an agent for which you want to configure a Backup Exec data collector.
- 3 On the Agent/Server Information page, click the **Create** link.
- 4 On the Create Data Collector Configuration page, select Symantec Backup Exec Windows from the Product drop-down list.
- 5 In the Target Host Name text box, enter the Backup Exec Server host name, from which you want to collect data.
- 6 Click **Next**.
- 7 On the Data Collector Details page, specify the log settings for the Backup Exec data collector.
- 8 Specify the following Backup Exec data collector configuration settings:

User Name	Enter the name of the user account required to connect to the Backup Exec database.
Password	Enter the password of this user account.
Version	Select the version of the Symantec BackupExec server - 10.x, 11.x, or 12.x - from which you want to collect data.

- 9 Select Discovered Hosts - Name Qualification Options.
- 10 Select the data types to be collected.

- 11 Select the collection interval, blackout period start time and duration, and fetch size.

Data types, Error and Skipped File do not have the Fetch Size option to be selected, as they are collected as part of Job data type.

For more details on log, collection interval, and other data collector settings, refer to the following section:

the section called “Configuring a data collector”

- 12 Click **Save**.

## Collecting data from PureDisk

Veritas Backup Reporter supports collection of data from Veritas NetBackup PureDisk. The collected data is stored in the Veritas Backup Reporter database, based on which you can generate reports. Veritas Backup Reporter can collect Job and Policy data types from a PureDisk Storage Pool Authority (PureDisk SPA).

PureDisk SPA and its components run on the PureDisk operating system (PDOS). The Single Instance Storage (SIS) or deduplication technology of NetBackup PureDisk is unique in storage and backup industry. PureDisk identifies files and data segments that contain identical data and treats them as a single instance of a file, which it backs up only once. This helps you to save storage space. Attributes of identical files, such as name and date of modification can vary.

While backing up a file, PureDisk determines whether multiple instances of the file are present on hosts across the network, including remote hosts. By using the deduplication technology, PureDisk stores only one instance of the file.

---

**Caution:** Veritas Backup Reporter Agent cannot be installed on PureDisk SPA host, as Veritas Backup Reporter does not support PDOS.

---

A single Veritas Backup Reporter Agent can collect data from multiple PureDisk SPA hosts.

---

**Note:** Symantec Product Authentication Service (AT) Root Broker can be present on the Veritas Backup Reporter Management Server host or PureDisk SPA host or any external host. If you want to use an AT Root Broker that is installed on a host different than the management server, you need to downgrade it to Authentication Broker (AB) mode.

---

[Table 5-6](#) describes the steps that you need to carry out to collect data from PureDisk.

**Table 5-6** Steps to collect data from PureDisk

Step number	Step	Reference topic
1	Understand the Symantec Authentication Service configuration.  For more information on AT configuration, refer to the AT documentation.	See <a href="#">“About the Symantec Product Authentication Service”</a> on page 25.
2	Review the AT configuration scenarios specific to PureDisk.	See <a href="#">“About AT configuration scenarios specific to PureDisk backup product”</a> on page 226.

**Table 5-6** Steps to collect data from PureDisk (continued)

Step number	Step	Reference topic
3	<p>As per your requirements, configure AT Root Broker on the VBR Management Server or PureDisk SPA host.</p> <p><b>Note:</b> You have the option to configure the AT at the time of installing VBR. If you want to change the AT configuration after the installation, you can do that manually.</p> <p>If you are moving the Root Broker of VBR Management Server to the external / remote or PureDisk SPA host, create Principal user on the this remote or PureDisk SPA host.</p> <p>If you are moving the Root Broker of PureDisk SPA to the VBR Management Server or any other external / remote host, create Principal user on the this remote or Management Server host and modify the AT configuration on the PureDisk SPA host.</p> <p><b>Note:</b> For the most recent information on modifying the AT configuration in PureDisk, refer to the PureDisk documentation.</p>	<p>See <a href="#">“Moving the Root Broker from PureDisk SPA host to VBR Management Server”</a> on page 230.</p>
4	<p>After changing the AT configuration on the VBR Management Server, run the agentauth command on all VBR Agent hosts connected to this Management Server. This will update the Authentication Broker information on the Agent hosts.</p>	
5	<p>Start the Management Server and Agent services.</p> <p><b>Note:</b> Step 3 to Step 5 have been described in the same ‘Modifying AT configuration manually’ section.</p>	
6	<p>Configure PureDisk data collector.</p>	<p>See <a href="#">“Configuring NetBackup PureDisk data collector”</a> on page 229.</p>

---

**Caution:** To collect data from PureDisk 6.2.2 host, you need to carry out a few additional steps. You need to install release update on PureDisk 6.2.2 host.

See [“Installing a release update on PureDisk 6.2.2 host”](#) on page 233.

---

## About AT configuration scenarios specific to PureDisk backup product

This section describes various configuration scenarios for AT (Symantec Authentication Service) that you should take into account before configuring PureDisk data collector.

The possible scenarios are as follows:

[Scenario 1: Local Agent - Local Root Broker](#)

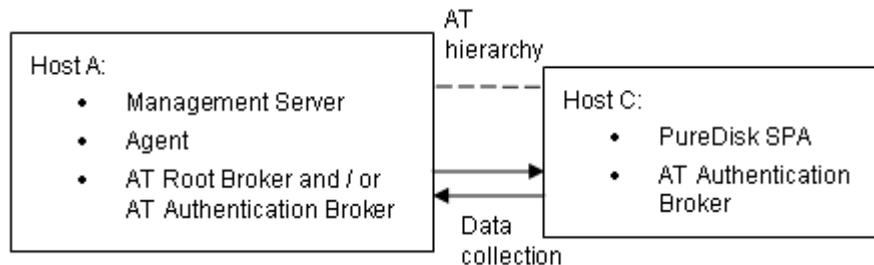
[Scenario 2: Remote Agent - Local Root Broker](#)

[Scenario 3: Local Agent - External Root Broker](#)

[Scenario 4: Remote Agent - External Root Broker](#)

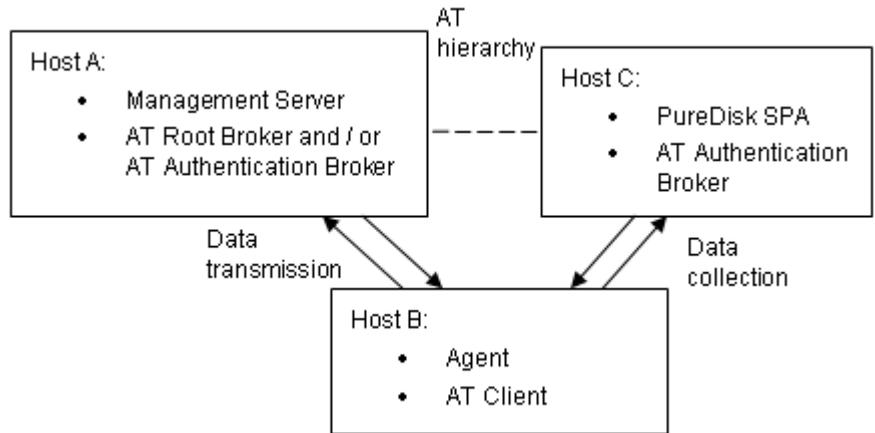
### Scenario 1: Local Agent - Local Root Broker

The following block diagram describes scenario 1 in which, Veritas Backup Reporter Agent and AT Root Broker are installed on the Veritas Backup Reporter Management Server host.



### Scenario 2: Remote Agent - Local Root Broker

The following block diagram describes scenario 2 in which AT Root Broker is installed on the Veritas Backup Reporter Management Server host and Agent is installed on a separate host.

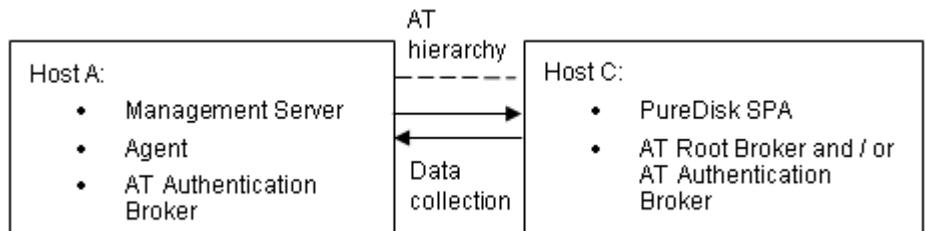


### Scenario 3: Local Agent - External Root Broker

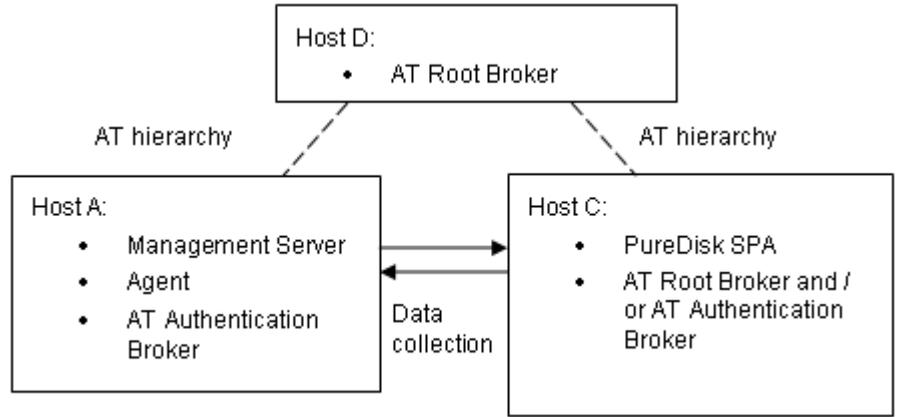
The following block diagrams describe scenario 3 in which Veritas Backup Reporter Agent is installed on the Management Server host and AT Root Broker is installed on PureDisk SPA host or some external host.

For Veritas Backup Reporter application, if you want to use an AT Root Broker that is installed on a host different than the management server, you need to downgrade it to Authentication Broker (AB) mode.

Root Broker on PureDisk SPA host



Root Broker on external host

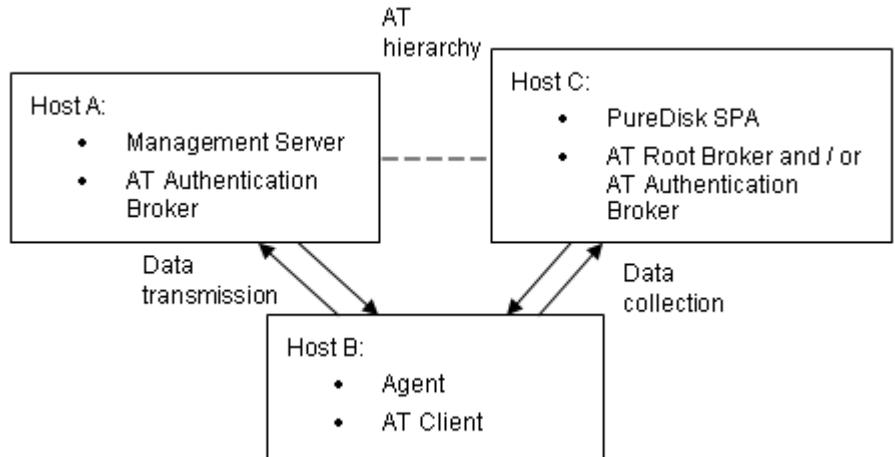


### Scenario 4: Remote Agent - External Root Broker

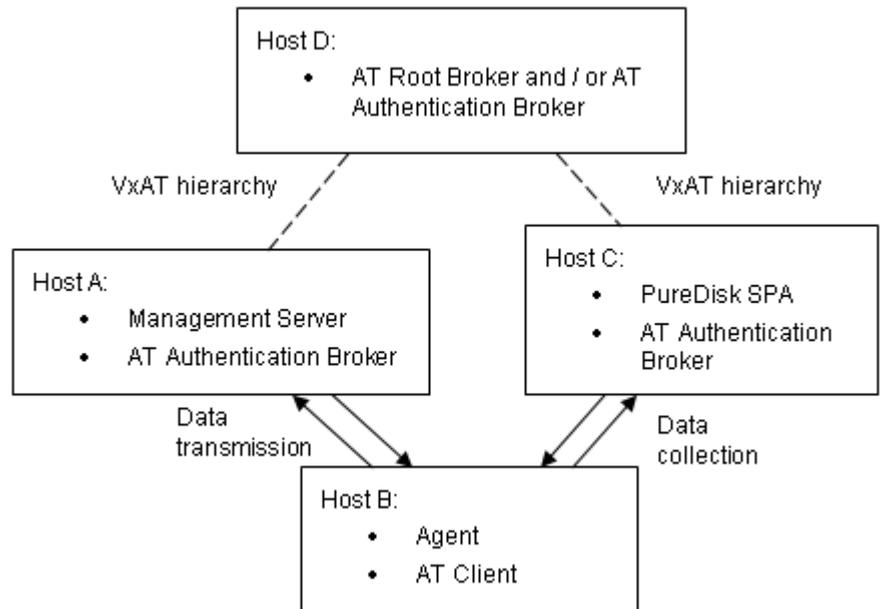
The following block diagram describes scenario 4 in which Veritas Backup Reporter Agent and Management Server host are installed on different hosts and AT Root Broker is installed on PureDisk SPA host or some external host.

For Veritas Backup Reporter application, if you want to use an AT Root Broker that is installed on a host different than the management server, you need to downgrade it to Authentication Broker (AB) mode.

Root Broker on PureDisk SPA host



Root Broker on external host



## Configuring NetBackup PureDisk data collector

This section provides the procedure to configure NetBackup PureDisk data collector on the Veritas Backup Reporter UI.

### To configure NetBackup PureDisk data collector

- 1 Click **Settings > Global Settings > Agent Configuration**.
- 2 On the Agents page, click an agent for which you want to configure a PureDisk data collector.
- 3 On the Agent/Server Information page, click the **Create** link.
- 4 On the Create Data Collector Configuration page, select Veritas PureDisk from the Product drop-down list.
- 5 Enter the PureDisk SPA host name.
- 6 Click **Next**.

- 7 On the Data Collector Details page, specify the following PureDisk variable:

Product Version	Select Veritas PureDisk version - 6.2, 6.2.1, 6.5, 6.2.2, 6.5.0.1, or 6.5.1
-----------------	---

For more details on log, collection interval, and other data collector settings, refer to the following section:

the section called “Configuring a data collector”

- 8 Click **Save**.

---

**Caution:** To collect data from PureDisk 6.2.2 host, you need to carry out a few additional steps. You need to install release update on PureDisk 6.2.2 host.

See [“Installing a release update on PureDisk 6.2.2 host”](#) on page 233.

---

## Moving the Root Broker from PureDisk SPA host to VBR Management Server

This section describes how to move the AT Root Broker from PureDisk SPA host to VBR Management Server.

---

**Note:** For the most recent information on AT configuration in PureDisk, refer to the PureDisk documentation.

---

- 1 On the VBR Management Server host, open the command Prompt and change directory to the Authentication Services bin folder:

Windows	C:\>cd Program Files\VERITAS\Security\Authentication\bin
Solaris	cd /opt/VRTSat/bin

- 2 Find the root domain of the VBR Root + AB Broker Host

Windows	C:\Program Files\VERITAS\Security\Authentication\bin>vssat listpd --pdrtype root
Solaris	./vssat listpd -pdrtype root

Example output:

Domain(s) Found 1

Domain Name root@vbr65m.myline.com

Expiry Interval 0

- 3 Create an authentication broker (AB) identity for the existing PureDisk SPA on the VBR Server as follows:

Windows	C:\Program Files\VERITAS\Security\Authentication\bin>vssat addprpl --pdrtype root --domain root@vbr65m.myline.com --prplname pd65n1.myline.com --password my_password --prpltype service
Solaris	/opt/VRTSat/bin/vssat addprpl --pdrtype root --domain root@vbr65m.myline.com --prplname pd65n1.myline.com --password my_password --prpltype service

Example output: createprpl

Created Principal: pd65n1.myline.com

- 4 On the PureDisk SPA host, locate and copy the root\_hash file from the VBR Management host to the PureDisk SPA host.

Do not overwrite the existing root\_hash, place in an alternate location.

Windows C:\Program  
Files\VERITAS\Security\Authentication\bin\root\_hash

Solaris /opt/VRTSat/bin/root\_hash

- 5 Run the following command to reconfigure the root broker on PureDisk 6.5 SPA:

```
/opt/pdinstall/edit_topology.sh
```

- 6 In the Topology Editor, select **Main Menu > Configure root broker**.

Select **Root Broker Menu > Root Broker is on an external node**. The following screen is displayed.

External root broker

IP/Hostname	[Redacted]
Root broker port	2821
Authentication broker login	[Redacted]
Domain name	[Redacted]
Domain type	vx
Location of root hash (full path)	[Redacted]
Host name of this SPA	pd65n1.myline.com

< OK >      <Cancel>

**7** Enter the following information on this screen:

IP/Hostname	Enter VBR Management Server host name. For example: vbr65m.myline.com
Root broker port	Enter default port, 2821
Authentication broker login	Enter principal user name created on VBR Management Server host, for example: pd65n1.myline.com
Domain name	Enter the domain name. For example, root@vbr65m.myline.com
Domain type	Enter the domain type, for example: vx
Location of root hash (full path)	Enter location of root hash. /var/tmp/root_hash
Host name of this SPA	Enter PureDisk SPA host name. For example, pd65n1.myline.com

**8** On the next screen, enter the authentication password and click **OK**. Save the configuration and exit.**9** Apply the new configuration by running the following command:

```
/opt/pdconfigure/scripts/atconfig/configure_at.sh
```

## Installing a release update on PureDisk 6.2.2 host

This section describes the procedure that you should carry out before collecting data from PureDisk 6.2.2 host. To collect data in Veritas Backup Reporter, you need to install a release update on a PureDisk 6.2.2 host.

**To install a release update on PureDisk 6.2.2 host**

- 1** On the PureDisk Web UI, make sure that no PureDisk jobs are currently running or are scheduled to be run.
- 2** Log out from the PureDisk Web UI.
- 3** Download the release update binaries from the following location:

```
/net/susa/Storage/data/fsdev.lcr.bdc.symantec.com/fs/builds/world/  
EEBs/6.2.2/NB_PDE_6.2.2_EEB12-vbr_job_stats-try0/linux/  
NB_PDE_6.2.2_EEB12-vbr_job_stats-try0.tar
```

- 4 Type the following command:

```
tar -C / -xf /root/NB_PDE_6.2.2_EEB12-vbr_job_stats-try0.tar ./opt
```

- 5 Type the following command to run and install the binaries:

```
/opt/pdinstall/apply-NB_PDE_6.2.2_EEB12-vbr_job_stats-try0.sh
```

If the `topology.ini` file is encrypted, the software prompts you for the password to decrypt this file.

The binaries automatically pushes the application to all nodes in the storage pool and to all clients. At the end of a successful installation, the software prompts you to encrypt the `topology.ini` file.

## Collecting data from Legato Networker

The variables to configure for the EMC Legato Networker data collector are as follows:

Home Directory	The home directory for the EMC Legato Networker installation.
Location of messages file	The directory path for the log file containing group-complete messages. This path may be absolute or relative to <code>homeDirectory</code> . The default file name is <code>messages</code> .  To increase the efficiency of the Networker data collector, configure Networker to create a log that contains only group complete messages, and point <code>messagesFile</code> to this log
Location of <code>mminfo.exe</code>	The directory path of the <code>mminfo</code> Command-Line Interface (CLI), absolute or relative to <code>homeDirectory</code>
Location of <code>nsradmin.exe</code>	The directory path of the <code>nsradmin</code> CLI, absolute or relative to <code>homeDirectory</code>
Location of <code>nsrres</code> file	The Networker resource file to use instead of the default file used by <code>nsradmin</code> (Optional)
Location of <code>nsr</code> file	Output of an <code>nsradmin</code> command (Optional)  The Veritas Backup Reporter console displays <code>nsrResFile</code> , <code>nsrFile</code> , and <code>mminfoFile</code> even though these variables are optional and should be set by advanced users only.
Location of <code>mminfo</code> file	Output of <code>mminfo</code> (Optional)

For more details on log, collection interval, and other data collector settings, refer to the following section:

the section called “Configuring a data collector”

## Collecting data from IBM Tivoli Storage Manager

Veritas Backup Reporter supports the collection of the following data types from IBM Tivoli Storage Manager (TSM):

The variables to configure for the IBM Tivoli Storage Manager data collector are as follows:

Home Directory	The home directory for the Tivoli Storage Manager installation. (This variable can be left blank.)
TSM ID	An administrator-level login used to connect to the Tivoli Storage Manager server. (The default is <code>admin</code> .)
TSM Password	The password for the account (specified in <code>tsmId</code> ) for connecting to the TSM server. (The default password is <code>admin</code> .)
TSM Server Port	(Windows only) The TCP port on the TSM server through which the data collector establishes a connection.  The TSM Server Port has no effect on Solaris. The Solaris data collector uses only product host settings.
dsmConfig	The path to the <code>dsm.opt</code> file.
dsmDir	The path where files to be run <code>dsmadm</code> reside.
dsmadm Location	The path of TSM administrative client ( <code>dsmadm</code> ).

---

**Note:** The TSM product environment variables `DSM_CONFIG` and `DSM_SYS` point to the `dsmadm` required files `dsm.opt` and `dsm.sys` (Solaris and AIX). For more information, refer to your TSM documentation.

---

Specify the TSM server host (also called product host) value for the TSM data collector in the following manner:

**Windows**

Use the fully qualified host name. In short, product host is the value that you can use with the `dsmadm -tcpserveraddress` option. For example, the following entries are valid for product host:

```
Host.sample.domain.com
```

Host

assuming that Host can be fully qualified.

**Solaris and AIX**

The product host must be the value specified in the `dsm.sys` file, for tag `SErvername` (note the case). In short, product host is the value that you can use with the `dsmadm -se` option. The following is a sample `dsm.sys` file:

```
*****  
SErvername server_a COMMmethod  
CoMMmethod TCPip  
TCPPort 1500  
TCPSErveraddress 255.255.255.255  
SERVERNAME MYHOST.Veritas.COM  
TCPSErverADDRESS 255.255.255.255  
NODENAME myhost.mycompany.com  
*****
```

For more details on log, collection interval, and other data collector settings, refer to the following section:

the section called “Configuring a data collector”

## Collecting data from CommVault

The variables to configure for the CommVault Galaxy Backup & Recovery data collector are as follows:

- User Name** The name of the user account required to connect to CommVault database.
- Password** The password for this user account.
- Port** The optional port required to connect to database. The default port is 1433.

---

**Note:** Because CommVault uses an MS SQL Server 2000 database to store data collected by the data collector, you must download the MS SQL Server 2000 JDBC drivers at <http://www.microsoft.com/downloads/details.aspx?FamilyID=07287b11-0502-461a-b138-2aa54bfdc03a&displaylang=en>.

---

Copy the following three files to \$CCSVC\_INSTALL/lib:

- msbase.jar
- msutil.jar
- mssqlserver.jar

For more details on log, collection interval, and other data collector settings, refer to the following section:

the section called “Configuring a data collector”

## Collecting data from Enterprise Vault

Veritas Backup Reporter can now collect Enterprise Vault / archive data.

In Veritas Backup Reporter 6.6, a new report category called Archives is added. This report category contains a number of new reports that are generated based on the archive data collected from Enterprise Vault. For example, Count of Messages, Original Size, or Target report.

See “[Reporting on archive data](#)” on page 405.

In Veritas Backup Reporter 6.6, the licensing model is modified to accommodate the new Enterprise Vault support.

See “[About licensing model](#)” on page 160.

In Veritas Backup Reporter 6.6, Java View Builder is enhanced to accommodate the changes related to the Enterprise Vault support.

See “[About Java View Builder enhancements in VBR 6.6](#)” on page 279.

## About Enterprise Vault

Enterprise Vault software application provides a flexible framework for archiving emails, file systems, and collaborative environments. It is supported only on Windows platform.

Enterprise Vault has the following features:

- Policy-controlled archiving
- Seamless retrieval of information

- Powerful search capability
- Compliance retention
- Data compression and single instancing

For more details, refer to Enterprise Vault documentation.

## About data collected from Enterprise Vault

Veritas Backup Reporter categorizes the data collected from Enterprise Vault database into various data types.

[Table 5-7](#) lists the data types in Veritas Backup Reporter that represent type of data collected from Enterprise Vault.

For example, VBR collects Policy and Retention Category data from Enterprise Vault database and stores it as Archive Policy data type.

**Table 5-7** Enterprise Vault data types

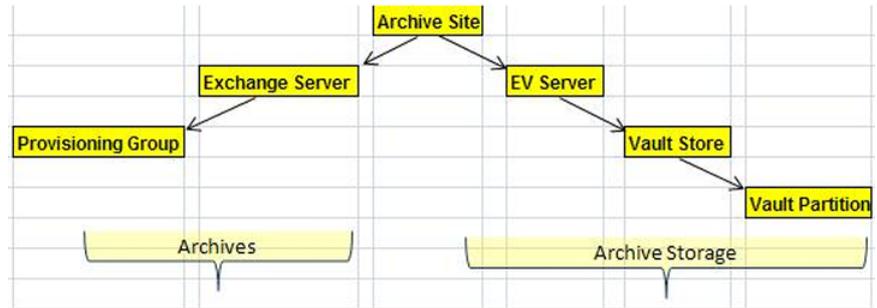
Data type in Veritas Backup Reporter	Data in Enterprise Vault
Archive Policy	Policy and Retention Category
Vault Store	Vault Store and Vault Store Partition
Target	Mailbox, Public Folder, and Provisioning Group
Archive	SaveSet

You can select these data types while configuring the Enterprise Vault data collector. The data collector collects information associated with the selected data types, from Enterprise Vault, as per the specified schedule.

See [“Configuring Enterprise Vault data collector”](#) on page 251.

[Figure 5-1](#) shows the hierarchy of archive data in Enterprise Vault:

**Figure 5-1** Representation of Enterprise Vault data in VBR reports



An archive site is a logical group of hosts that need to archived (Exchange Servers, Provisioning Groups), storage media (vault stores, vault partitions), and Enterprise Vault Servers. It is at the highest level in the Enterprise Vault data hierarchy. Using VBR archive reports you can determine the details about both archiving activities and archival storage, depending on which path you follow to drill-down the site information.

See [“Reporting on archive data”](#) on page 405.

VBR reports present archive data in the following two ways:

**Archiving activities** A few archive reports show details about archiving activities. For example: Details of mailboxes to be archived, original size of data that has been archived, number of mailboxes that are exceeding their warning limits per Exchange Server or Provisioning Group, and so on.

These are all archiving activities, which you can view reports for. These archiving activity reports are available in the ‘Exchange’ report folder of backup reports. VBR 6.6 collects archive data only from Exchange Server. In later versions, VBR will be leveraged to provide reports based on Lotus Notes, SharePoint, and so on.

**Note:** Mailboxes are referred to as targets and individual email is referred to as item.

**Storage of archived data** A few archive reports show details about the storage of archived data. For example: details of vault stores and vault partitions where the archive data has been stored, or how many emails were archived per Enterprise Vault Server, and so on.

## About versions supported by Veritas Backup Reporter

In Veritas Backup Reporter 6.6, you can generate reports based on the archive data pertaining to Microsoft Exchange Server.

Veritas Backup Reporter supports the following versions of Enterprise Vault. It supports all versions of Microsoft SQL Server that are supported by Enterprise Vault.

Enterprise Vault      2007 SP3, 2008

Microsoft SQL Server   2005, 2008

## Planning the Enterprise Vault data collector deployment

Enterprise Vault stores the archive metadata in the directory and storage database residing in Microsoft SQL Server. You need to deploy and configure Enterprise Vault data collector using the Veritas Backup Reporter console, which collects this archive metadata from Microsoft SQL Server.

Veritas Backup Reporter supports local as well as remote archive-data collection. However, Symantec recommends the remote data collection method, in which Veritas Backup Reporter Agent and MS SQL Server are installed on different hosts.

[Table 5-8](#) lists the steps that you need to carry out before configuring the Enterprise Vault data collector for archive-data collection in the Veritas Backup Reporter console.

**Table 5-8**      Planning and deployment steps

Step number	Step	Reference topic
1	<p>Deploy Enterprise Vault data collector in any of the following ways, to collect archive data remotely:</p> <ul style="list-style-type: none"> <li>■ Single-domain mode</li> <li>■ Multi-domain mode</li> <li>■ Standalone mode</li> </ul> <p><b>Note:</b> Symantec recommends that you deploy the Enterprise Vault data collector in single-domain mode.</p>	<p>See “<a href="#">About single-domain deployment mode</a>” on page 242.</p> <p>See “<a href="#">About multi-domain deployment mode</a>” on page 242.</p> <p>See “<a href="#">About standalone deployment mode</a>” on page 243.</p>

**Table 5-8** Planning and deployment steps (*continued*)

Step number	Step	Reference topic
2	<p>Make sure that the user whose credentials you will use for the integrated login has required access rights on the MS SQL Server, where the archive data resides.</p> <p>This can be an existing user, or you can create a new user in MS SQL Server and give required access rights.</p>	See <a href="#">“Accessing MS SQL Server host”</a> on page 243.
3	Depending on the deployment mode you chose, add a user in the appropriate domain or workgroup, which you want to use for integrated login between Agent host and MS SQL Server host.	<p>See <a href="#">“About creating a user in single-domain deployment mode”</a> on page 246.</p> <p>See <a href="#">“About creating a user in multi-domain deployment mode”</a> on page 247.</p> <p>See <a href="#">“About creating a user in standalone deployment mode”</a> on page 247.</p>
4	Install MS SQL Server JDBC driver on the Veritas Backup Reporter Agent host.	See <a href="#">“Installing MS SQL Server JDBC driver”</a> on page 250.
5	For integrated login, configure the Veritas Backup Reporter Agent to run in the context of the user or group that has access to MS SQL Server, where the Enterprise Vault data resides, depending on the Enterprise Vault data collector deployment mode.	See <a href="#">“Configuring the Veritas Backup Reporter Agent properties for integrated login”</a> on page 248.

Once you have deployed the Enterprise Vault data collector, you need to configure it using the Veritas Backup Reporter console and schedule data collection.

See [“Configuring Enterprise Vault data collector”](#) on page 251.

## About Enterprise Vault data collector deployment modes

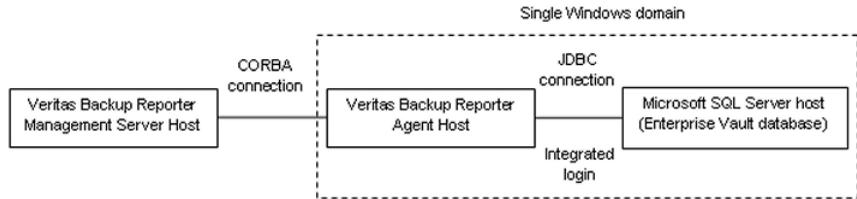
This section describes various deployment modes in which you can deploy Enterprise Vault data collector, depending on your setup. This section mainly talks about the remote Agent deployment modes. However, Enterprise Vault also

supports local Agent deployment. You can deploy the VBR Agent on MS SQL Server host or Management Server host.

## About single-domain deployment mode

Symantec recommends that you deploy the Enterprise Vault data collector in single-domain mode. In this deployment mode, the Veritas Backup Reporter Agent host and the MS SQL Server host (Enterprise Vault database instance) share the same Windows domain.

The following block diagram describes how the Enterprise Vault data collector is deployed in the single-domain mode:



## About multi-domain deployment mode

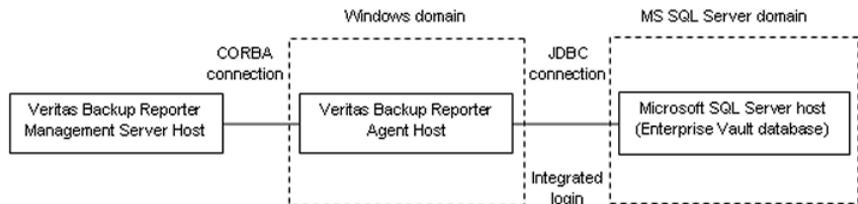
In addition to single-domain mode, you can deploy the Enterprise Vault data collector in multi-domain mode. In this deployment mode, the Veritas Backup Reporter Agent host and the MS SQL Server host (Enterprise Vault database instance) do not share the same Windows domain. The Veritas Backup Reporter Agent host is in a domain different than the SQL Server domain.

---

**Note:** Symantec does not recommend the multi-domain or standalone deployment of the Enterprise Vault data collector.

---

The following block diagram describes how the Enterprise Vault data collector is deployed in the multi-domain mode:



## About standalone deployment mode

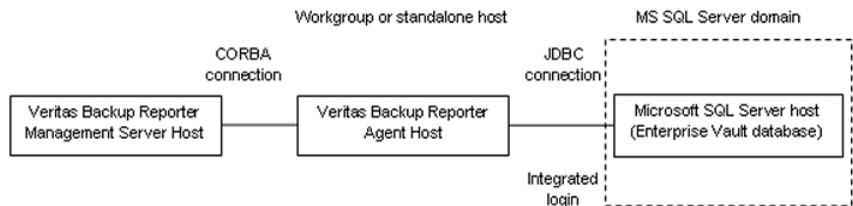
In this deployment mode, the Veritas Backup Reporter Agent host and the MS SQL Server host (Enterprise Vault database instance) do not share the same Windows domain. The Veritas Backup Reporter Agent host is installed on a standalone host.

---

**Note:** Symantec does not recommend the multi-domain or standalone deployment of the Enterprise Vault data collector.

---

The following block diagram describes how the Enterprise Vault data collector is deployed in the standalone mode:



## Accessing MS SQL Server host

This section describes how to give the required rights to a user to access MS SQL Server.

### To give rights to a user to access MS SQL Server

- 1 Create a Windows domain user on the MS SQL Server host. For example, create a user with credentials 'localadmin' and 'pass'.
- 2 Open the MS SQL Server admin console, using SQL Server Management Studio Express or any other MS SQL Server client. Add this Windows domain user (localadmin) to the MS SQL Server.
- 3 Add this user (localadmin) to the Enterprise Vault databases, on which you want the access rights.

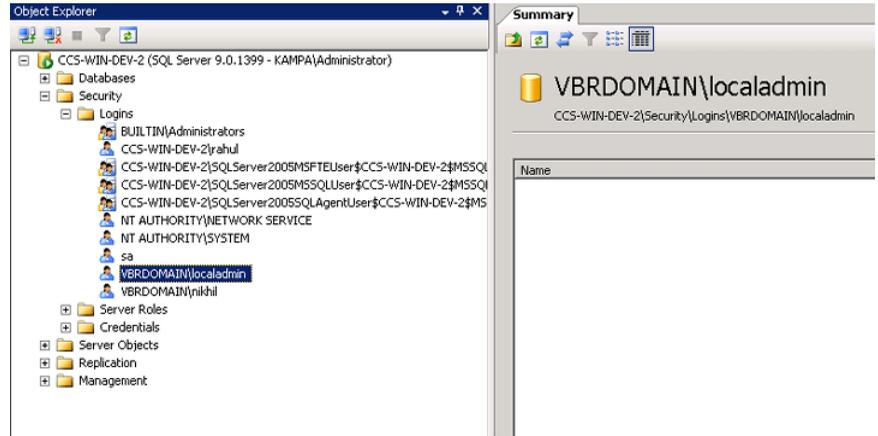
---

**Note:** To report on Enterprise Vault / archive data, VBR Agent needs access to the Enterprise Vault directory and storage databases. You need to add the user to these databases and give the required access rights on these databases.

---

- 4 In the MS SQL Server admin console, in the Object Explorer, expand the Security folder.

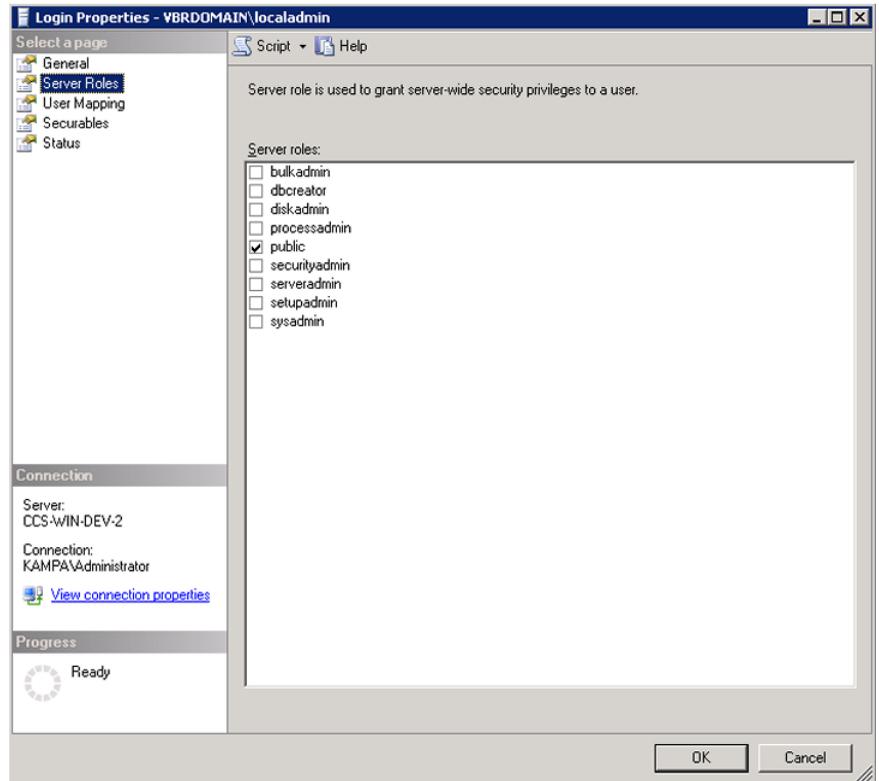
5 Expand the Logins folder as shown in the following figure:



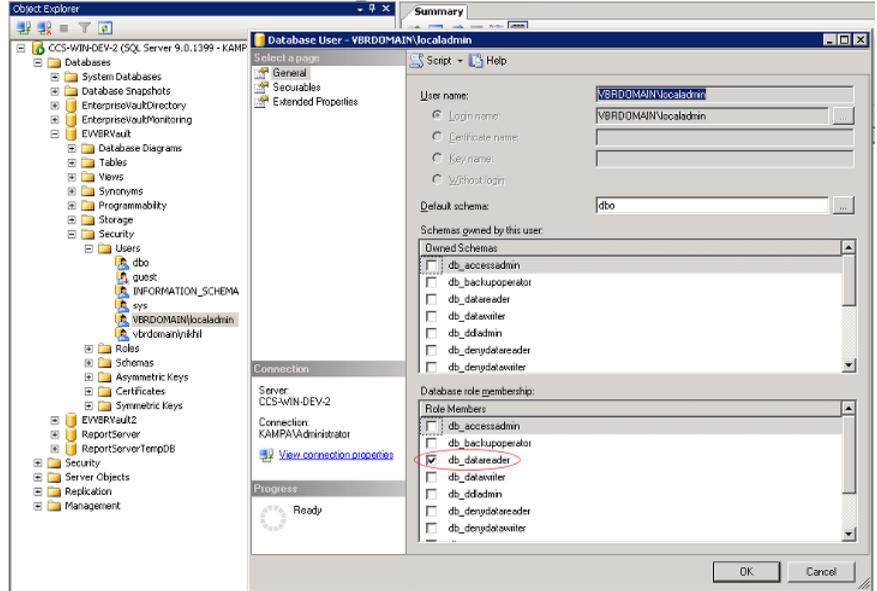
- 6 Right-click the user name - for example 'VBRDOMAIN\localadmin' with the password 'pass' - with which you want to perform integrated login on the Agent host and MS SQL Server host.
- 7 Click **Properties**.
- 8 On the Login Properties screen, in the Select a page pane, select Server Roles.

- 9 In the Server roles pane at the right-hand side, select the 'public' check box as shown in the following figure:

The user localadmin in the VBRDOMAIN (VBRDOMAIN\localadmin) now has the rights to access MS SQL Server.



10 Additionally, make sure that the user has 'datareader' rights to access the desired database as shown in the following figure:



## About creating a user for integrated login

This section provides procedures to create a user that is required for integrated login between the Veritas Backup Reporter Agent host and MS SQL Server host, where the archive data resides.

Depending on the Enterprise Vault data collector deployment mode, the procedure to create a login user varies.

### About creating a user in single-domain deployment mode

Make sure that the user whose credentials (for example, User name: 'localadmin' and Password: 'pass') you will use for the integrated login has required access rights on the MS SQL Server, where the archive data resides.

The user 'localadmin' can be an existing user, or you can create a new user with these credentials in MS SQL Server and give required access rights.

See “[Accessing MS SQL Server host](#)” on page 243.

If you have deployed the Enterprise Vault data collector in the single-domain mode, create a user, (User name: 'localadmin' and Password: 'pass') in the Agent host domain that is the Windows domain.

See [“About single-domain deployment mode”](#) on page 242.

Use credentials of this user (User name: 'localadmin' and Password: 'pass') while configuring the Agent properties for integrated login.

See [“Configuring the Veritas Backup Reporter Agent properties for integrated login”](#) on page 248.

### **About creating a user in multi-domain deployment mode**

Make sure that the user whose credentials (for example, User name: 'localadmin' and Password: 'pass') you will use for the integrated login has required access rights on the MS SQL Server, where the archive data resides.

The user 'localadmin' can be an existing user, or you can create a new user with these credentials in MS SQL Server and give required access rights.

See [“Accessing MS SQL Server host”](#) on page 243.

If you have deployed the Enterprise Vault data collector in the multi-domain mode, create a user (User name: 'localadmin' and Password: 'pass') in the Agent host domain.

See [“About multi-domain deployment mode”](#) on page 242.

Use credentials of this user (User name: 'localadmin' and Password: 'pass') while configuring the Agent properties for integrated login.

See [“Configuring the Veritas Backup Reporter Agent properties for integrated login”](#) on page 248.

### **About creating a user in standalone deployment mode**

Make sure that the user whose credentials (for example, User name: 'localadmin' and Password: 'pass') you will use for the integrated login has required access rights on the MS SQL Server, where the archive data resides.

The user 'localadmin' can be an existing user, or you can create a new user with these credentials in MS SQL Server and give required access rights.

See [“Accessing MS SQL Server host”](#) on page 243.

If you have deployed the Enterprise Vault data collector in the standalone mode, create a user for example (User name: 'localadmin' and Password: 'pass') in the appropriate workgroup.

See [“About standalone deployment mode”](#) on page 243.

Use credentials of this user (User name: 'localadmin' and Password: 'pass') while configuring the Agent properties for integrated login.

See “[Configuring the Veritas Backup Reporter Agent properties for integrated login](#)” on page 248.

## Configuring the Veritas Backup Reporter Agent properties for integrated login

The Enterprise Vault data collector configured in Veritas Backup Reporter collects the Enterprise Vault archive data residing on the MS SQL Server. However, the data collection is not possible if the Veritas Backup Reporter Agent is not configured to run in the context of the user / group that has access to the SQL Server.

---

**Note:** Make sure that this user has required rights to access MS SQL Server

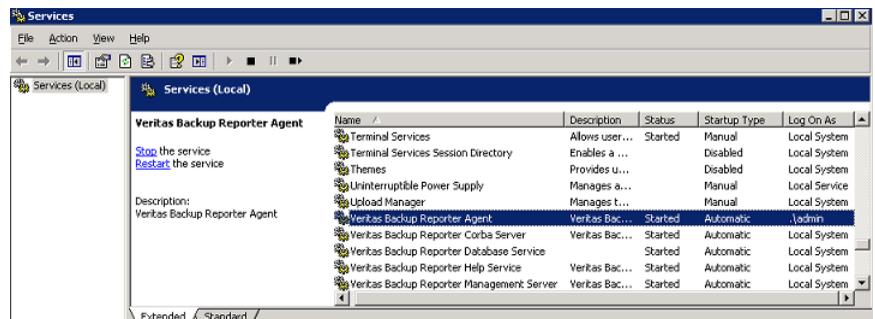
See “[Accessing MS SQL Server host](#)” on page 243.

---

### To configure Veritas Backup Reporter Agent properties

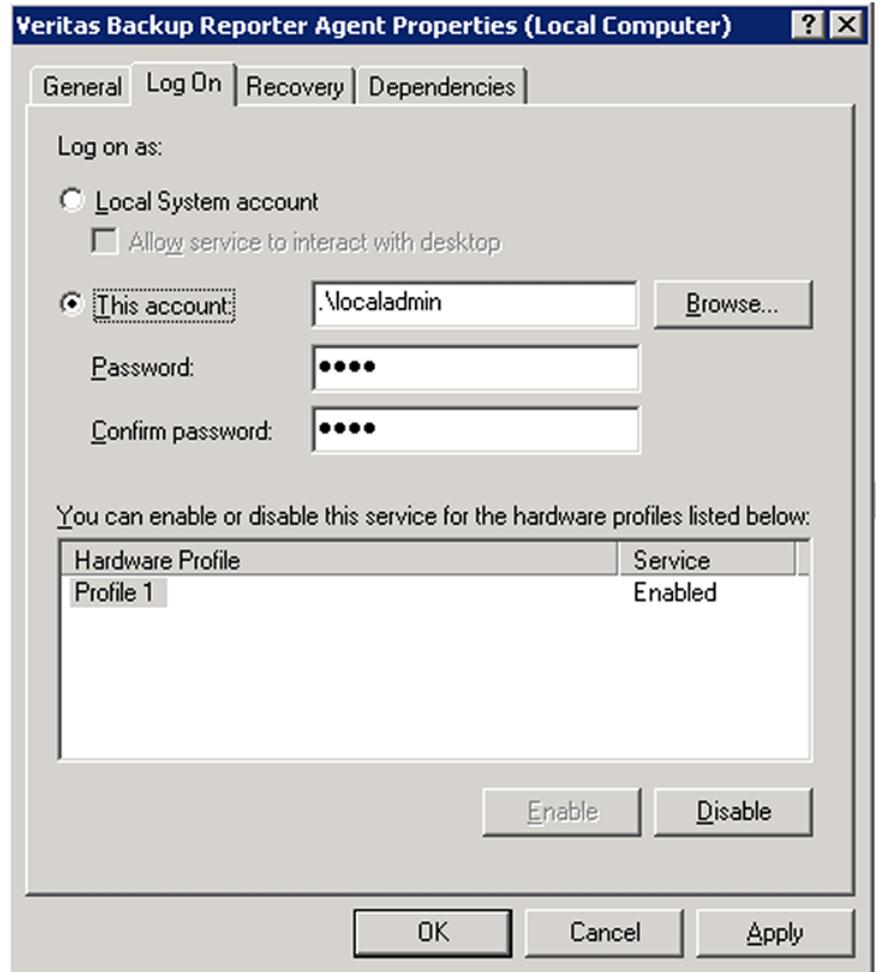
- 1 On the Veritas Backup Reporter Agent host (Windows system), click **Start > Run**.
- 2 In the Run dialog box, in the Open text box, enter `services.msc`.
- 3 Click **Enter**.

The Windows Services screen is displayed as shown in the following figure:



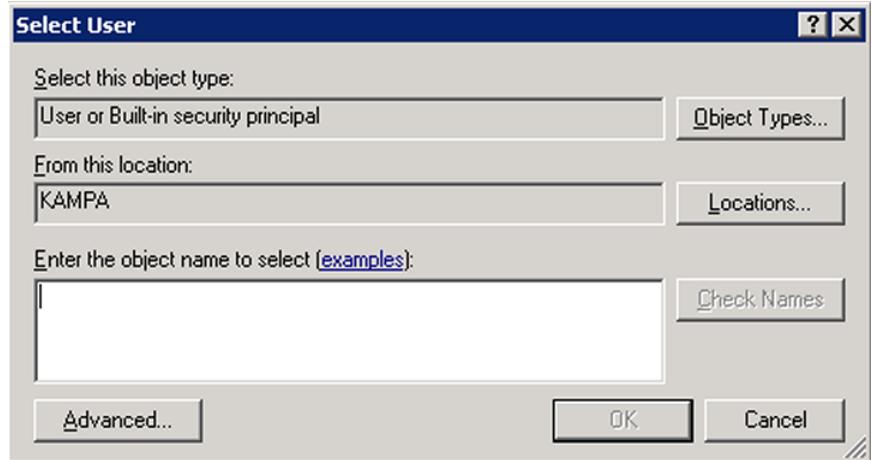
- 4 On the Services screen, on the services list, right-click the Veritas Backup Reporter Agent service.
- 5 On the right-click menu, click **Properties**.

- On the Veritas Backup Reporter Agent Properties screen, on the Log On tab, select the This account option as shown in the following figure:



- 7 Enter the credentials of the user - for example 'localadmin' with the password 'pass' - who has the rights to access the MS SQL Server, where the Enterprise Vault archive data resides.

Alternatively, click **Browse**. This opens the **Select User** dialog box as shown in the following figure:



- 8 Enter a user name in the text box. This user should have access rights on MS SQL Server. Click **Check Names** to check whether the user name specified is present in the Windows domain or not.
- 9 Click **OK**.
- 10 Click **OK** on the LogOn tab.

## Installing MS SQL Server JDBC driver

To collect the Enterprise Vault data residing on Microsoft SQL Server (or MS SQL Server or SQL Server), you require SQL Server JDBC driver installed on the Veritas Backup Reporter Agent host. The Agent requires the JDBC driver to communicate with the MS SQL Server.

Microsoft provides a Java Database Connectivity (JDBC) driver for use with SQL Server 2005. The SQL Server 2005 JDBC driver is available to all SQL Server users at no additional charge, and provides access to SQL Server 2000 and SQL Server 2005 from any Java application, application server, or Java-enabled applet. This driver is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in J2EE (Java2 Enterprise Edition). The SQL Server 2005 JDBC Driver is JDBC 3.0 compliant and runs on the Java Runtime Environment (JRE) 1.4 and later versions.

### To install MS SQL Server JDBC driver

- 1 Click the following link:  
[Download Microsoft SQL Server 2005 JDBC Driver 1.2](#)
- 2 On the Microsoft SQL Server 2005 JDBC Driver 1.2 page, click **Download**.
- 3 On the MICROSOFT SOFTWARE LICENSE TERMS page, select the following:  
I Accept and I want to download the Microsoft Windows version  
The File Download dialog box is displayed.
- 4 Click **Save** to save the .zip file to a desired location.
- 5 Unzip the file.
- 6 Copy `sqljdbc_1.2\enu\auth\x86\sqljdbc_auth.dll` and `sqljdbc_1.2\enu\sqljdbc.jar` files to the following location on the Agent host.  

```
Install Dir\Symantec\Veritas Backup Reporter\Agent\lib
```

  
*Install Dir* is the location where you have installed Veritas Backup Reporter  
Click the following link for more information and Frequently Asked Questions on the JDBC driver.  
[Microsoft SQL Server 2005 JDBC Driver](#)
- 7 Restart the Agent service.

## Configuring Enterprise Vault data collector

This section provides the procedure to configure the Enterprise Vault data collector in the Veritas Backup Reporter console. This data collector collects archive data from MS SQL Server where the Enterprise Vault database resides.

To collect archive data, the Enterprise Vault data collector needs the Agent to be configured to run in the context of the user / group that can access MS SQL Server.

See “[Configuring the Veritas Backup Reporter Agent properties for integrated login](#)” on page 248.

### To configure Enterprise Vault data collector

- 1 In the Veritas Backup Reporter console, click **Settings > Global Settings > Agent Configuration**.
- 2 On the Settings page, click the agent for which you want to configure an Enterprise Vault data collector.
- 3 On the Agent/Server Information Configuration page, click **Create**.

**4** On the Create Data Collector Configuration page, enter the following information:

- Product** Select the name of the product from which you want to collect data. Select Symantec Enterprise Vault (2007 SP3, 2008).
- Target Host Name** Enter the name of the MS SQL Server host name from which the Enterprise Vault data collector collects the archive data.

**5** Click **Next**.

On the Data Collector Details page, the Target Details, Configuration Settings, Log Settings, And Discovered Hosts details are displayed as shown in the following figure:

**Data Collector Details**

**Target Details**

Product : Symantec Enterprise Vault (2007 SP3, 2008)  
 enterprisevault.EnterpriseVaultAgentModule.version  
 Target Host Name : ccs-win-qe-9.vbrqedomain.com  
 Data Collector Status :

**Log Settings**

Level :   
 Max Size (MB) :   
 Rollover Count :

**Configuration Settings**

Database Instance Name :   
 Database Port Number :

**Discovered Hosts -**

**Name Qualification Options**

- Append Domain @
- Via DNS (not recommended for DHCP)
- Do Not Qualify

Configuration Status	Collectable Data Type	Collection Interval	Blackout Period Start Time	Blackout Period Duration (hr)	Last Successful Data Load	Fetch Size (Nos.)
<input type="checkbox"/>	Archive Policy	15 Minute(s)	-----	1 hour	Never Reported	500
<input type="checkbox"/>	Vault Store	15 Minute(s)	-----	1 hour	Never Reported	500
<input type="checkbox"/>	Target	15 Minute(s)	-----	1 hour	Never Reported	500
<input type="checkbox"/>	Archive	15 Minute(s)	-----	1 hour	Never Reported	500

This feature has been tested against Enterprise Vault environments containing 30,000 Exchange Server mail boxes and 100,000 items archived per day

**6** Check / enter the following Target Details:

Product	Displays the name of the product as Symantec Enterprise Vault (2007 SP3, 2008). You have specified this product name on the Create Data Collector Configuration page.
Target Host Name	Displays the name of the MS SQL Server host name that you have specified on the Create Data Collector Configuration page.
Data Collector Status	By default, the data collector status is Enabled. You can disable the data collection by changing the status.

**7** Enter the following Configuration Settings:

Database Instance Name	This is the database instance name. By default this field is left blank.
Database Port Number	Enter the port number that is used to connect to the MS SQL Server.  The default port number is 1433.

**8** Enter the following Log Settings:

the section called “About Veritas Backup Reporter log files”

Level	<p>From the drop-down list, select the level of information, with which you want to store the data collector log files. The log levels are as follows:</p> <ul style="list-style-type: none"><li>■ Off</li><li>■ Severe</li><li>■ Warning</li><li>■ Info</li><li>■ Config</li><li>■ Debug-Fine</li><li>■ Debug-Finer</li><li>■ Debug-Finest</li><li>■ All</li></ul> <p>If you set the log level to 'Off', no logs will be stored for this log level and if you set it to 'All', every bit of the data collector information will be logged. When you set the logging to a particular level, the log information for all levels previous to that level is also stored. For example, if you set the log level to 'Warning', all warnings and errors / exceptions (log information pertaining to the 'Severe' log level) are logged.</p> <p>In Debug type of logs, all CLIs that were fired during data collection are stored, along with the information pertaining to previous log levels.</p>
Max Size (MB)	<p>Enter the maximum size in MB that you want to set for a data collector log file. For example, enter 5, if you want a data collector log file to grow upto 5 MB before it rolls over to the next log file. The number of log files created depends on the Rollover Count that you specify.</p>
Rollover Count	<p>Enter the rollover count for the data collector log files.</p> <p>For example: If you specified the Max Size of a log file as 5 MB and Rollover Count as 4, a log file (say 0.log) can grow upto 5 MB. When the size reaches 5 MB, the log information is pushed to the next log file (say 1.log) and the latest log information is stored in the first log file (that is 0.log). Thus, when four log files are full and log information is still increasing, the oldest log information that is in 3.log file is deleted. Thus, at any given time the number of log files is less than or equal to 4 and the latest log information is available in the 0.log file.</p> <p>Example of the log file name: <code>module-002-enterprisevault-server1-0.log</code></p>

**9** Enter the following Discovered Hosts - Name Qualification Options:

With these options, you can specify the way you want to refer to the Enterprise Vault hosts in Veritas Backup Reporter context.

- |                                    |  |
|------------------------------------|--|
| Append Domain                      | <p>Select this option and add text in the @ text box to append this text to all Enterprise Vault host names.</p> <p>For example: Veritas Backup Reporter has discovered a Vault Server host name, say 'VaultServer1' from the Enterprise Vault database. Veritas Backup Reporter may not be able to refer to VaultServer1 using the same host name, while requesting archive data. In this case, select the Append Domain option and add domain name say 'DomainName', which will be appended to the host name, that is VaultServer1@DomainName</p> <p>This is useful if different Enterprise Vault Server sites refer to physically different Vault Servers by the same name.</p> |
| Via DNS (not recommended for DHCP) | <p>This is a default option. This option enables the Veritas Backup Reporter Agent to perform DNS lookup on the Enterprise Vault host names to get the associated IP addresses. Use this option only if you have a common DNS environment for Enterprise Vault hosts and Veritas Backup Reporter Agent.</p> <p><b>Caution:</b> Do not use this setting if the hosts in Enterprise Vault environment use DHCP, because there may be conflicts with the same IP addresses being used by the different servers at different times.</p>  |
| Do Not Qualify                     | <p>Select this option if you do not want to Veritas Backup Reporter Agent to modify the host names discovered from Enterprise Vault database.</p> <p><b>Caution:</b> Do not use this option if you do not have unique host names across all Enterprise Vault sites. Because HostA from one Enterprise Vault Server will now match against a HostA discovered from another Enterprise Vault Server and you cannot identify them in reports.</p>   |

**10** Enter the following information regarding data types to be collected:

- |                      |  |
|----------------------|--|
| Configuration Status | Select this check box to collect the associated data type. |
|----------------------|--|

Collectable Data Type	<p>Lists the data types that the data collector collects. Enterprise Vault data collector collects the following data types from the MS SQL Server:</p> <ul style="list-style-type: none"><li>■ Archive Policy</li><li>■ Vault Store</li><li>■ Target</li><li>■ Archive</li></ul> <p>See “<a href="#">About data collected from Enterprise Vault</a>” on page 238.</p>
Collection Interval (sec)	<p>Enter the collection interval in seconds, minutes, hours, and days. This is the time interval that you want to set between the two consecutive data collections.</p> <p>For example: You have set the Collection Interval to 15 Minutes. The first data collection starts at say 9 AM and continues until all archive records are collected and ends at 11 AM. The next data collection will start at 11.15 AM.</p>
Blackout Period Start Time	<p>Select the start time of a blackout period. The data is not collected for the time specified in Blackout Period Duration, since Blackout Period Start Time.</p>
Blackout Period Duration (hr)	<p>Select the blackout duration in hours, for which the data is not collected since the time specified for the Blackout Period Start Time field.</p> <p>For example: You have set the Blackout Period Start Time as 1:00 PM and the Blackout Period Duration as 2 hours. No data is collected between 1 PM to 3 PM.</p>
Last Successful Data Load	<p>States whether last data load was successful or not.</p> <p>the section called “Viewing agent status”</p>
Collection Status	<p>Displays the status of data collection. You can either resume or pause the data collection.</p>

**Fetch Size** Select the number of records of the data type that you want to fetch at a time.

For example:

If the Fetch Size is set 500, the Veritas Backup Reporter Agent can at a time send maximum of 500 Archive records to the Management Server. If the Agent has collected 600 Archive records from the Enterprise Vault database, it can send them to the Management Server in two chunks, 1st chunk of 500 records and 2nd one of 100.

Symantec recommends that you set the fetch size to 5000 for the Archive data type because of the following reason:

There can be thousands of records of the Archive data type that Agent collects from the Enterprise Vault database, in a given time interval. The Agent sends these records to the Management Server, as soon as it receives them from the Enterprise Vault database. If you set the fetch size of the Archive data type to a value lesser than 5000, the data collection and data transmission by the Agent will not be in sync and the Agent performance will drop.

---

**Note:** If you want to collect data at your discretion (irrespective of the collection intervals specified) you can use the force poll method.

You can force poll for all Enterprise Vault events, but you can specify the time limit only for Archive and Target events. For example, you can specify that you want to collect Archive or Target data for last 4 hours. For the remaining Enterprise Vault events, you cannot specify the time limit, the data collector collects all available data.

You can collect the data also during the Blackout Period using the force poll method.

---

## 11 Click Save.

### About Enterprise Vault data collector log files

The log files related to Enterprise Vault data collector are stored at the following location:

```
Install Path\Symantec\Veritas Backup Reporter\Agent\Logs\module-moduleNumberAsCreated-enterprisevault-agenthostname-0.log
```

Where *Install Path* is the location where you have installed the Veritas Backup Reporter application. By default *Install Path* is: `C:\Program Files`

Where *moduleNumberAsCreated* can vary depending on the number of data collectors you have configured for the Agent and the sequence in which they have configured.

Where *agenthostname* is the name of the Agent host where you have configured the Enterprise Vault data collector.

Example of the log file name: `module-002-enterprisevault-EVserver-0.log` or `module-004-enterprisevault-server-3.log`

At any point of time, the latest log information is available in 0.log.

## Enterprise Vault data collection checklist

Ensure the following before you start collecting data from Enterprise Vault database:

- The SQL Server JDBC driver has been installed on the Veritas Backup Reporter Agent host  
See [“Installing MS SQL Server JDBC driver”](#) on page 250.
- The Veritas Backup Reporter Agent has been configured to run in the context of the user / group that has access to MS SQL Server database where Enterprise Vault data is stored.  
See [“Configuring the Veritas Backup Reporter Agent properties for integrated login”](#) on page 248.
- The Veritas Backup Reporter Agent service is running.
- The SQL Server services are running.
- You have entered the appropriate information for Enterprise Vault data collector variables.  
See [“Configuring Enterprise Vault data collector”](#) on page 251.
- You have selected the data types / events to be collected from the Enterprise Vault database, that is the MS SQL Server.
- You have specified the collection interval within which you want to collect the archive data.

## About enhancement in agentdatacollectionutility

In Veritas Backup Reporter 6.6, `agentdatacollectionutility` has been modified to include new data types pertaining to Enterprise Vault.

You can use `agentdatacollectionutility` to perform a manual force poll, which means that you can send a request to the Veritas Backup Reporter Agent to collect data from product server by running this utility from the command prompt.

`agentdatacollectionutility` resides at the following location:

Solaris                    `/opt/VRTSccsva/bin`

Windows                 `InstallDir\Symantec\Veritas Backup Reporter\Server\Util`

In the `agentdatacollectionutility`, in the event argument the following options have been added:

- Archive Policy
- Vault Store
- Target
- Archive

```

C:\WINDOWS\system32\cmd.exe
C:\>"Program Files\Symantec\Veritas Backup Reporter\Server\Util\agentdatacollectionutility.exe"
-----
-usr option is required
-----
Usage:
agentdatacollectionutility.exe -usr <username> -moduleInstance <module> -event <event> [options]

Required:
-----
-usr      : The username for credential
-moduleInstance: Instance Identifier <integer>
-event    : Event Identifier
           <Job!Error!Policy!Tape Drive Usage!Media!Skipped File!Image!ArchivePolicy!Vault Store!Target!Archive>
-----

Options:
-----
-time     : The start time for data collection (optional)
-server   : Name of the host to connect
-port     : Port number to use
-brokerHost : Name of the host that provided credential
-brokerPort : Port number of broker that provided credential
-domainName : The domainName for credential
-domainType : The domainType for credential
-----
    
```



# Managing User Settings

This chapter includes the following topics:

- [Updating your personal information](#)
- [Changing your password](#)
- [Configuring and managing report-based notifications](#)
- [Exporting reports](#)
- [Setting a default currency for cost reports](#)

## Updating your personal information

Use the My Profile dialog box to update your personal information, including your email address, and to change your password.

### To change your personal information

- 1 On the console Settings tab, click **Settings > My Profile and Settings**.
- 2 In the My Profile dialog box, type updated information in the First Name, Last Name, and Email Address text boxes.
- 3 Click **Save**.

## Changing your password

You should change the administrator-assigned password the first time you access the Veritas Backup Reporter console and then change it at regular intervals thereafter.

### To change the password with which you log on to Veritas Backup Reporter

- 1 On the console Settings tab, click **My Profile and Settings**.
- 2 In the My Profile dialog box, click **Change Password**.
- 3 In the Change Password dialog box, do the following:
  - Type your old password in the Old Password field.
  - Type your new password in the New Password field. Asterisks display in place of the password text.  
Passwords are case-sensitive and must contain at least five characters.
  - Type your new password again in the Confirm New Password text box.
- 4 Click **Save**.

## Configuring and managing report-based notifications

You can configure reports to initiate automatic notifications. There are two forms of notifications: email and alerts.

Email notifications are email messages containing data from reports that are sent on a regular schedule to interested parties. They are useful for notifying key IT staff when problems or potential problems arise as well as for providing status updates at regular intervals.

The following topics describe the setup of report-based notifications using email:

See [“Managing report schedules”](#) on page 263.

See [“Managing email distribution lists ”](#) on page 264.

See [“Managing email notifications”](#) on page 265.

---

**Note:** Before setting up email features, make sure that the SMTP Mail server is configured properly.

See [“Configuring SMTP server using global system settings”](#) on page 137.

---

Report-triggered alerts are generated when reports running on a predefined schedule identify a problem or potential problem involving backup or restore.

An alert is a form of notification designed to call attention to a potential problem. Alerts appear in the Veritas Backup Reporter console. You can also use them to initiate automated responses, called policies.

The following topics describe the setup of report-based notification using alerts:

See [“Managing report schedules”](#) on page 263.

See [“Configuring reports to trigger alerts”](#) on page 269.

## Managing report schedules

The report schedule specifies the days and the time of day for running the reports on which both email notifications and alerts are based. Each schedule you define can be assigned to one or more email notifications, report-triggered alerts, or both.

Following are some examples of how you can use report schedules for notification:

- You can arrange to send an email notification, containing data from several different reports, at 6:00 A.M. every day so that operators can view the status of the network when they arrive for work each morning. Alternatively, you can send a different email notification at 12:00 noon on the first day of each month, so that executives have up-to-date data for their monthly status meeting.
- You can schedule reports to run each day or each week so that backup admin is notified whenever potential problems exist in the network. Because the email notifications are based on reports that contain conditions, they are sent only when a potential problem is detected.

You can use the same scheduling process for the following additional purposes:

- Regular updating of cached reports.
- Regular archiving, or exporting, of reports.

### To schedule reports to run for notification

- 1 On the console Settings tab, click **Schedules**.
- 2 In the Schedules window, click **Create**.
- 3 In the Create Schedule dialog window, in the Name field, type a name for the schedule.
- 4 Select a time on the At Time drop-down list.  
This is the time at which reports will be sent on the specified days.
- 5 Select a recurrence pattern for running the reports, and then do one of the following:
  - If you selected Daily, check one or more days each week.
  - If you selected Monthly, select a day of the month from the drop-down list.
- 6 Click **Save**.

### To edit a report notification schedule

- 1 On the console Settings tab, click **Schedules**.
- 2 In the Schedules window, click the **Edit** icon next to the name of the schedule.
- 3 In the Modify Schedule dialog box, do any of the following:
  - In the Name field, type a name for the schedule.
  - Change the time by indicating a new time from the At Time drop-down list.  
This is the time at which reports will be sent on the specified days.
  - Change the recurrence pattern to either Daily or Monthly, and then do one of the following:
    - If you selected Daily, check one or more days for reports to be sent each week.
    - If you selected Monthly, select a day of the month from the drop-down list.
- 4 Click **Save**.

### To delete a report schedule

- 1 On the console Settings tab, click **Schedules**.
- 2 In the Schedules window, check the names of the schedules you want to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

### To set font style and font size of email messages

- 1 Open the `application.properties` file.
- 2 Modify the following parameters:
  - `schedule.email.font.face` (Type the font name.)
  - `schedule.email.font.size` (Type the font size.)
- 3 Save the file.

## Managing email distribution lists

You can set up email distribution lists for distributing reports to interested parties and for notifying key IT staff when problems or potential problems arise.

**To create a distribution list for email notifications**

- 1 On the console Settings tab, click **Distribution Lists**.
- 2 In the Distribution Lists window, click **Create**.
- 3 In the Create Distribution List dialog box, type the name of the distribution list in the Name field.
- 4 Type (or paste from your system clipboard) a list of email addresses in the Send To field.

Use commas to separate each address in the list, for example  
 reggie@example.com,mark@example.com,sammy@example.com.

- 5 Click **Save**.

**To edit a distribution list for email notifications**

- 1 On the console Settings tab, click **Distribution Lists**.
- 2 In the Distribution Lists window, click the **Edit** icon next to the name of the distribution list you want to edit.

- 3 In the Edit Distribution List dialog window, do one or both of the following:

- Change the name of the list by typing over the value in the Name field.
- Update the list of email addresses in the Send To field.

Use commas to separate each address in the list, for example  
 reggie@example.com,mark@example.com,sammy@example.com.

- 4 Click **Save**.

**To delete a distribution list for email notifications**

- 1 On the console Settings tab, click **Distribution Lists**.
- 2 In the Distribution Lists window, check the names of the distribution lists you want to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

## Managing email notifications

After you have created schedules and distribution lists, you must configure each email notification by specifying the following:

- The reports to include in the email notification
- The delivery schedule of the notification
- The intended recipients of the notification

- The content of the email message

If the email notification contains reports with conditions, you can set it up so that the reports are included only when the conditions are met. Note that, if no conditions are met and no reports are included, then no email notification is sent. (In other words, users do not receive an empty email notification.)

#### To configure the distribution of an email notification

- 1 On the console Settings tab, click **Email/Export Reports**.
- 2 In the Email Reports list, click **Create**.
- 3 In the Create Email Report dialog box, in the Name field, type a name for the email notification.  
  
The name should be descriptive so that you can recognize each notification that you create by name.
- 4 Click **Enabled** to activate email distribution for the indicated report.  
  
Deselect if you want to defer email distribution for this report until later.
- 5 From the Schedule drop-down list, select a schedule.  
  
The schedule determines the time and days on which the email is sent.
- 6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.  
  
See [“Managing report schedules”](#) on page 263.
- 7 From the Select Report list box, click the names of one or more reports to send within the email notification.
- 8 To specify who receives the email, do one of the following:
  - Click a list of recipients from the Distribution List drop-down list.  
To define a distribution list that does not appear in the drop-down list, click the **Edit** icon next to the list.  
See [“Managing email distribution lists”](#) on page 264.
  - Type email addresses for individual recipients, separated by commas, in the Send to, CC to, and BCC to fields.  
For example: operator1@example.com,joe@example.com

- 9** In the Subject box, type a descriptive title.

This text appears as the subject for each email message that is sent. Use substitution tokens to include variable data, such as the name of an alert.

See [“About substituting tokens to provide variable data in notifications”](#) on page 272.

Example: \$Alert.Alert Key\$ in Backup Report

- 10** Select a suitable email format that decides the presentation of the data contained by the email. The email formats are described as follows:

HTML	Display in a Web browser. Unlike the other formats, HTML preserves the original format of the data as well as any graphics in the original report.
CSV	For use with spreadsheet programs.
TSV	Compatible with word-processing applications and text editors.
XML	Can be imported (using user-written scripts) by other programs like databases or billing applications.

- 11** Type an optional message in the Message field.

This text appears within each email message along with the contents of the indicated reports.

- 12** If you clicked reports in which exception conditions are defined, do the following in the Exception Conditions area of the dialog window:

- Check the reports to run.
- Check the conditions within reports that when met cause the corresponding report to be included in an email notification.  
 The exception conditions defined for these reports represent problems or potential problems. When you click conditions in this dialog box, Veritas Backup Reporter includes the report data in an email message whenever a potential problem is detected.
- To send the email notification only when one or more of the selected exception conditions are met, click **Send email only if reports are attached**. If you uncheck this box, an email notification is always sent at the scheduled interval, regardless of whether any reports are included.
- Click **Update Conditions List** to confirm the Exception Conditions settings.

- 13** Click **Save**.

### To edit an email notification

- 1 On the console Settings tab, click **Email/Export Reports**.
- 2 In the Email Reports window, click the **Edit** icon next to the name of the email notification.
- 3 In the Edit Email Report dialog box, do any or all of the following:
  - In the Name field, change the name of the email notification.
  - Check **Enabled** to activate email distribution for the selected report. The report will be sent at the next scheduled interval. (Uncheck if you want to defer email distribution for this report until later.)
  - From the Schedule drop-down list, select a schedule. The schedule determines the time and days on which the email is sent. To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list. See [“Managing report schedules”](#) on page 263.
  - In the Select Report drop-down list, select one or more reports to send. Cancel the selected reports you no longer want to send.
  - Specify who receives the email by doing one of the following:
    - Select a list of recipients from the Distribution List drop-down list. To define a distribution list that does not appear in the drop-down list, click the **Edit** icon next to the list. See [“Managing email distribution lists”](#) on page 264.
    - Add or remove email addresses for individual recipients in the Send to, CC to, and BCC to fields. Use commas to separate addresses, for example operator1@example.com,joe@example.com.
  - Change the text in the Subject field. This text appears as the subject for each email message that is sent. Use substitution tokens to include variable data, such as the name of an alert. Example: `Alert.Alert Key` in Backup Report See [“About substituting tokens to provide variable data in notifications”](#) on page 272.
  - Select one of the following formats:
    - HTML
    - XML
    - CSV

- TSV
  - Change the text in the Message field.  
This text appears within each email message along with the contents of the selected reports.
  - Update the list of reports and conditions to determine which exception conditions when met cause the corresponding report to be included in the email notification, and then click **Update Conditions List**.
- 4 Click **Save**.

#### To delete email notifications

- 1 On the console Settings tab, click **Email/Export Reports**.
- 2 In the Email Reports window, check the names of the email notifications you want to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

## Configuring reports to trigger alerts

After setting threshold conditions in a report's definition, you can cause Veritas Backup Reporter to generate alerts when those conditions are met. For example, you can set up report-triggered alerts to indicate that the percentage of failed backup jobs has reached a certain level, or that the total size of all backup jobs has exceeded a certain threshold.

Following is the process with which Veritas Backup Reporter generates a report-triggered alert:

- A report containing one or more conditions runs according to a predefined schedule.  
See "[Managing report schedules](#)" on page 263.
- The report shows that at least one of its conditions has been met, that is, a threshold was exceeded.
- Based on this result, Veritas Backup Reporter generates an alert.

See "[Working with alerts](#)" on page 315.

#### To define a report-triggered alert

- 1 On the console Settings tab, click **Alert Trigger Reports**.
- 2 In the Alert Trigger Reports list, click **Create**.

- 3 In the Create Alert Trigger Report dialog box, in the Name field, type a name for the alert definition.

The name should be descriptive enough that you can click it from a list of alert definitions.

- 4 Click **Enabled** to activate the alert definition.

Veritas Backup Reporter will begin generating alerts whenever any of the clicked reports are run and their conditions met. (Cancel the selection if you want to avoid generating alerts for now.)

- 5 On the Schedule drop-down list, select a schedule.

The schedule determines the time and days on which the reports are run to test their conditions.

- 6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

See [“Managing report schedules”](#) on page 263.

- 7 On the Select Report drop-down list, select the names of one or more reports to run.

- 8 Type summary text in the Alert Summary field.

- 9 To associate the alert with a specific report condition, use the following substitution strings in the text:

`$(Condition$`            The metric used for the report condition, for example Total Backup Job Size

`$(ReportName$`        The name of the report containing the condition.

`Condition`            Default

`$(Condition$ on  
$(ReportName$ has  
matched`

- 10 Type optional descriptive text in the Alert Description field.

This text appears when a console user views details about the alert.

Default: `Condition $(Condition$ on $(ReportName$ has matched`

- 11 If you clicked reports in which exception conditions are defined, do the following in the Exception Conditions area of the dialog box:

- Check the reports to run.

- Check the conditions within reports that when met trigger an alert. (A separate alert is triggered for each condition met.)  
 The exception conditions defined for these reports represent problems or potential problems. When you click conditions in this dialog box, Veritas Backup Reporter triggers an alert whenever a potential problem is detected.
- Click **Update Conditions List** to confirm the Exception Conditions settings.

**12 Click Save.**

**To edit a report-triggered alert**

- 1** On the console Settings tab, click **Alert Trigger Reports**.
- 2** In the Alert Trigger Reports list, click the **Edit** icon next to the name of the report-triggered alert.
- 3** In the Edit Alert Trigger Report dialog box, do any of the following:
  - In the Name field, change the name of the alert definition.
  - Click **Enabled** to activate the alert definition.  
 Veritas Backup Reporter begins generating alerts whenever any of the selected reports are run and their conditions met. (Cancel the selection if you want to avoid generating alerts for now.)
  - On the Schedule drop-down list, click a schedule.  
 The schedule determines the time and days on which the reports are run to test their conditions.
  - To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.  
 See [“Managing report schedules”](#) on page 263.
  - On the Select Report drop-down list, select the names of one or more reports to run.  
 Cancel the clicked reports you no longer want to run.
  - Change the summary text in the Alert Summary field.
  - Change the descriptive text in the Alert Description field.
  - Update the list of conditions which when met cause an alert to be generated, and then click **Update Conditions List**.
- 4** Click **Save**.

## About substituting tokens to provide variable data in notifications

You can use substitution tokens to provide variable data in notifications. For example, you can insert the name of an alert into the subject line of a notification email.

**Table 6-1** includes an alphabetical list of the substitution tokens available for including variable data in notifications.

**Table 6-1** Substitution tokens for variable data in notifications

Token	Description
\$Alert.Agent\$	Name of the Veritas Backup Reporter Agent host that issued the alert.
\$Alert.Alert Group\$	Category to which the alert belongs, for example <code>Partial Success</code> .
\$Alert.Alert Key\$	Numeric identifier optionally be associated with the alert. In the case of Backup Job failure alert, it refers to the error code returned from the backup software. (Same as \$Alert.JobStatus\$.)
\$Alert.Count\$	Number of times this alert was issued by the host since the last time it was cleared manually.
\$Alert.EventType\$	Alert class. For example, all backup failures, even if reported by different products, display an alert class of <code>BackupJob</code> .
\$Alert.First Occurrence\$	Date and time of origin for the event that created the alert. When there is a delay between the event and the creation of the alert, this token preserves the original event time.
\$Alert.IP\$	IP address of the host issuing the alert.
\$Alert.Initial Severity\$	Numeric designation of the alert’s severity: 5 = CRITICAL 4 = ERROR 3 = WARNING 2 = INFORMATION
\$Alert.Job ID\$	Job ID for the job associated with the alert.
\$Alert.JobStatus\$	Numeric identifier optionally be associated with the alert. In the case of Backup Job failure alert, it refers to the error code returned from the backup software. (Same as \$Alert.Alert Key\$.)
\$Alert.Last Occurrence\$	Time when the last de-duplicated event was generated.  Example: A backup job on <code>HostA</code> fails with error code 3, and an alert already exists from <code>HostA</code> with error code 3. <code>\$Alert.Last Occurrence\$</code> contains the time the backup job was performed.

**Table 6-1** Substitution tokens for variable data in notifications (*continued*)

Token	Description
\$Alert.Leveln\$	The name of the object level within a view (specified in \$Alert.View Name\$) associated with the alert. n can be any integer between 1 and 12.  Examples (within the <i>Geography</i> view): <i>Canada, Vancouver</i>
\$Alert.Node\$	Node of the Veritas Backup Reporter Agent host that issued the alert.
\$Alert.Other Info n\$	Optional additional information about the alert, such as the name of the schedule on which it was generated (where n is 1 or 2).
\$Alert.View Name\$	The primary view (specified in Settings > Global Settings > Monitoring Settings) used to identify attributes of the machine where the alert originated, such as its location or contact person.  Examples: <i>Geography, Business Unit</i>

## Exporting reports

You can archive reports by exporting them to the Veritas Backup Reporter. You can configure exporting of reports to occur periodically, as defined in a schedule.

Data from exported reports is stored in a default directory.

### About managing export schedules

The report schedule specifies the days and the time of day at which reports are exported. Each schedule you define can be assigned to one or more export activities.

The process for defining schedules for exports is the same as that for email notifications and report-triggered alerts. In fact, you can use the same schedule to export reports and generate notifications.

### Setting up exporting of reports

You can configure the export activities. You do this by specifying which reports are exported, the format of the exported file, and the export schedule.

#### To set reports for exporting

- 1 On the console Settings tab, click **Email/Export Reports**.
- 2 In the Export Reports list, click **Create**.

- 3 In the Create Export Report dialog box, in the Name field, type the file name to be used for the export operations.

The name should be descriptive enough that you can select it from a list of export operations.

- 4 Click **Enabled** to activate exporting.

At the next scheduled interval, the indicated reports are exported to the directory location that appears at the bottom of the dialog box. (Deselect if you want to defer exporting until later.)

- 5 On the Schedule drop-down list, select a schedule.

The schedule determines the time and days on which the export operation occurs.

- 6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

- 7 On the Select Report drop-down list, select the names of one or more reports to export.

- 8 Select one of the following file formats:

- CSV (comma-separated)
- TSV (tab-separated)
- HTML
- XML

The format you choose depends on how the data is to be displayed and manipulated. For example, many spreadsheet programs import data in CSV format, while TSV-formatted files are compatible with word-processing applications and text editors.

- 9 Click **Save**.

The new export operation appears in the Export Reports list. The export operation will include data from all of the selected reports in a file that has the name and format you specified.

#### To edit export reports

- 1 On the console Settings tab, click **Email/Export Reports**.

- 2 In the Export Reports list, click **Edit**.

- 3 In the Edit Export Report dialog box, do any of following:

- In the Name field, change the file name to be used for the export operation.
- Click **Enabled** to activate exporting.

At the next scheduled interval, the selected reports are exported to the directory location that appears at the bottom of the dialog box. (Deselect if you want to defer exporting until later.)

- On the Schedule drop-down list, select a schedule.  
The schedule determines the time and days on which the export operation occurs.
- To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
- On the Select Report drop-down list, select one or more reports to export. Cancel the selected reports you no longer want to export.
- Change the file format to **CSV** (comma-separated) or **TSV** (tab-separated).

4 Click **Save**.

#### To delete export operations for reports

- 1 On the console Settings tab, click **Email/Export Reports**.
- 2 In the Export Reports window, check the names of the export operations you want to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

## Setting a default currency for cost reports

In Veritas Backup Reporter, you can choose the currency that you want to appear on cost reports. If you have VBR administrator privilege, you can set multiple global currencies, one of which can be set as default currency.

You also have the option to overwrite this default currency while generating reports. The default currency that you set appears with the cost report values.

---

**Note:** Setting the default currency gives you the flexibility of displaying cost report values in the currency of your choice. However, Veritas Backup Reporter does not support conversion of currencies.

---

#### To set the default currency

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the console, click **Settings > User Settings > User Currency Settings**.

**Setting a default currency for cost reports**

- 3** On the Set Default Currency page, in the Default Currency drop-down list, all global currencies that are set by the administrator are available for selection. Select a currency from the drop-down list.
- 4** Select currency code or symbol. For example, for US dollar currency, you can either select a currency code USD or symbol \$, which appears on chargeback reports.
- 5** Select the Display Option in Wizard check box to have the option of overwriting the default currency you selected from the Default Currency drop-down list, while generating cost reports. If you do not select this check box, the cost values in the chargeback reports use the currency you selected from the Default Currency drop-down list.
- 6** Click Save.

# Managing Veritas Backup Reporter views

This chapter includes the following topics:

- [About Java View Builder](#)
- [About Java View Builder enhancements in VBR 6.6](#)
- [Running the Veritas Backup Reporter Java View Builder](#)
- [Creating views in Java View Builder](#)
- [Creating levels in views](#)
- [Adding objects to views](#)
- [Searching for objects](#)
- [Removing views, levels, or objects](#)
- [Renaming views, levels, and objects](#)
- [Managing user access to views](#)
- [Managing user access to levels or objects](#)
- [Viewing object views](#)
- [Customizing views](#)
- [Managing attributes](#)

## About Java View Builder

Veritas Backup Reporter views are logical groups of IT assets (hosts or file systems) organized in a hierarchical manner. You can create views in Java View Builder and make them available in the Veritas Backup Reporter console. The following view details appear in the Veritas Backup Reporter console.

---

**Note:** If you do not have the admin privileges you can still copy a view object from a read-only view to your view. However, you cannot modify its attributes because you do not have the write permissions for that view.

---

- Host mapping summary
- Host mapping details
- Host aliases
- Host IPs

---

**Note:** In the Veritas Backup Reporter console you can search for details of hosts that constitute a view.

See [“Searching for objects”](#) on page 283.

You can access the Java View Builder from the Veritas Backup Reporter console.

See [“Running the Veritas Backup Reporter Java View Builder ”](#) on page 281.

---

In a Veritas Backup Reporter view, IT assets scattered across organization can be arranged according to their locations, business units, or applications. You can generate various Veritas Backup Reporter reports filtered by views. With these reports, you can identify the locations or departments with hosts storing business critical data.

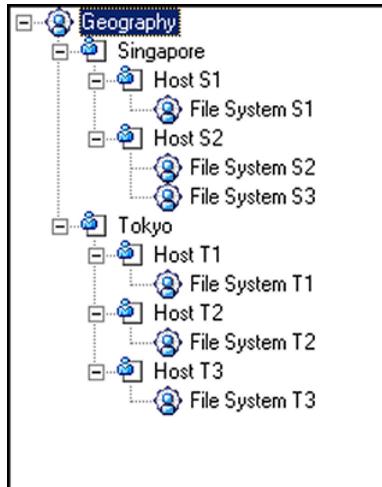
After you install and run the Veritas Backup Reporter Management Server and the Agent, IT assets are detected by Veritas Backup Reporter, which are then stored in the database. The Java View Builder makes these IT assets available while creating a view.

---

**Note:** To run the Java View Builder, you need Java Runtime Environment (JRE) installed on the host.

---

In a view hierarchy, between top and bottom levels you can create a number of user-defined levels. For example, you can create a view called Geography as follows:



This example contains two nodes, Singapore and Tokyo, which are at the first level of the tree structure. The hosts are at the second level and the file systems are at the third level of the structure.

## About Java View Builder enhancements in VBR 6.6

In Veritas Backup Reporter 6.6, Java View Builder is enhanced to accommodate the changes related to the Enterprise Vault integration.

In Veritas Backup Reporter 6.6, the following new view objects are added using which you can create object views to represent an Enterprise Vault setup:

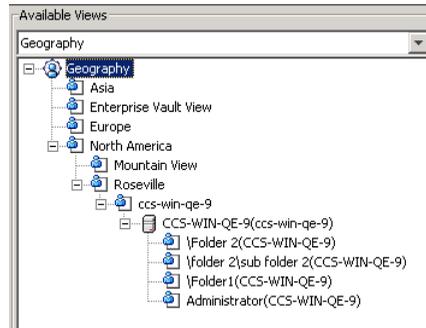
- Domain
- Target

The hierarchy of an object view based on archive data is as follows:

Abstract objects (Geography > Region > City) > Domain (Site) > Host (Exchange Server / Enterprise Vault Server) > Target (Mailbox / Journal Mailbox / Public Folder)

[Figure 7-1](#) depicts the view representing the Enterprise Vault setup.

Figure 7-1 Enterprise Vault view



In the [Figure 7-1](#) figure, the view called Geography contains the objects defined as in the following hierarchy.

- The view contains the abstract objects, such as Asia, Enterprise Vault View, Europe, North America.
- The second-level abstract object North America contains the objects Mountain View and Roseville.
- The third-level view object contains the actual view object called ccs-win-qe-9, which is a domain.

---

**Note:** A site in Enterprise Vault is referred to as a domain in Veritas Backup Reporter.

---

- The fourth-level view object is a host called CCS-WIN-QE-9, which is the Exchange Server host
- The fifth-level view objects are public folders (Folder 2 or Folder 1) and mailbox (Administrator). This implies that, Veritas Backup Reporter has been configured to collect the archive data associated with these objects.

In an Enterprise Vault setup, the Unassigned Objects tab in the Java View Builder UI contains unassigned domains, hosts, and targets. Double-click a domain to view its associated hosts. Double-click a host to view the targets associated with it.

---

**Note:** In Veritas Backup Reporter 6.6, you cannot use Follow the Master and Import / Export CSV features for the views that are based on archive data.

---

# Running the Veritas Backup Reporter Java View Builder

You can run the Veritas Backup Reporter Java View Builder in multiple ways. However, before running the Java View Builder, you need to establish the connection between the Java View Builder and the Veritas Backup Reporter Management Server with valid user credentials.

## To run the Veritas Backup Reporter Java View Builder

- 1 Log on to the Veritas Backup Reporter Management Server with administrator privileges.
- 2 In the Veritas Backup Reporter console, click the Views tab and then click **Java View Builder**.

# Creating views in Java View Builder

A Veritas Backup Reporter view can comprise multiple logical categories referred to as levels. The first level of a view is called node. For example:

Create a view with Application as a node. The view can contain multiple levels, such as ERP, database, and email, which are at level 2. You can create as many intermediate levels of logical or physical categories as you want before adding actual IT assets.

---

**Note:** To create views in the Veritas Backup Reporter Java View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

## To create views

- 1 On the View Builder toolbar, click **Create View**, or from the menu, click **Actions > New > Create New View**.
- 2 In the Create New View dialog box, in the View Name text box, type the name of the new view.

The name of the view must be unique.

- 3 Select the Automate View check box if you want to specify tasks for the view.

You can automate views, which lets you automatically identify backup clients that are recently added to the network. You can define view tasks that run on the specified schedules and identify new backup clients. The new backup client is then added to an object view that contains the respective master or media server host.

- 4 Click **OK**.

The view appears in the left pane of the Java View Builder console.

## Creating levels in views

A newly created view has only one level. After you modify the view to have more levels of view objects, you will always find the IT assets, such as hosts, file systems, or applications are at the lowest levels in the view.

Between the top level and the bottom levels, you can create multiple intermediate levels to organize view objects into logical groups, creating a hierarchical structure in the view.

---

**Note:** To create levels to a view in the Java View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

### To create levels in views

- 1 In the Java View Builder window, from the Available Object Views drop-down list box, select the view in which you want to create a new level.
- 2 Right-click the view name.
- 3 On the right-click menu, click **Create New Object**.
- 4 In the Add Object dialog box, in the Name field, type the name of the new level (or a logical category).  
The name must be unique.
- 5 Click **OK**.

## Adding objects to views

After adding objects to a view in the Java View Builder, you can view them in the Veritas Backup Reporter console.

---

**Note:** In Veritas Backup Reporter, you can copy (drag and drop) an existing view object to your view even if you do not have the required write permissions. However, you cannot modify any of its attributes.

---

---

**Note:** To add objects to a view in the Java View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

#### To add objects to views

- 1 In the View Builder window, select the view and the level or logical category (if any) in which you want to add view objects.
- 2 On the Unassigned Objects tab, select one or more objects in the table that you want to add to the view.

You can select objects in succession by using click + SHIFT. Select distinct objects by using click + CTRL.

- 3 Drag the selected objects and drop it onto the view or level.

The View Builder increments the number directly beneath the view or level to which you added the object. To view a list of all recently modified objects, click the Recently Accessed Assets tab.

## Searching for objects

You can search for objects (IT assets) in the Veritas Backup Reporter database.

---

**Note:** To access the Java View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

#### To search for objects

- 1 In the View Builder window, on the Search Objects tab, in the Search text box, type a name (or part of a name) for an object that you want to locate.

The search is case insensitive.

- 2 Click **Search**.

## Removing views, levels, or objects

You can delete views, levels, or objects from the View Builder. If you delete a view (or a level), all objects under the view (or the level) are also deleted.

---

**Note:** To access the Veritas Backup Reporter View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

**To remove views, levels, or objects**

- 1 In the View Builder window, select the view, level, or object that you want to delete.
- 2 Right-click the view, level, or object.
- 3 On the right-click menu, click **Delete**.
- 4 In the Delete All dialog box, click **OK**.

## Renaming views, levels, and objects

You can rename views, levels, and objects that are stored in the Veritas Backup Reporter database.

---

**Note:** To access the Veritas Backup Reporter View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

**To rename views and levels**

- 1 In the View Builder window, select the view or level that you want to rename.
- 2 Right-click the view, level, or object that you want to rename.
- 3 On the right-click menu, click **Rename**.
- 4 Type the new name for the view, level, or object and then press **Enter**.

The new name must be unique.

## Managing user access to views

You can specify which user accounts or user groups should have access to a view.

---

**Note:** To access the Veritas Backup Reporter View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

### To manage user and group access to views

- 1 In the View Builder window, select the view for which you want to set access rights.  
Setting access rights for the view has precedence over access rights set at the object level.
- 2 Right-click the view that you want to set access right for.
- 3 On the right-click menu, click **Properties**.
- 4 On the User Security tab, add available users to the Granted Read Permission list box or the Granted Write Permission list box, and click **Ok**.
- 5 On the Group Security tab, add available user groups to the Granted Read Permission list box or the Granted Write Permission list box, and click **Ok**.

## Managing user access to levels or objects

You can specify which user accounts or user groups should have access to a level or an object.

---

**Note:** To use the Veritas Backup Reporter View Builder, you must have administrator privileges on the Veritas Backup Reporter Management Server.

---

### To manage user and group access to views

- 1 In the View Builder window, select the level or the object for which you want to set access right.
- 2 Right-click the level or the object that you want to set access rights for.
- 3 On the right-click menu, click **Properties**.
- 4 On the User Security tab, add available users to the Granted Write Permission list box, and click **Ok**.
- 5 On the Group Security tab, add available user groups to the Granted Write Permission list box, and click **Ok**.

## Viewing object views

Use the Views tab in the Veritas Backup Reporter console to view information about your information technology (IT) assets. These views, called object views, can be organized in a variety of ways to suit your needs.

### To view object views

- ◆ In the Veritas Backup Reporter console, click **Views**. The Views page displays information about backup resources and groupings.

An object view can contain detailed information about an object, such as a host or file system, or lists of data for a class of objects in table format.

See [“Viewing details about hosts and file systems”](#) on page 288.

The type of information that appears in a detail view depends on the object category.

See [“Selecting object view categories”](#) on page 286.

The task pane, on the left side of the console window, provides easy access to views by means of a hierarchical tree view.

## About navigating object views

Familiarity with the structure of object views is helpful for navigating through the views and for performing other tasks in the console, such as generating reports.

Object views are organized into multiple hierarchical levels. The highest is the level of the entire view itself, referred to as the top level or view level. Discovered objects such as hosts and file systems occupy the lowest levels of the view.

Typically, between the top and bottom levels there are several user-defined levels that serve to organize objects in the view into a useful structure.

When you are in the Views section of the console, the task pane displays the view hierarchy in the format of a tree view. A navigation path at the top of the content pane displays the hierarchy of views and allows you to retrace your steps easily.

## Selecting object view categories

Your administrator defines object view categories for your installation. Following are some examples of object view categories:

- Geography
- Line of business
- Application
- Service provider
- Data classification
- Regulatory
- Server type

■ Backup infrastructure

**To select object view categories**

- 1 At the top of the task pane, select the category of object views you want to browse from the drop-down list.
- 2 Click **Go**.

## About object levels

As you work in the console, it is helpful to understand object levels and the way they are represented in the tree view. The Report Wizard, for example, has controls that use object levels to define the scope of your reports and how they display data.

All levels below the top level (the view level) are numbered, from Level 1 down to the lowest level defined for the view. The lowest levels consist of discovered objects: hosts and their associated file systems. The higher levels consist of nodes created by an administrator to organize the lower-level objects into logical groupings.

Figure 7-2 shows a sample tree view called Geography, with level numbers shown for some of the objects in the tree.

**Figure 7-2** Views tab



In this example, the tree view displays three numbered levels: Level 1, which includes AsiaPac and North America; Level 2, which includes country names such as Australia and Canada; and Level 3, which includes city names such as Sydney and Toronto.

Lower levels representing hosts (Level 4) and file systems (Level 5) are not shown in the tree view for this example.

## Viewing a list of hosts

You can view a list of hosts in the content pane.

### To view a list of hosts

- ◆ Do one of the following:
  - Select an object at the next highest level (such as Toronto) to display a list of its hosts in the content pane.
  - Click **Show/Hide Hosts** to display hosts in the tree view.  
You can display additional levels by drilling down in the content pane. For example, when you display the object view for a host (Level 4) in the content pane, you can click from lists of file systems (Level 5).

## Searching for hosts

You can search for specific hosts within the content pane. For example, when Toronto appears in the content pane, you can quickly find and display details about host\_01 in Toronto, or about all hosts whose names start with host\_0.

### To search for hosts

- 1 Display a high-level view in the console content pane.
- 2 On the Search Hosts subtab, in the Search text box, type a text string.  
The string can be a host name or a partial host name. Use the percent sign (%) as a wildcard character.  
Examples:
  - `host_01` displays the host named host\_01.
  - `host_0%` displays all hosts whose names begin with host\_0.
  - `%row%` displays all of the following hosts: row, arrow, rowland35, and brown.
- 3 Click **Go**.
- 4 Select a host name to view the object view for the host.

## Viewing details about hosts and file systems

The detail view for a host displays the host's attributes and lists of the file systems defined on the host.

### To display the detail view for a host

- ◆ Select the name of a host in a higher-level view or in the tree view.

## Viewing host attributes

Veritas Backup Reporter Agent Modules discover a great deal of data about objects in your network. The terms information or details are used to describe these different kinds of data. Attributes refer to a specific kind of data; details pertain to a specific object type. For example, the attributes for a host include its name, operating system, and whether it is a NetBackup master server or media server.

To display a list of attributes for a host, click **Edit** in a table.

You can edit host attributes.

## Viewing host file systems

In a host's detail view, the **Defined File Systems** list displays a list of the file systems defined on the host.

### To display host file systems

- ◆ Select the name of a file system.

## Viewing host backup jobs

If the host is a NetBackup master server or media server, you can view detailed information about current and completed backup jobs running on the host.

### To view current backup jobs

- ◆ Click **Backup Jobs**.

### To view completed backup jobs

- 1 Click **Backup Jobs** in the drop-down list, and then click **Go**.
- 2 Select a backup job in the list to view details about it.

## Managing host aliases

You can give each host alias names. The host's primary alias displays in tree views and in higher-level object views. Its other aliases are used when you are searching for hosts on the network. Alias names are also used by agent modules as they gather information from hosts in the network.

In Veritas Backup Reporter Java View Builder, you can alias multiple hosts simultaneously by using the **Alias Hosts** option.

For more details, refer to *Java View Builder Online Help*.

### To view a list of host aliases

- ◆ In the Veritas Backup Reporter console, click **Views > Host Aliases**.

---

**Warning:** It is essential that your alias names are compatible with your hosts' DNS names or with the names by which they are known to applications such as NetBackup and Backup Exec. For example, if you use an alias that is unknown to NetBackup, the explorer stops collecting information from the NetBackup host and instead attempts to collect data from a host with the alias name.

---

### To create a host alias

- 1 In the task pane view, click a host name.
- 2 In a host's detail view, click **Host Aliases** from the drop-down list, and then click the green checkmark icon.
- 3 In the Manage Host Aliases dialog box, do the following:
  - In the Host Name drop-down list, select the name of the host.
  - Type a new alias in the New Name field, or change the primary alias in the Primary Name field.
  - Optionally, modify other alias names that appear in the dialog box.
  - Click **Save**.
- 4 When you finish, click **Cancel** to exit the dialog window.
- 5 To create additional alias names for the host, repeat 3.

## Viewing host IP addresses

You can view host IP addresses.

### To view a list of host IP addresses

- 1 Click **Views > Host IPs**.
- 2 Click a column header to sort the list by IP address.

The sort is a text sort. For example, IP addresses would be listed in this order:  
nn.nn.nn.109, nn.nn.nn.11, nn.nn.nn.110.

## Viewing reports for individual hosts

You can view reports for an individual host or a collection of hosts by clicking the **Report Mode** icon in the task pane.

**To view a report for individual hosts**

- ◆ To view a report, check an item in the tree view (such as Toronto) or an individual host, and then click **Create Report**.

**About viewing tabular information about a class of objects**

Agent modules that run on one or more hosts in your network collect information about objects in the network. This information is presented in the form of tables in the Views section of the Veritas Backup Reporter console.

**About displaying a table of objects**

Whenever you select an object in the tree view (other than a host), the content pane displays a table listing the objects at the next level. For example, if you select Sydney in the tree view, a table listing the hosts in the Sydney office appears.

**Figure 7-3** Example of a table in the Veritas Backup Reporter console

Details ▲	Object Name	Object Type	Attributes
	ccsqawindp1	Host	
	illusion.vxindia.veritas.com	Host	
	blueberry.vxindia.veritas.com	Host	
	ccsqawinsp1.vxindia.veritas.com	Host	
	gorpu.vxindia.veritas.com	Host	
	pinacolada.vxindia.veritas.com	Host	
	harishw.vxindia.veritas.com	Host	
	harishw	Host	
	adrenolize	Host	
	ccsqawinsp1	Host	
#	<b>Total Objects: 10</b>		

**About launching an additional object view**

In many object views, you can select the display names for higher-level and lower-level objects in the tables. Selecting the name of a lower-level object displays a view for that object. For example, if you are displaying a list of all the hosts in Hong Kong, you can select the name of a host to display a detailed object view for that host.

See [“About navigating object views”](#) on page 286.

**Customizing views**

You can create custom views that fit the particular needs of your enterprise.

## About creating custom views using the View Builder

An administrator can create custom views that display selected information for a particular class of objects or grouping of objects. This is done using the View Builder, an application for creating, modifying, and managing access to object views.

## About creating backup views to display data by file system

If most of your backup policies create backup jobs that include only one path, your views and reports can show data at the file system level. For example, if you have a machine where `D:\` is used by Division D and `E:\` is used by Division E, you can create views and reports showing jobs that affect one division without showing other jobs being run for that machine.

For example, you can create a view similar to the following:

Divisions

Division D

HostA

D:\

Division E

HostA

E:\

## Verifying your customized host views

To verify that hosts are listed in your customized views as you expect, check the host mapping settings. You can access these displays by clicking their subtabs in the Views area of the console.

### To verify customized host views

- ◆ Click **Host Mapping Summary** to view, for each host, an icon indicating whether or not it is represented in each type of view.

For example, a green icon in the Geography column for `db2host` indicates that `db2host` is represented in the Geography view. Click an icon to display the host's detail view.

### To verify the higher-level grouping for each host

- ◆ Click **Host Mapping Details**.

For example, `samplehost` might be found in the Geography view under `Toronto` and in the Application view under `DB2 Servers`.

### To verify the detail view for a particular host

- ◆ In the Host Mapping Details table, click a hyperlinked cell.

For example, on the row for `samplehost`, clicking `Toronto` in the Geography column will display the detail view for `samplehost` with the Geography tree visible in the task pane.

## Managing attributes

Veritas Backup Reporter discovers a great deal of data about hosts and other objects. The terms information or details are used to describe these different kinds of data.

The term attributes refers to detailed data that pertains to a specific object type. For example, the attributes for a host include its vendor name, model, and operating system. Veritas Backup Reporter Agent Modules query objects on the network and retrieve a standard set of attributes for each type of object.

Some attributes contain relevant details that cannot be discovered by Veritas Backup Reporter or any other software application. These user-created or custom attributes convey information that is meaningful to you but is not part of the object's physical or software makeup.

Some common examples include:

- Physical location of the object
- Warranty date for the object
- Date of purchase
- Date of most recent service
- Contact information for parties responsible for maintenance

You can add, change, or delete customized attributes for an object.

---

**Note:** Custom attributes are added on a per object basis. There is no way to create an attribute for a group of objects and set a default value for that attribute.

---

## About viewing attributes

You can view attributes for a host by displaying the host's detail view.

## Editing attributes

You can edit the value of several attributes, including the name by which a host object displays in the console. A `Misc Info` attribute is provided for specifying details such as the object's physical location.

### To edit attributes

- 1 Display the object's detail view.
- 2 On the drop-down list, click **Edit Attributes**, and then click **Go**.
- 3 In the Edit Attribute dialog box, do the following:
  - For each attribute you want to edit, type a new value in the Value column, or select a value from the drop-down list.
  - Click **Update**.

# Understanding Veritas Backup Reporter alerts

This chapter includes the following topics:

- [About alerts and the Alert Manager](#)
- [Working with alert recipients](#)
- [Working with alert policies](#)
- [Setting alert filters](#)
- [Configuring pagination settings](#)
- [Working with alerts](#)
- [Customizing Alert Manager settings](#)
- [Using SNMP with Veritas Backup Reporter](#)

## About alerts and the Alert Manager

An alert is a warning that Veritas Backup Reporter (VBR) generates when a specific condition - usually an alarming situation - occurs in the system. You can notify the concerned officials about the alerts by sending an email or an SNMP trap, which help them take corrective actions. The generated alerts are stored in the VBR database. You can view them using the Alerts section in the VBR console.

See [“Using SNMP with Veritas Backup Reporter”](#) on page 323.

VBR 6.6 replaces VxAM - a shared alerting component - with the new alert engine called Alert Manager because it supports Sybase SA 10. VBR 6.6 uses Sybase SA 10 database management system to store the data collected from various point products.

Alert Manager is a part of the CORBA server.

See [“About the CORBA Client/Server”](#) on page 29.

Unlike the VxAM service, the Alert Manager service does not appear in the list of the VBR services that are currently running.

Alert Manager keeps track of the alert conditions / policy types specified in the alert policies and generates alerts appropriately.

In VBR 6.6, alert conditions are referred to as Policy types.

---

**Note:** By default, the Alert Manager functionality is enabled. To disable it, modify the `server.conf` file.

See [“Enabling or disabling Alert Manager”](#) on page 322.

---

[Table 8-1](#) lists the conditions and their corresponding Policy types in VBR, for which alerts are generated.

**Table 8-1** Policy types

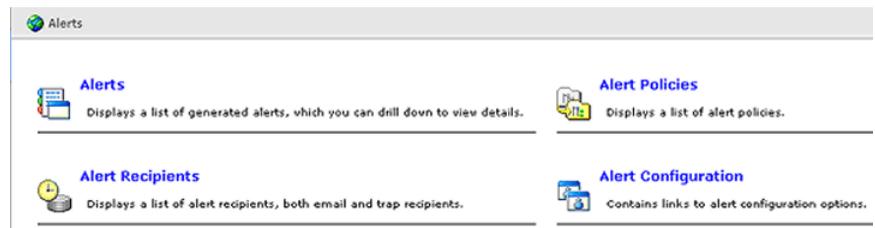
Condition	Policy type
When VBR agent collects an unsuccessful job	Backup Job Unsuccessful  <b>Note:</b> This policy type is valid only in case of backup data. Ignore this policy type if you want to generate an alert depending on archive data collected from Enterprise Vault.
When the spooler disk space reaches its maximum value (or threshold)  The maximum spooler disk space is specified while configuring a Veritas Backup Reporter Agent.  Refer to the Agent configuration documentation for more details.	Spooler Disk Space Reached Threshold
When the communication between Veritas Backup Reporter Agent and Management Server breaks	Agent Server Communication Break
When an agent throws an exception while collecting backup data	Agent Exception
When a condition, stated while generating a report, is satisfied	Report Trigger

Each alert condition or policy type corresponds to a policy. When a condition stated in a policy is satisfied, an alert is generated and notifications in the form of emails or SNMP traps are sent to the associated recipients.

See [“Working with alert policies”](#) on page 307.

[Figure 8-1](#) shows the Alerts home page, where all alerts-related links are available.

**Figure 8-1** Alerts home page



[Table 8-2](#) lists the steps describing the usage of the alerts functionality, not necessarily in that order.

**Table 8-2** Using the alerts functionality

Step number	Step	Reference topic
1	<p>Create alert recipients to whom emails or SNMP traps are sent when a particular alert condition is met.</p> <p>Make sure that the mail server is configured to send emails.</p>	<p>See <a href="#">“Creating email recipients”</a> on page 300.</p> <p>See <a href="#">“Creating SNMP trap recipients”</a> on page 303.</p> <p>See <a href="#">“Configuring SMTP server using global system settings”</a> on page 137.</p> <p>See <a href="#">“Using SNMP with Veritas Backup Reporter”</a> on page 323.</p>
2	<p>Set alert policies for various conditions or policy types.</p> <p><b>Note:</b> You need administrator’s rights to create alert policies.</p>	<p>See <a href="#">“Creating alert policies”</a> on page 307.</p>
3	<p>Set alert filters that you can apply while viewing alerts.</p> <p><b>Note:</b> This is an optional step.</p> <p><b>Note:</b> You need administrator’s rights to set alert filters.</p>	<p>See <a href="#">“Setting alert filters”</a> on page 314.</p>

**Table 8-2** Using the alerts functionality (*continued*)

Step number	Step	Reference topic
4	View generated alerts.	See <a href="#">“Viewing alerts”</a> on page 315.
5	Manage alerts. You can acknowledge or clear an alert. You can also add comments for an alert.	See <a href="#">“Managing alerts”</a> on page 318.

## Working with alert recipients

This section provides information on creating and managing email and trap recipients, who receive alert notifications.

You can also create user groups of email recipients, or trap recipients, or email and trap recipients. You can send alert notifications to these groups instead of sending them to individual recipients.

- [Viewing alert recipients](#)
- [Creating email recipients](#)
- [Creating SNMP trap recipients](#)
- [Modifying email / trap recipient information](#)
- [Adding alert recipient groups](#)

### Viewing alert recipients

This section provides information about viewing the existing email recipient, trap recipients, and recipient groups.

**To view email recipients**

- ◆ In the VBR console, click **Alerts > Alert Recipients**. The existing email recipients and email recipient groups are displayed as shown in the following figure:

	Name	Type	Status	Description
<input type="checkbox"/>	Dani	email	Active	Dani@email.com
<input type="checkbox"/>	John	email	Inactive	john@email.com
<input type="checkbox"/>	NBU	email-group	Active	Member Count : 2
<input type="checkbox"/>	VBR	email-group	Inactive	Member Count : 2

The following table describes the fields associated with the existing email recipients and email recipient groups:

See “[Creating email recipients](#)” on page 300.

See “[Creating SNMP trap recipients](#)” on page 303.

Name	Name of the email recipient or recipient group
Type	Type of the recipient. An individual email recipient is represented with the type 'email' and email recipient group is represented with the type 'email-group'.
Status	Status of the email recipient or email recipient group - Active or Inactive
Description	Description of the recipient. It is the email ID in case of the individual email recipient and in case of the email recipient group, it is the number of email recipients / groups it comprises.

### To view trap recipients

- ◆ In the VBR console, click **Alerts > Alert Recipients > Trap Recipients**. The existing trap recipients are displayed as shown in the following figure:

Name	Type	Status	Description
host-group	trap-group	Active	Member Count : 2
success	trap	Active	success.162
victory	trap	Active	victory.162
winner	trap	Active	winner.162

The following table describes the fields associated with the existing trap recipients and trap recipient groups:

See “[Creating email recipients](#)” on page 300.

See “[Creating SNMP trap recipients](#)” on page 303.

Name	Name of the trap recipient or recipient group
Type	Type of the recipient. An individual trap recipient is represented with the type 'trap' and trap recipient group is represented with the type 'trap-group'.
Status	Status of the trap recipient or trap recipient group - Active or Inactive
Description	Description of the recipient. It is the port number for sending the trap in case of the individual trap recipient and in case of the trap recipient group, it is the number of trap recipients / groups it comprises.

## Creating email recipients

Alerts are generated when specific conditions occur. The concerned officials are notified about these alerts by sending emails. While creating an alert policy, you can specify which email ID you want to send a notification to.

---

**Note:** Make sure that the mail server is configured to send emails.

the section called “[Configuring SMTP server using global system settings](#)”

---

---

**Note:** You need administrator’s rights to create email recipients.

---

See “[Modifying email/ trap recipient information](#)” on page 305. to modify recipient attributes, status and other available settings.

You can notify multiple users about a particular alert via SNMP traps, at a time. To do this, you need to create user groups and mark this group to receive notifications, instead of marking individual users.

See “[Adding alert recipient groups](#)” on page 306.

**To create email recipients**

- 1 In the VBR console, click **Alerts > Alert Recipients**.
- 2 In the Email Recipients tab, click **Create** to create new email recipients. The Email Recipient Attributes page is displayed as shown in the following figure:

**Email Recipient Attributes**

Name :

Email :

Active :

---

**Alert Notification Delivery Limit Settings**

Maximum Number Of Messages :

Delivery Time Span :  Hour(s)

Reset Message Count After Time :  Hour(s)

Activate Delivery Limit :

**3** Enter the following information:

Name	Enter the name of the official whom you want to notify about an alert.
Email	Enter the email ID of the official, to which alert notifications are sent.
Active	Select this check box if you want this recipient to receive alert notifications via emails.
Maximum Number of Messages	Enter the maximum number of notifications that you want to receive within the specified Delivery Time Span.
Delivery Time Span	Enter the time duration in hours, minutes, or seconds, during which notifications are sent. Once the message count reaches Maximum Number of Messages, Alert Manager blocks the delivery of any new notifications to the associated recipient for the time period specified for Reset Message Count After Time.
Reset Message Count After Time	<p>Enter the time interval in hours, minutes, or seconds, during which notifications are blocked if the message count has reached Maximum Number of Messages. Once this time period is over, Maximum Number of Messages is reset and Alert Manager starts sending notifications for the specified Delivery Time Span.</p> <p><b>Note:</b> For example, if Maximum Number of Messages = 10, Delivery Time Span = 30 Minutes, and Reset Message Count After Time = 2 Hours, Alert Manager sends messages until message count reaches 10 in 30 Minutes. Once it has sent 10 messages, it blocks the delivery of new messages for next 2 Hours. After 2 hours, Alert Manager once again starts sending messages until message count reaches 10.</p>
Activate Delivery Limit	Select this check box to activate the Alert Notification Delivery Limit settings. If you do not select this check box, Maximum Number of Messages, Delivery Time Span, and Reset Message Count After Time are not taken into account while sending notifications. The notifications are sent as soon as alerts are generated.

**4** Click **Save**.

## About email notification formats

This section provides a few examples of the email notification formats for various policy types.

Email notification format for the Agent Server Communication policy type

Agent Host Name : ccs-win-qe-1

Server Host Name : ccs-win-qe-1

Heartbeat Time : Thu Nov 20 12:30:34 IST 2008

Email notification format for the Backup Job Unsuccessful policy type

Job ID : 122690357400012269035760003102

Start Time : Mon Nov 17 12:02:54 IST 2008

End Time : Mon Nov 17 12:02:56 IST 2008

Master Server Name : HOGWARTS

Media Server Name : HOGWARTS

Client Name : HOGWARTS

Policy Name : STANDARD

Schedule Name : No Schedule

Product Name : Veritas NetBackup

Email notification format for the Report Trigger policy type

Condition Backup Job Size (MB) is less than 200.00 or greater than 100.00 on trigger has matched

## Creating SNMP trap recipients

Traps, also known as interrupts, are signals sent to inform programs that an event has occurred. In VBR, traps are notifications that are sent to a specified SNMP host or group of hosts when a condition is met.

A trap recipient is a host that receives notifications in the form of SNMP traps when an alert condition is met. For example, a trap is sent after an alert was generated as a result of failure of communication between the VBR Agent and Management Server.

See [“Using SNMP with Veritas Backup Reporter”](#) on page 323.

---

**Note:** You need administrator's rights to create SNMP trap recipients.

---

See “[Modifying email/ trap recipient information](#)” on page 305. to modify recipient attributes, status and other available settings.

You can notify multiple users about a particular alert via SNMP traps, at a time. To do this, you need to create user groups and mark this group to receive notifications, instead of marking individual users.

See “[Adding alert recipient groups](#)” on page 306.

### To create trap recipients

- 1 In the VBR console, click **Alerts > Alert Recipients**.
- 2 On the Trap Recipients tab, click **Create**. The Trap Recipient Attributes page is displayed as shown in the following figure:

**Trap Recipient Attributes**

Name :

Host :

Port :

Active :

**Alert Notification Delivery Limit Settings**

Maximum Number Of Messages :

Delivery Time Span :  Hour(s)

Reset Message Count After Time :  Hour(s)

Activate Delivery Limit :

[Back](#)

**3** Enter the following information:

Name	Enter the name of the official whom you want to notify about an alert.
Host	Enter an SNMP host, which you want to send traps to.
Port	Enter the port number on the SNMP host where you want to send traps.
Active	Select this check box if you want this recipient to receive alert notifications via SNMP traps.
Maximum Number of Messages	Enter a maximum number of notifications that can be sent within the specified Delivery Time Span.
Delivery Time Span	Enter the time duration in hours, minutes, or seconds, during which notifications are sent. Once the message count reaches Maximum Number of Messages, Alert Manager blocks the delivery of any new notifications to the associated recipient for the time period specified for Reset Message Count After Time.
Reset Message Count After Time	Enter the time period in hours, minutes, or seconds, during which notifications are blocked if the message count has reached Maximum Number of Messages. Once this time period is over, Maximum Number of Messages is reset and Alert Manager starts sending notifications for the specified Delivery Time Span.
Activate Delivery Limit	Select this check box to activate the Alert Notification Delivery Limit settings. If you do not select this check box, Maximum Number of Messages, Delivery Time Span, and Reset Message Count After Time are not taken into account while sending notifications. The notifications are sent as soon as alerts are generated.

**4** Click **Save**.

## Modifying email / trap recipient information

Only VBR administrator can modify email / trap recipient information.

See [“Creating email recipients”](#) on page 300.

See [“Creating SNMP trap recipients”](#) on page 303.

### To modify email / trap recipient information

- 1 In the VBR console, click **Alerts > Alert Recipients**.
- 2 In the Email Recipients tab or Trap Recipients tab, select email / trap recipient from the table, that you want to edit.
- 3 On the modify email / trap recipient page, change email / trap recipient attributes and Alert Notification Delivery Limit Settings.
- 4 Click **Save**.

## Adding alert recipient groups

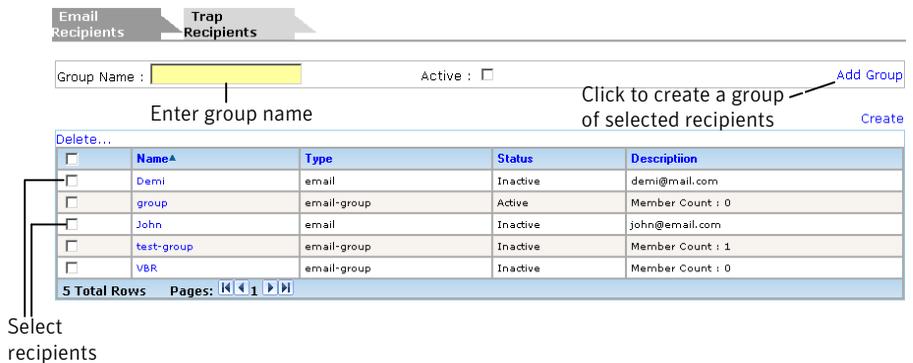
Only VBR administrator can add email / trap recipient groups, to which you want to send alert notifications. You can send alert notifications to these groups instead of sending them to individual recipients. You can create user groups comprising email recipients, or trap recipients, or email and trap recipients.

See “[Creating email recipients](#)” on page 300.

See “[Creating SNMP trap recipients](#)” on page 303.

### To add alert recipient groups

- 1 In the VBR console, click **Alerts > Alert Recipients**.
- 2 You can create email recipient groups on the Email Recipients tab. To create trap recipient group, click **Trap Recipients**.
- 3 On Email / Trap Recipients tab, select individual recipients or groups that you want to add to a group, as shown in the following figure:



- 4 In the Group Name text box, enter the name of the group.

- 5 Select the Active check box.

If the status of a group is not set to 'Active', recipients in that group do not receive alert notifications irrespective of their individual statuses.

- 6 Click **Add Group**.

## Working with alert policies

This section provides information about creating and managing alert policies.

---

**Note:** You need administrator's rights to create, modify, view, or manage alert policies.

---

- [Creating alert policies](#)
- [About modifying alert policies](#)
- [Viewing alert policies](#)
- [Managing alert policies](#)

## Creating alert policies

An alert policy holds a definition of an alert. You need to create an alert policy and specify a condition, which you want to generate an alert for. Each alert policy corresponds to a single alert condition. An alert condition is referred to as policy type in VBR context.

For example: Create an alert policy called P1Job with Job Unsuccessful as a policy type. If the status of the P1Job policy is 'Active', while collecting unsuccessful job data, an alert is generated.

The Alert Manager provides a wizard that makes creating alert policies easier. The alert policy wizard asks for the following information, in that order:

Policy Types	Select a policy type, for which you want to generate alerts. You can select only one policy type and this is a mandatory step.  The detailed steps to create an alert are described in the following section.
Policy Attributes	Enter attributes for the policy such as, name, description, severity, and status.  Policy name is a mandatory field.

- Email Recipients**      Select email recipients to whom you want to send email notifications when alerts are generated against the policy type associated with this policy. You can select the recipients later and save the policy at this stage and close the wizard.
- All email recipients that you have created earlier are made available for selection.
- See “[Creating email recipients](#)” on page 300.
- Trap Recipients**      Select trap recipients to whom you want to send notifications in the form of SNMP traps when alerts are generated against the policy type associated with this policy. You can select the recipients later and save the policy at this stage and close the wizard.
- All trap recipients that you have created earlier are made available for selection.
- See “[Creating SNMP trap recipients](#)” on page 303.

---

**Note:** You need administrator’s rights to create alert policies.

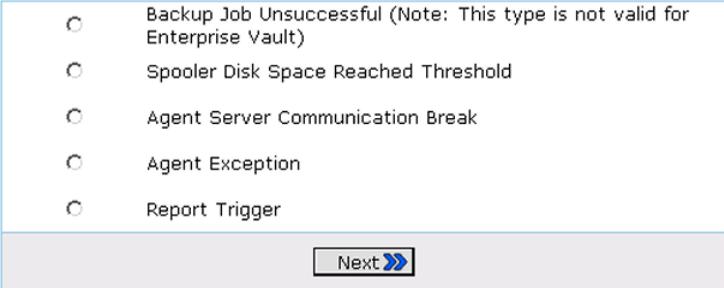
---

#### To create an alert policy

- 1 In the VBR console, click **Alerts > Alert Policies**.
- 2 On the Configured policies page, click **Create**. The Policy Types page is displayed as shown in the following figure:

[Create alert recipients](#) if you do not already have them. You require these recipients while creating a policy.

#### Policy Types:



- Backup Job Unsuccessful (Note: This type is not valid for Enterprise Vault)
- Spooler Disk Space Reached Threshold
- Agent Server Communication Break
- Agent Exception
- Report Trigger

Next >>

**3** Select any of the following policy types:

Backup Job Unsuccessful	<p>Select to generate an alert while collecting unsuccessful job data.</p> <p><b>Note:</b> This policy type is valid only in case of backup data. Ignore this policy type if you want to generate an alert depending on archive data collected from Enterprise Vault.</p>
Spooler Disk-Space Reached Threshold	<p>Select to generate an alert when the spooler disk space reaches its maximum value (or threshold), that is Maximum Data Spool Size On Disk specified while configuring the VBR Agent. Refer to the Agent configuration documentation for more details.</p>
Agent Server Communication	<p>Select to generate an alert when the communication between VBR Agent and Management Server breaks.</p>
Agent Exception	<p>Select to generate an alert when agent throws an exception while collecting backup data.</p>
Report Trigger	<p>Select to generate an alert when a condition stated while generating a report is satisfied.</p> <p>For example, if you have set the following condition while generating a report: Notify if media is used more than 75%. An alert is generated when this condition is satisfied.</p>

To create email / trap recipients, click **Create alert recipients**.

**4** Click **Next**.

**5** Depending on the alert condition you have selected, the application displays the screens that let you refine your alert policies:

- After selecting 'Backup Job Unsuccessful' as the alert condition, the following page is displayed:

**Job Exit Status**

**Select All**

Failure

Missed

Partial Success

Exit Status Code to Include :

**Select View:**

Within View:

You can specify the job status and error code for which you want to raise an alert, described as follows:

Job Exit Status	Select the job status such as, Failure, Missed, Partial Success, or all to generate an alert for a job having this status.
Exit Status Code to Include	Enter an error code to generate an alert when this type of error occurs in the backup product.  You can enter multiple exit status codes, separated by commas.
Within View	Select a view from the drop-down list, if you want to generate an alert for a client that is associated with this view.

- If you have selected 'Spooler Disk-Space Reached Threshold' as the alert condition, the Threshold Limit Options screen appears as shown in the following figure:

**Threshold Limit Options**

Threshold Limit :  % ▼

<< Back
Next >>

---

**Note:** The threshold limit for the spooler that you specify here should not exceed the spooler size mentioned on the Agent Configuration page (Maximum Data Spool Size On Disk).

---

You can specify the spooler threshold limit in MB, GB, or TB, or percentage (%) of the Maximum Data Spool Size On Disk. An alert is generated when the spooler size reaches the threshold limit specified here.

**6** Enter the following policy attributes:

- |                    |  |
|--------------------|--|
| Policy Name        | Enter name of the policy. This is a mandatory field.   |
| Policy Description | Enter brief description of the policy  |
| Policy Severity    | Select severity of the alert to be generated <ul style="list-style-type: none"> <li>■ Informational</li> <li>■ Warning</li> <li>■ Major</li> <li>■ Critical</li> </ul>   |
| Policy Status      | Select the check box if you want to set the policy as 'Active'. <p><b>Note:</b> If you miss to set a policy as 'Active', alerts are not generated even after the condition associated with this policy occurs.</p> |

You can click **Save** and skip the optional steps in the policy wizard or click **Next** to add email recipients.

**7** Select email recipients whom you want to send an email to, when an alert is generated.

You can click **Save** and skip the optional steps in the policy wizard or click **Next** to add trap recipients.

- 8 Select recipients whom you want to send an SNMP trap to, when an alert is generated.
- 9 Click **Save**.

## About modifying alert policies

To modify attributes of an existing alert policy, click **Alerts > Alert Policies**, from the policy list, select the policy name, modify the policy attributes and alert recipients using the policy wizard and click **Save**.

You cannot modify the policy type for the existing policy.

See “[Creating alert policies](#)” on page 307.

## Viewing alert policies

You can view all alert policies in a list.

### To view alert policies

- ◆ In the VBR console, click **Alerts > Alert Policies**. The Policies page is displayed as shown in the following figure:

<input type="checkbox"/>	Name*	View	Status	Description	Severity
<input type="checkbox"/>	agent_exception	Global View (No view selected)	Active		Warning
<input type="checkbox"/>	AgentServerCommunicationBreak	Global View (No view selected)	Active		Warning
<input type="checkbox"/>	JobUnsuccessful	Global View (No view selected)	Active		Warning
<input type="checkbox"/>	JobUnsuccessful-View		Active		Warning
<input type="checkbox"/>	JobUnsuccessfulQES		Active		Warning
<input type="checkbox"/>	ReportTrigger	Global View (No view selected)	Active		Informational

6 Total Rows    Pages: 1 | 1 | 1

Name	Name of the policy
View	Name of the view associated with the unsuccessful job, which you want to generate an alert for
Status	Status of the policy - Active or Inactive
Description	Brief description of the policy
Severity	Severity of the alert associated with this policy.

## Managing alert policies

You can manage an alert policy by changing its status. You can delete alert policies. You can also view alerts generated for the selected alert policy.

---

**Note:** You need administrator's rights to manage policies.

---

### To manage an alert policy

- 1 In the VBR console, click **Alerts > Alert Policies**.
- 2 On the Configured Policies page, select a check box in front of the policy you want to manage.
- 3 Select any of the options from the Settings drop-down list as shown in the following figure:



Activate	Select to activate the selected alert policy. Alerts are generated when the condition specified in this policy occurs.
Deactivate	Select to deactivate the selected alert policy. Alerts are not generated when the condition specified in this policy occurs.
Delete	Select to delete the selected policy.
View Alerts	Select to view the alerts that are generated for this policy type.

- 4 Click **Go**.

## Setting alert filters

To filter alerts to view the required information, you need to first set the alert filters. These filters are made available while viewing the generated alerts.

See “Managing alerts” on page 318.

### To set alert filters

- 1 In the VBR console, click **Alerts > Alert Configuration > Alert Filter**.

The following filter criteria are available as shown:

**Alert Filter**

Retrieve a maximum of  alerts, ordered by **Last Modification Time**  descending

**And**

Show alerts for selected severities

- Informational
- Warning
- Major
- Critical

**And**

Show alerts created or modified since

Month : **JAN** Date : **01** Year : **1999** Hours : **00** Minutes : **00**

**And**

Show alerts for id : **<**

**And**

Show alerts for id : **>=**

**And**

Show alerts updated by : **=**

**And**

Show alerts for selected status

- Active
- Cleared

**Back** **Save**

- Specify the maximum number of alerts you want to view
- Order alerts by Last Modification Time, Creation Time, or Severity
- Sort alerts in the ascending or descending order of their IDs
- Show alerts only with specific severities: Informational, Warning, Major, or Critical
- Show alerts that are generated or modified on or after the specified date
- Show alerts with specific IDs
- Show alerts updated by a specific user
- Show alerts with status Active or Cleared

If you want to set multiple filters, select the associated 'And' check boxes and enter the required values.

- 2 Click **Save**.

# Configuring pagination settings

You can set the number of alerts that you want to view on a single page.

---

**Note:** You need administrator's rights to configure pagination settings.

---

See "[Viewing alerts](#)" on page 315.

## To set pagination

- 1 In the VBR console, click **Alerts > Alert Configuration > Alert Pagination**.
- 2 Enter the page size. For example, enter 50, if you want to view only 50 alerts on one page. If there are more than 50 alerts, the alerts they will be displayed on the following pages.
- 3 Click **Save**.

# Working with alerts

This section provides information about managing alerts.

- [Viewing alerts](#)
- [Managing alerts](#)
- [About Alert Manager log files](#)

## Viewing alerts

You can view all generated alerts in a list. You can set page size and specify the number of alerts you want to view on a single page.

See "[Configuring pagination settings](#)" on page 315.

---

**Note:** Generated alerts are retained for the number of days set in **Settings > Global Settings > Data Retention** section.

After this retention period is over, the alerts are purged.

---

### To view alerts

- 1 In the VBR console, click **Alerts > Alerts**. The following alert details are available on the Alerts page as shown:

Select...		GO					
<input type="checkbox"/>	ID	Count	Severity	Status	Predicate Type	Acknowledged	Summary
<input type="checkbox"/>	1	1	Informational	Active	Report Trigger		Condition Total Backup Job Size (MB) is less than 1.00 or 5
<input type="checkbox"/>	2	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E000FE09
<input type="checkbox"/>	3	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E000FE29
<input type="checkbox"/>	4	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	5	1	Warning	Cleared	Agent Server Communication Break		Agent Server Communication Failure [Agent Host : illusion]
<input type="checkbox"/>	6	3	Warning	Active	Agent Exception		Exception while Data Collection [Agent Host : illusion]
<input type="checkbox"/>	7	3	Warning	Active	Agent Exception		Exception while Data Collection [Agent Host : illusion]
<input type="checkbox"/>	8	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	9	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	10	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	11	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	12	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	13	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	14	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E000881F
<input type="checkbox"/>	15	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E000881F
<input type="checkbox"/>	16	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	17	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	18	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	19	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445
<input type="checkbox"/>	20	1	Warning	Active	Job Unsuccessful		Job is Unsuccessful with Error Code : E0008445

47 Total Rows    Pages: [1](#) [2](#) [3](#) [4](#) [5](#)

**2** You can manage the generated alerts using the Select drop-down list.

See [“Managing alerts”](#) on page 318.

Note the following alert details:

ID	<p>Unique identification number for the alert</p> <p><b>Note:</b> Alerts generated with the same conditions are represented with the same ID.</p>
Count	<p>Number of alerts that are generated against the same condition</p> <p><b>Note:</b> You can view separate alerts against the same condition by modifying the <code>am.conf</code> configuration file. By default, the Alert Manager notifies only about the first alert among the multiple alerts generated against the same condition.</p> <p>See <a href="#">“About customizing autoclear and autocount alert settings”</a> on page 322. .</p>
Severity	<p>Severity of the alert that you have set while creating the policy</p>
Status	<p>Status of the alert, 'Active' or 'Cleared'</p> <p>If the status of an alert is 'Active', it implies that the alert condition is still valid and you should take corrective actions to resolve the issue. The 'Cleared' status of the alert implies that the alert condition is no longer valid.</p> <p><b>Note:</b> All new alerts are active. You can set an alert to 'Cleared', if the condition is no longer valid, using the <b>Alerts &gt; Alerts</b> page. However, you cannot set this alert back to 'Active' if the condition becomes valid after sometime. The Alert Manager generates a new alert against this condition.</p> <p>See <a href="#">“Managing alerts”</a> on page 318.</p> <p><b>Note:</b> By default, the Alert Manager automatically clears alerts of type Agent Server Communication, when the communication is reestablished.</p> <p>See <a href="#">“About customizing autoclear and autocount alert settings”</a> on page 322.</p>
Summary	<p>Brief description about an alert. For example, a job is unsuccessful with error code: 46</p>

Acknowledged	Name of the user who has acknowledged the alert See “ <a href="#">Managing alerts</a> ” on page 318.
Created On	Date on which the alert was generated
Modified On	Date when the alert was last modified. See “ <a href="#">Managing alerts</a> ” on page 318.

## Managing alerts

You can manage alerts, which includes acknowledging them, clearing them, adding comments to them, or applying or resetting alert filters.

### To manage alerts

- 1 In the VBR console, click **Alerts > Alerts**.
- 2 Select the check box in front of the alert that you want to modify.

- 3 From the drop-down list placed above the alerts list, select any of the options as shown:

**Alerts**

---

Select...	GO				
<b>Select...</b>	<b>Severity</b>	<b>Status</b>	<b>Predicate Type</b>		
Acknowledge	Informational	Active	Report Trigger		
Clear	Warning	Active	Job Unsuccessful		
Add Comment	Warning	Active	Job Unsuccessful		
Apply Filter	Warning	Active	Job Unsuccessful		
Reset Filter	Warning	Active	Job Unsuccessful		
<input type="checkbox"/>	4	1	Warning	Active	Job Unsuccessful
<input type="checkbox"/>	5	1	Warning	Cleared	Agent Server Communication Break
<input type="checkbox"/>	6	3	Warning	Active	Agent Exception
<input type="checkbox"/>	7	3	Warning	Active	Agent Exception
<input type="checkbox"/>	8	1	Warning	Active	Job Unsuccessful
<input type="checkbox"/>	9	1	Warning	Active	Job Unsuccessful

Acknowledge

Select this option to state that you have are aware of the alert conditions. After you have acknowledged an alert, your user name appears in the 'Acknowledged' field.

Clear	<p>Select this option if the condition of the selected alert is no longer valid.</p> <p>For example: If an alert is generated after the communication between agent and management server breaks. After a while if the communication is reestablished, you can clear this alert.</p> <p>After clearing an alert, its status is changed from 'Active' to 'Cleared'.</p> <p><b>Note:</b> However, you cannot set the 'Cleared' alert back to 'Active' when the alert condition becomes valid after sometime. Alert Manager generates a new alert if the same alert condition occurs again.</p> <p>By default, the Alert Manager automatically clears the alerts generated as a result of the Agent Server Communication failure, after the communication reestablished. You can change this default setting and choose to clear these type of alerts manually.</p> <p>See “<a href="#">About customizing autoclear and autocount alert settings</a>” on page 322.</p>
Add Comment	<p>Select this option if you want to add any comments about an alert such as, your observations or views about the alert condition.</p>
Apply Filter	<p>Select this option if you want to filter the available alert information as per the alert filter you have set.</p> <p>See “<a href="#">Setting alert filters</a>” on page 314.</p>
Reset Filter	<p>Select this option if you want to reset the alert filter, and view all alerts.</p>

**4 Click Go.**

If you have selected the Add Comments option, clicking the Go button takes you to the next page. Add your comments in the given text box and click **Save**.

## About Alert Manager log files

This section provides information about the locations of Alert Manager log files. You can use these log files for troubleshooting issues that you may face while working with alerts.

The following table provides the locations for Server log files:

Solaris	/var/VRTSccsvs/log/vbr_server-0.log
Windows	Server\CorbaServer\Logs\vbr_server-0.log

The following table provides the locations for Web UI log files:

Solaris	/var/VRTSccsvs/log/vbr-alertmgr0.0.log
Windows	Server\Logs\vbr-alertmgr0.0.log

---

**Note:** You can set Server log file parameters using `server.conf` file located at: `<Install Dir>\Symantec\Veritas Backup Reporter\Corba\conf` and Web UI log file settings using the **Settings > Global Settings > Web Console Configuration** section.

---

## Customizing Alert Manager settings

In certain cases, if you want to change the default Alert Manager settings, you can accomplish it by modifying the Alert Manager configuration files at the following location: `<Install Dir>\Symantec\Veritas Backup Reporter\Corba\conf`.

You can change the default Alert Manager settings by modifying parameters in the following configuration files:

<code>server.conf</code>	You can use this configuration file to enable or disable the Alert Manager functionality.  See <a href="#">“Enabling or disabling Alert Manager”</a> on page 322.
<code>am.conf</code>	You can use this configuration file to change the autocount or autoclear settings.  See <a href="#">“About customizing autoclear and autocount alert settings”</a> on page 322.

---

**Note:** You must restart the CORBA server after modifying the default Alert Manager settings to reflect the latest changes.

See [“Stopping and starting Veritas Backup Reporter services”](#) on page 112.  
the section called “About the CORBA Client/Server”

---

## Enabling or disabling Alert Manager

You can enable or disable the Alert Manager functionality by modifying the `server.conf` configuration file.

### To enable / disable the Alert Manager

- 1 Open the `server.conf` file located at `<Install Dir>\Symantec\Veritas Backup Reporter\Corba\conf`.
- 2 Modify the `com.veritas.ccsvc.am.enable` parameter setting as follows:
  - To enable the Alert Manager, set `com.veritas.ccsvc.am.enable=true`.
  - To disable the Alert Manager, set `com.veritas.ccsvc.am.enable=false`.
- 3 Save the `server.conf` file.
- 4 Restart the CORBA server.

## About customizing autoclear and autocount alert settings

Change the following parameters in the `am.conf` configuration file located at `<Install Dir>\Symantec\Veritas Backup Reporter\Corba\conf` to change autocount and autoclear settings:

`am.autoCount`

Set this parameter to 'false', if you want the Alert Manager to generate separate alerts against the same condition or policy type.

By default, this parameter is set to 'true'. This means that the multiple alerts that are generated against the same condition are represented by a number. This number or count is incremented each time a new alert, against the same condition, is generated.

`am.autoClear`

Set this parameter to 'false', if you want the Alert Manager to automatically clear the alerts that are generated after the communication between the Agent and Management Server breaks.

`am.notifyOnAutoIncrement`

Make sure that the `am.autoCount` parameter is set to 'true', to apply the change in the `am.notifyOnAutoIncrement` parameter setting, on the Alert Manager functionality.

Change this parameter to 'true', if you want to send notifications when the alert count increases each time.

By default, the Alert Manager does not notify about all the alerts that are generated against the same condition, it notifies only about the first alert.

`am.notifyOnAutoClear`

Make sure that the `am.autoClear` parameter is set to 'true', to apply the change in the `am.notifyOnAutoClear` parameter setting, on the Alert Manager functionality.

Set this parameter to 'true', if you want to send notification after an alert was automatically cleared.

`am.notifyOnManualClear`

Set this parameter to 'true', if you want to send notifications after manually clearing alerts.

---

**Note:** Restart the CORBA server after modifying the default alert settings to reflect the latest changes made to the configuration files.

---

## Using SNMP with Veritas Backup Reporter

This section provides information about SNMP and how it is used by VBR.

### About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager and agent model consisting of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

## About SNMP versions

Many versions of SNMP are available.

The versions of SNMP protocol are as follows:

- **SNMPv1**

This is the first and standard version of the protocol and is defined by RFC 1157. This document replaces the earlier versions that were published as RFC 1067 and RFC 1098. Security is based on community strings.

- **SNMPv2**

It was created as an update of SNMPv1 adding several features. The key enhancements to SNMPv2 are focused on the SMI, manager-to-manager capability and protocol operations.

SNMPv2c combines the community-based approach of SNMPv1 with the protocol operation of SNMPv2 and omits all SNMPv2 security features.

The different SNMPv2 variants are as follows:

- The original SNMPv2 (SNMPv2p)
- Community-based SNMPv2 (SNMPv2c)
- User-based SNMPv2 (SNMPv2u)
- SNMPv2 star (SNMPv2\*).

- **SNMPv3**

This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p, and support for proxies. The security is based on that found in SNMPv2u and SNMPv2\*. It is defined by RFC 1905, RFC 1906, RFC 2261, RFC 2262, RFC 2263, RFC 2264, and RFC 2265.

## About SNMP version supported in Veritas Backup Reporter

The default version of SNMP supported in VBR is SNMPv2c. VBR users cannot configure this default version of SNMP.

## About the Management Information Base (MIB) and Veritas Backup Reporter support

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (for example, 1.3.6.1.4.1.2682.1).

These OIDs form a tree. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages.

## About generating SNMP traps using Alert Manager

The Alert Manager component in VBR creates alert policies and generates alerts based on alert conditions or policy types. It sends notifications against the generated alerts, in the form of emails and SNMP traps.

The SNMP configuration is provided by VBR and it is stored in the `nm.conf` configuration file. On the startup of the VBR Management Server, the MIB supported by the Alert Manager is loaded.

When defining an alert policy, VBR associates an SNMP configuration with an alert policy. When an alert policy is created in VBR, a corresponding policy is also created in the Alert Manager. The Alert Manager policy understands different notification actions (traps, Email, and so on) associated with the policy. When an alert is generated the corresponding notification action is automatically executed by the Alert Manager.

## Configuring the SNMP trap community name for Veritas Backup Reporter

For VBR traps, the SNMP trap community name string is VBR by default. The VBR community used by VBR is a public community. Public community implies a read-only access to SNMP traps.

Use the following procedures to configure the SNMP trap community name on Windows and Solaris.

### To configure the SNMP trap community name for Veritas Backup Reporter traps on Windows

- 1 Stop Veritas Backup Reporter CORBA server service.  
See “[Stopping and starting Veritas Backup Reporter services](#)” on page 112. the section called “About the CORBA Client/Server ”
- 2 Navigate to `INSTALL_PATH\Veritas Backup Reporter\Server\CorbaServer\conf` directory and open the `nm.conf` file.  
This file shows the following content under trap configuration:  
`nm.trapCommunity=VBR`  
You can configure the value of `nm.trap.community.name` to a name other than VBR.
- 3 Save the `nm.conf` file.
- 4 Restart Veritas Backup Reporter CORBA server service.

### To configure the SNMP trap community name for Veritas Backup Reporter traps on Solaris

- 1 Stop Veritas Backup Reporter CORBA server service.  
`/opt/VRTSccsvs/bin/vbrserver stop vbrcorbaserver`
- 2 Navigate to `/opt/VRTSccsvs/corbaserver/conf` directory and open the `nm.conf` file.  
The file shows the following content under trap configuration:  
`nm.trapCommunity=VBR`  
You can configure the value of `nm.trap.community.name` to a name other than VBR.
- 3 Save the `nm.conf` file.
- 4 Restart Veritas Backup Reporter CORBA server services by running the following command:  
`/opt/VRTSccsvs/bin/vbrserver start vbrcorbaserver`

## Configuring the port for sending SNMP traps

The default port number that Veritas Backup Reporter uses to send SNMP traps is 0 (currently available port or an ephemeral port). However, this port number can be changed by modifying `nm.conf` file.

---

**Note:** You can configure any non-default port number between 1024 and 65535.

---

The following procedures detail how to configure a non-default port for SNMP traps in Veritas Backup Reporter on Windows and Solaris.

#### To configure the port for sending SNMP traps on Windows

- 1 Stop Veritas Backup Reporter CORBA server service.
- 2 Navigate to `INSTALL_PATH\Veritas Backup Reporter\Server\CorbaServer\conf` directory and open the `nm.conf` file.

The file shows the following content under trap configuration:

```
nm.trapAgentPort=<Port Number>
```

Set the value of `nm.trapAgentPort` parameter to the desired port number.

- 3 Save the `nm.conf` file.
- 4 Restart Veritas Backup Reporter CORBA server service.

#### To configure the port for sending SNMP traps on Solaris

- 1 Stop Veritas Backup Reporter CORBA server service.  

```
/opt/VRTSccsvs/bin/vbrserver stop vbrcorbaserver
```
- 2 Navigate to `/opt/VRTSccsvs/corbaserver/conf` directory and open the `nm.conf` file.

The file shows the following content under trap configuration:

```
nm.trapAgentPort=<Port Number>
```

- 3 Set the value of `nm.trapAgentPort` parameter to the desired port number.
- 4 Save the `nm.conf` file.

Restart Veritas Backup Reporter CORBA server service by running the following command:

```
/opt/VRTSccsvs/bin/vbrserver start vbrcorbaserver
```

## Frequently asked SNMP questions

What is the default version of SNMP that is supported in Veritas Backup Reporter?  
SNMPv2c.

Can the version be configured by the user?

No, you cannot configure the SNMP version.

What is SNMPv2c? How it is different from SNMPv2?

See [“About SNMP versions”](#) on page 324.

Is the Veritas Backup Reporter SNMP community name configurable?

Yes.

See [“Configuring the SNMP trap community name for Veritas Backup Reporter”](#) on page 325.

How is the Veritas Backup Reporter community related to the public community?

Is the default community name of "Veritas Backup Reporter" just a name for the community, but still considered public because of certain attributes?

Generally, the "default read community string" for the public community is "public". Public community means read-only access to SNMP traps.

The community used by Veritas Backup Reporter is public, but the community name is maintained as "VBR".

# Reporting on backup and archive data

This chapter includes the following topics:

- [About VBR reports](#)
- [About backup and recovery reports](#)
- [Using reports for notification](#)
- [Using the reports portal pages](#)
- [Using default reports](#)
- [Generating backup reports](#)
- [Reporting on archive data](#)
- [Creating custom reports](#)
- [Saving report data](#)
- [Exporting reports](#)
- [Printing reports](#)
- [Using custom SQL queries](#)

## About VBR reports

Veritas Backup Reporter reports help you monitor and predict activity in several areas of business services. For example, you can monitor the success rate and predict future trends for backup jobs on the network. You can also display historical

data on the volume of backup tasks being performed on behalf of service consumers.

---

**Note:** Archive data collection from Symantec Enterprise Vault is introduced with VBR 6.6 version.

---

Veritas Backup Reporter provides default reports for backup, recovery, cost, and archiving. You can manipulate the scope and time frame for these default reports to create reports that are useful to you. Veritas Backup Reporter also gives you the option of creating custom reports for specific areas of backup operations.

The default reports, along with the custom reports you create, are accessible using the sub-tabs in the Reports section of the console. For ease in viewing, you can organize the reports you use most often into portal pages, such as My Reports. You can also archive reports and arrange for them to be sent by email to other people.

Additionally, for each report subject, Veritas Backup Reporter provides different types of reports including simple ranking and distribution (pie chart) reports, historical (trending) and forecast reports, and reports correlating multiple data types, such as a comparison of the job success rate versus job size for data backups.

Veritas Backup Reporter reports gather data via Veritas Backup Reporter data collector.

See [“About data collection in Veritas Backup Reporter”](#) on page 172.

You can also use and manage the contents of reports portal pages, customize default reports and create your own reports, use reports for automatic notification, and run custom SQL queries.

## About report types

Veritas Backup Reporter reports include the following types:

Backup reports	The backup reports show information related to backups, such as success rate, job status, and protected bytes. This category also includes recovery reports.
----------------	--

Archive reports	In Veritas Backup Reporter 6.6, a new report category called Archives has been added. This report category contains a number of new reports that are generated based on the archive data collected from Enterprise Vault. You can report on the number of messages that are archived across mailboxes, the size of these messages before and after the archive operation.  See <a href="#">“Reporting on archive data”</a> on page 405.
Explorer reports	Reports under Monitors tab have been moved in the Explorers section in Veritas Backup Reporter 6.6.  See <a href="#">“Viewing explorer reports”</a> on page 399.
Cost reports	The cost reports show chargeback information.  See <a href="#">“Generating a cost report”</a> on page 460.

## Using report formats

Most types of reports available in Veritas Backup Reporter are self-explanatory. For example: A Historical Activity report showing backup job duration for a group of hosts for the past six months. However, many reports fall into one of several broad, easily described format categories, and some report types are special cases that require explanation.

### About Historical reports

You can generate trend and clustered column chart type reports through a Historical (formerly Stacked Bar) report.

Table 9-1 provides the procedures to generate Historical reports

**Table 9-1** How to generate Historical reports

Report type	Procedure
Historical	On a historical report, click Edit. In the Report Time Frame Trendline section, select Yes and run the report.
Clustered Column Chart Type	On a historical report, click Edit. In the Report Grouping section, select Level Type from the Report On drop-down list and run the report.

### About graphical report formats

Report formats are described as follows:

Rankings reports	Display a horizontal bar graph showing all the data for each view level object, from greatest to least, within the selected time frame.
Distribution reports	Display a pie chart showing all the data for each view level object within the selected time frame.
Historical reports	<p>Display a stacked (segmented) bar graph with a trend line superimposed over it, showing the average upward and downward trends of the data over time.</p> <p>For example the total size of each day's backup jobs broken out by geography. Some backup reports use a different bar chart format, displaying clustered columns for easy comparison between two classes of objects or events</p>
Forecast reports	Display a line graph with a forecast line extending to future dates, using linear regression to predict values based on the trend of data within the report's time frame.
Correlation reports	Compare two sets of data, such as backup job success rate and backup job count, to show how the number of jobs affects the success rate. The report displays a separate Y-axis for each data set.
Window reports	<p>Display a bar graph depicting the following data with the specified backup window:</p> <ul style="list-style-type: none"><li>■ Size of backup data</li><li>■ Number of jobs that are backed up</li><li>■ Number of files that are backed up</li></ul>
Tabular reports	Display backup or archiving data in a table

---

**Note:** Historical and forecast reports do not let you select the view level at which report data is aggregated. They always aggregate data at the top level of the view.

---

### About viewing numeric data in a graphical report

Graphical reports present data in a convenient, 'at a glance' fashion. However, some precision may be lost when you use this format. When you are viewing a graphical report, tool tips are available to provide the precise numerical data.

To view the numerical data on which a graphical report is based, move your mouse pointer over an area of the graph.

### About viewing data for a lower aggregate level

When you are viewing a backup report, you can easily view lower-level reports. On a graphical report, when you click an area within a graph, the report refreshes to display data for the next lowest object level.

For example, in a Geography view, you can click a bar labeled Canada to display a bar chart showing data for Toronto and Vancouver. You can select the bar for a host to display data for the host's file systems.

### Saving the contents of a graphical report

You can save a copy of a graphical report to your workstation.

#### To save the contents of a graphical report

- 1 Right-click the report, and then click **Save Picture As**.
- 2 In the Save Picture dialog box, specify a directory path, file name, and format (such as .png).

### Displaying tabular formats in graphical reports

When you are viewing a graphical report, you can view more detailed data in a table. This is helpful when you want to display precise numerical data for more than one object or event at the same time. It is also helpful when you want to capture the data in hard copy or in an email message.

#### To display the contents of a graphical report in a tabular format

- 1 Click **Show Table** at the top of the report display.
- 2 Select any column heading to sort the table by the data in that column: alphabetical order for text, chronological order for dates, and so forth. Select the heading again to sort in reverse order.
- 3 To return to the graphical report, click **Show Chart**.

You might observe blank columns in tabular reports for non-NetBackup jobs. This happens when a column represents data that Veritas Backup Reporter obtains only from NetBackup hosts.

## About backup and recovery reports

Backup reports display historical data about backup operations performed on the network.

Veritas Backup Reporter supports collection of various data types from the multiple backup products. However, for uniformity, Veritas Backup Reporter uses the

NetBackup descriptions for all data types to be collected. The backup data collected by Veritas Backup Reporter is categorized into the following seven data types:

---

**Note:** Since Veritas Backup Reporter 6.5.1, Backup and Recovery reports are combined and displayed under the Backups section. The Recovery section is removed. Note: If you have upgraded from a previous version to Veritas Backup Reporter 6.5.1, after upgrade the previously saved Recovery reports are available at the following location:**Reports > My Reports > My Backup Reports > Recovery**

---

- Job
- Policy and Schedule
- Skipped File
- Error
- Media
- Tape Drive Information
- Image

See “[About data collectors](#)” on page 185.

You can display the following types of information on backup reports:

Activity Planning	Includes the following reports: <ul style="list-style-type: none"><li>■ Job size, file count, job count, and duration.</li><li>■ Forecast of size, job count, and file count.</li><li>■ Size, job count, and file count for a given backup window</li><li>■ Capacity planning reports</li><li>■ Scheduled jobs reports</li></ul> These reports are added in VBR 6.6.
Job Browser	Reports on NetBackup Master Server data
Tape Devices	Reports on tape library capacity and related information
Risk Analysis	Contains Client Coverage, Client Risk Analysis, and Recovery Point Objective reports
Status	Reports on status of jobs - Successful or Failed
Success Rate	Reports on success rate of backing up data

Deduplication	Reports on job protected bytes, job protected files, deduplication savings, deduplication factor. Additionally, shows comparison between backed up bytes and protected bytes and backed up files and protected files.
Disk Pools	Disk-based data protection (DBDP) reports show disk pool capacity and its usage, performance of clients on LAN or SAN, NetBackup Storage Lifecycle Map
Media	Reports on media information, such as tape count, tape used capacity
Custom	Open the Custom Wizard

See “[Generating backup reports](#)” on page 357.

---

**Note:** For description about each of the default / canned backup reports, refer to *Veritas Backup Reporter Report Description White Paper* posted at the following location:

<http://support.veritas.com/docs/320685>

---

The following section describes a few backup reports.

Recovery Point Objective Report	In the event of catastrophic data loss, it is advantageous to have recently backed up all your important data. The longer the interval since your last backup, the greater the amount of lost data. The Recovery Point Objective report displays all servers whose data was not backed up within a recent period of time that you specify. This shows you which servers are at risk.
Tabular Backup Report	This report is more customizable than most others. It lets you choose a set of table columns to display in the report, configure the order in which they appear, and sort the table by column after generating the report. It is best to limit the scope of a tabular report to one or two view level objects and a short time frame to keep from producing tables of an unwieldy length.
Job Status and Job Count By Level Reports	Many reports produce graphs with active hyperlinks that you can select to drill down and display report data aggregated at a lower view level. The Job Status and Job Count By Level reports produce graphs that do not permit drill-down to lower view levels, because the elements represented in the graph are not levels of the object view, but job success and failure rates. As a rule, if the graph legend for a report does not show view levels, you cannot select the active parts of the graph to drill down to a lower view level.

---

**Note:** Job attempt data is included with job data. Data collectors may not return any attempt information, either because the backup product does not keep track of attempts, or as a design decision while job information is collected. You can retrieve job attempt data for any report if you include a Backup Attempt field. If you try to report on attempt data when there is no attempt data, No Data Found message appears in case of a chart report and an empty table in case of a tabular report.

---

## About disk-based data protection reports

Veritas Backup Reporter supports the disk-based data protection (DBDP) feature, which was introduced in NetBackup 6.5. Veritas Backup Reporter provides a set of reports that contain DBDP information.

Tapes are no longer adequate for operational recovery from errors. Disk-based data protection has a number of advantages over tapes, such as reliability, recovery, and storage optimization.

Disk-based data protection reports are as follows:

**NetBackup Disk Pool Capacity** This report lets you determine the total capacity and the actual usage of disks in a disk pool. You can filter the report by parameters such as disk pool name, backup media type, or backup media status. You can also receive notifications if disk pool size reaches a specified threshold.

This report shows high and low watermarks set for a disk pool. The report also shows the actual usage of the disk and its forecasts.

**NetBackup Disk Pool Size Vs. Percentage Full** This report lets you determine the total capacity and the actual usage of disks in a disk pool. You can filter the report by parameters such as disk pool name, backup media type, or backup media status. You can also receive notifications if disk pool size reaches a specified threshold.

On the report chart, click a disk pool name to view the total and used capacity of the respective backup media.

NetBackup SAN Client Performance	<p>This report lets you determine the performance of clients in various transport types, such as SAN (storage area network) or LAN (local area network). The report displays number of jobs that are backed up by a client over SAN or LAN and respective backup job throughputs.</p> <p>Backup job throughput = KB/second Using the Client Performance report data, you can determine the performance of transport types. Using this information, you can decide the transport type to use in the future.</p>
NetBackup Storage Lifecycle Map	<p>This tabular report lists backup clients, their respective protection service levels, policies, job success rates.</p>

## About deduplication backup reports

Deduplication reports are specific to NetBackup PureDisk backup product, which are saved in the Backups reports section.

Veritas Backup Reporter supports data collection from NetBackup PureDisk in addition to the other backup products, such as BackupExec, NetBackup, or Tivoli Storage Manager. The Single Instance Storage (SIS) or deduplication technology of PureDisk is unique in the storage and backup world. PureDisk identifies files and data segments that contain identical data and treats them as a single instance of the file, which it backs up only once. Attributes of identical files, such as name and date of modification can vary. If one or more identical files are modified, PureDisk can identify the uniqueness of the file residing on hosts across the network including remote hosts. It stores only single instance of the changed data segment.

For example, NetBackup has backed up 100 MB data, in which 20 MB of data is duplicate or identical. PureDisk protects the same data but eliminates the duplicacy using deduplication. Therefore, the data protected is 100 MB, but the actual data backed up by PureDisk is 80 MB, as 20 MB of data is duplicate. This results into 20 MB saving of data. In other words, PureDisk saved backing up 20 MB of duplicate data using deduplication.

You can generate the following deduplication reports:

File Factor	<p>Shows the file factor with respect to the number of backed up files. For example, if prior to deduplication, the number of files backed up was 50 and after deduplication, the number of files backed up is 10. The deduplication factor is 50/10, that is 5.</p>
File Savings	<p>Shows total number of files that are saved by PureDisk using the deduplication technology.</p>

Size Factor	Shows the size factor with respect to the size of backed up data. For example, if prior to deduplication, the size of backed up data was 100 MB and after deduplication, the number of size of backed up data is 80 MB, the deduplication factor is as follows:  Deduplication Factor = 100 MB (Pre SIS size) / 80 MB (Post SIS size)  Deduplication Factor = 10 / 8
Size Savings	Shows total size of data that is saved by PureDisk using the deduplication technology.
Protected Size vs. Backedup Size	Shows the graph of total protected data against actual backed up data in MB.
Protected Files vs. Backedup Files	Shows the graph of total protected files against actual backed up files.

## About the new nomenclature in post-VBR-6.5 versions

The following table lists the differences between the user interfaces in Veritas Backup Reporter 6.5 and later versions, such as locations and nomenclature of reports.

**Table 9-2** Difference in report UIs in VBR 6.5 and post 6.5

Nomenclature in VBR 6.5	Nomenclature in post-VBR-6.5 versions
Historical Activity	Activity Planning
Size	Job Size
Duration	Job Duration
Occupancy	Stored Backup Images
Stacked Bar	Historical  <b>Note:</b> You can generate trend and clustered column chart type reports through Historical report, by selecting various filter parameters.  See <a href="#">“About Historical reports”</a> on page 331. for more information.
Pie Chart	Distribution
Drive Throughput - Line	Drive Throughput

**Table 9-2** Difference in report UIs in VBR 6.5 and post 6.5 (*continued*)

Nomenclature in VBR 6.5	Nomenclature in post-VBR-6.5 versions
Tape Library Explorer	Library Summary
Recovery Point Exposure	Recovery Point Objective - RPO
Detailed Report	All Failed Backups
Success Rate vs Backed Up Bytes	Success Rate vs. Amount Backed Up Success Rate vs. Amount Backed Up
Success Rate vs No. of Files	Success Rate vs. File Count
Success Rate Last Attempt (Unremediated)	Success Rate - At Least 1 Success Per Client
Summary Dashboard	Daily Summary of Backup Activity
Window Reports	Backup Window
Size	Job Size
Disk Based	Disk Pools
Client Performance Report	NetBackup SAN Client Performance
Client Protection Service Level Map	NetBackup Storage Lifecycle Map
Disk Capacity v/s Usage	NetBackup Disk Pool Size vs. Percentage Full
High-Low Watermark	NetBackup Disk Pool Capacity
Deduplication Factor (Files)	File Factor
Deduplication Factor (Size)	Size Factor
Deduplication Savings (Files)	File Savings

**Table 9-2** Difference in report UIs in VBR 6.5 and post 6.5 (*continued*)

Nomenclature in VBR 6.5	Nomenclature in post-VBR-6.5 versions
Deduplication Savings (Size)	Size Savings
Future Forecast	Forecast
Size - Forecast	Job Size
Job Count - Forecast	Job Count
File Count - Forecast	File Count
Custom Reports	Custom
Agent Monitoring	Agent Status

**Note:** If you had saved the rankings and distribution formats for reports like Active Job Count, Master Server Count etc., you can still access/edit these reports on upgrading to Veritas Backup Reporter 6.5.1. Similarly, if you had saved any reports in previous versions like Image Size, Success Rate-Line, Library Capacity Comparison etc. which have been removed from Veritas Backup Reporter 6.5.1, you can access and edit these reports in Veritas Backup Reporter 6.5.1 after the upgrade. Only Drive Queue Time-Line report is removed after you upgrade to Veritas Backup Reporter 6.5.1. This is because Veritas Backup Reporter 6.5.1 does not support Drive Queue Time - Line reports.

## Using reports for notification

You can plan for and generate automatic, report-based notifications tailored to the needs of the people in your enterprise. You can also archive data in reports.

Veritas Backup Reporter reports provide several ways to notify staff members when problems occur or generate routine status updates. Veritas Backup Reporter can do the following:

- Notify staff of problems  
 See [“Using report data to notify staff when problems occur”](#) on page 341.
- Generate alerts  
 See [“Using report data to trigger alerts”](#) on page 341.
- Send status updates  
 See [“Sending routine report information”](#) on page 342.

## Using report data to notify staff when problems occur

By setting threshold conditions in a report's definition, Veritas Backup Reporter can notify staff members by email whenever those conditions are not being met.

For example, you can set up a report so that backup admin receives an email message when the backup success rate falls below a certain level.

### To notify staff by email when problems occur

- 1 In the Veritas Backup Reporter console, open a default / canned report or start the Custom Report Wizard.
- 2 Using the controls in the Exception Conditions section of the wizard, define thresholds to represent potential problem conditions.  
  
These are the conditions under which Veritas Backup Reporter will send notifications.
- 3 Click **Run** to run the report.
- 4 Save the report.
- 5 Create or edit an email report.
- 6 In the Create Email Report or Edit Email Report page, select the report you just saved, select schedule, and then update the conditions list so that the report is included in the email report when the conditions are met.
  - If there are no schedules available for selection, click the **Create New Schedule** icon.
  - On the Create Schedule page, enter schedule name, time, and recurrence pattern.
  - Click **Save**. This redirects you to the Create Email Report or Edit Email Report page and the added schedule is available in the Schedule drop-down list, for selection.

Veritas Backup Reporter runs the report as per the selected schedule and sends email notifications when a potential problem is detected.

## Using report data to trigger alerts

When you set threshold conditions in a report's definition, Veritas Backup Reporter can trigger an alert when those conditions are met. An alert is a form of notification designed to call attention to a potential problem. Alerts appear in the Veritas Backup Reporter console. You can also use them to initiate automated responses, called policies.

For example, you can set up a report so that an alert is generated when the percentage of failed backup jobs reaches a certain level, or when the total size of all backup jobs exceeds a certain threshold.

#### To define a report to trigger alerts

- 1 In the Veritas Backup Reporter console, open a predefined (default) report or start the Custom Report wizard.
- 2 On the Custom Report wizard, in the Exception Conditions section, define thresholds to represent potential problem conditions.
- 3 Click **Run** to run the report.
- 4 Save the report.
- 5 Create or edit alert trigger reports.
- 6 In the Create Email Report or Edit Email Report dialog box, select the report you just saved and then update the conditions list so that the report is not attached when the conditions are met.

Veritas Backup Reporter runs the report at regular intervals and triggers an alert whenever the report conditions are met (whenever a potential problem is detected).

## Sending routine report information

You can send an individual report, contents of a portal page, or set of reports by email to other personnel in your organization. This topic describes how to send the report or portal page you are currently viewing in the Veritas Backup Reporter console.

You can also schedule routine email deliveries of report data on a regular basis.

#### To email a report

- 1 Display a report in the console.
- 2 Click **Email**.
- 3 In the Email Report dialog box, type a subject line in the Subject field.
- 4 Specify one or more recipients by doing one of the following:
  - Type (or paste from your system clipboard) a list of email addresses in the Send To field. Use commas to separate each address in the list, for example **reggie@example.com,mark@example.com,sammy@example.com**.
  - Select a distribution list from the drop-down list.

- 5 Type (or paste from your system clipboard) an optional list of carbon copy (cc) recipients in the CC to field.

Use commas to separate each address in the list.

- 6 Type an optional message in the Message field, for example:

**This report shows backup job status as of Thursday morning.**

- 7 Click **Send**.

#### To send the contents of a report portal page by email

- 1 Select a report subject from the menu bar on the My Reports page, and click Email Portal.

- 2 In the Email Report dialog box, type a subject line in the Subject field.

- 3 Specify one or more recipients by doing one of the following:

- Type (or paste from your system clipboard) a list of email addresses in the Send To field. Use commas to separate each address in the list, for example **reggie@example.com,mark@example.com,sammy@example.com**.

- Select a distribution list from the drop-down list.

- 4 Optionally, specify additional recipients in the CC to box.

Use commas to separate each address in the list.

- 5 Type an optional message in the Message field, for example:

**These reports show key backup data as of Thursday morning.**

- 6 Click **Send**.

## Using the reports portal pages

Reports tab has a portal page, which you can personalize. This portal page is referred to as the 'My Reports' page.

This page functions as your personalized portal that displays a personalized set of reports.

---

**Note:** In VBR versions after 6.5, all saved reports - default or custom - are saved in the **Reports > My Reports** section. You can edit or delete these reports as you want. The sections, such as Backups or Costs show only generated reports and not saved reports. The My Reports portal shows all saved reports in a single main portal, instead of showing them under separate portals, such as My Backup Reports.

---

## Refreshing reports portal pages

When you load a portal page for the first time during a session, Veritas Backup Reporter runs that page's reports and displays the current data. The reports are then cached so that, on subsequent page loads, they are not refreshed.

As your needs change, you can change the contents of your portal page, adding new content and deleting content that you no longer need.

### To refresh reports portal page

- 1 Click the **Reports > My Reports**.
- 2 To refresh the reports, click **Refresh all reports** at the top of the page.

Reports on portal page are refreshed under three additional circumstances:

- When you schedule regular updates for cached reports
- When you modify a report in any way
- When the reports run for notification purposes

## About selecting reports using the tree view

For each portal page, a tree view in the task pane provides access to your saved reports and to additional reports.

The first branch of the tree view is the *My Report Type* Reports folder, for example My Backup Reports. This folder contains all of your saved reports for the indicated subject, and it helps you organize your reports into customizable subfolders. Select a saved report to view it in the content pane.

Below My <Subject> Reports are additional folders representing other reports available for the indicated subject. Expand one of these branches to view the individual reports beneath it.

When you click a report in the tree view, the Custom Report Wizard displays in the content pane, giving you the chance to run the report with the specific characteristics you want, such as format, scope, and time frame.

Using quick links at the top of a displayed report, you can change the report, send the report data by email, and preserve the data in either online or printed format.

## Creating sections on a portal page

The first step in displaying reports on a reports portal page is to create a section on the page to contain the reports.

---

**Note:** You must save a report before you create a new section on a portal page.

---

#### To create a new section on a portal page

- 1 Click the Reports tab.
- 2 On the My Tools list (in the task pane), click **Customize My Portal**.
- 3 Click **Create**.
- 4 On the Create Section page, in the Name text box, type the name of a new section.
- 5 In the Available Reports list box, select a report, click the right arrow button. The selected report is moved to the Selected Reports list box.  
  
Repeat this step for each report you want to include.
- 6 In the Selected Reports list box, use the up and down arrow buttons to move reports up and down in the list.
- 7 Click **Save**.

## Editing sections on a portal page

You can edit the sections on a portal page by renaming them and by adding and deleting reports.

#### To edit a section on a portal page

- 1 Click the Reports tab.
- 2 On the report portal page, click the **Edit** link corresponding to the section to be edited.
- 3 Change the name of the section by typing a new name in the Name text box.
- 4 Modify the list of reports by removing the existing reports from the Selected Reports list or adding new reports to it, with the help of right and left arrow buttons.  
  
In the Selected Reports list box, use the up and down arrow buttons to move reports up and down in the list.
- 5 Click **Save**.

## Deleting sections on reports' portal page

You can delete sections on a reports portal page. When you delete a section, the reports that appear in the section remain in the folders where you saved them.

#### To delete a section on a report portal page

- 1 Click the Reports tab.
- 2 On the report portal page, select checkbox in front of the section to be deleted and click **Delete**.
- 3 On the confirmation message box, click **OK**.

## Managing the report folders

By default, all your custom reports are saved in the top-level *My Subject Reports* folder for the indicated subject, for example *My Backup Reports*. To better organize your saved reports, you can create additional folders within either the *My Report Type Reports* folders or the main *My Reports* folder.

#### To manage report folders

- 1 Click the Reports tab.
- 2 From the My Tools list (in the task pane), select one of the following:
  - Manage My Reports
  - Manage *Report Category Reports*. For example: *My Backup Reports*.

The content pane displays a list of folders you defined either in *My Reports* or in *My Report Category Reports*, depending on what tab you indicated. The list is alphabetically sorted by folder names, but the names of subfolders are concatenated to the names of their parent folders, for example, *parent.child*.

- 3 Create, rename or delete the folder.

#### To create a new folder

- 1 On the My Reports page, click **Create**.
- 2 On the Create Folders dialog box, in the Name text box, type the name of a folder.
- 3 From the drop-down list, select a parent folder for the new folder. *My Reports* is the default folder, indicating the main *My Reports* or *My Report Type Reports* folder.
- 4 Click **Edit**.
- 5 Click **Save**.

#### To rename a folder

- 1 On the My Reports page, click
- 2 On the Rename Folders dialog box, in the Name text box, type the new name of a folder.

- 3 From the drop-down list, select the folder you want to rename.
- 4 Click **Save**.

If the folder is a parent folder, its new name appears in the folder's list for every subfolder.

#### To delete folders

- 1 On the My Reports page, select the check boxes in front of the folder names that you want to delete.
- 2 Click **Delete**.
- 3 On the confirmation message box, click **OK** to confirm the deletion.

Though the folders are deleted, the reports contained by them still exist within the My Reports folder. You can access the reports from the task pane tree view.

## Updating cached reports

When you load a reports portal page for the first time during a session, Veritas Backup Reporter refreshes all reports on the page; that is, the data in each report display is updated. The reports are then cached so that on subsequent page loads they do not refresh.

You can arrange for some or all of your cached reports to be refreshed on a regular schedule.

#### To update cached reports

- 1 On the Settings tab, click **Report Cache Updates**.
- 2 On the Report Cache Updates page, click **Create**.
- 3 On the Create Report Cache Update page, in the Name text box, type a descriptive name for the update.
- 4 Click **Enabled** to activate updates for the selected cached reports.

The reports update at the next scheduled interval. Cancel the selection if you want to turn off updating for the time being.
- 5 From the Schedule drop-down list, select time. This is the schedule on which cached reports are updated.
- 6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

7 From the drop-down list, select one or more reports to update.

8 Click **Save**.

If the update is enabled, cached versions of the indicated reports are automatically updated according to the schedule you specified.

#### To change updates for cached reports

1 On the console Settings tab, click **Report Cache Updates**.

2 In the Report Cache Updates window, click the **Edit** icon next to the name of the cache update.

3 On the Update Report Cache Updates page, change one or more attributes and click **Save**.

## Using default reports

Veritas Backup Reporter provides a number of default / canned reports for backup, archiving, and cost data. Using the Report Wizard, you can manipulate the scope, time frame, and other attributes of these default reports to create reports that display the specific information you want.

---

**Note:** For description about each of the default / canned backup reports, refer to *Veritas Backup Reporter Report Description White Paper* posted at the following location:

<http://support.veritas.com/docs/320685>

---

As you work with different report types, the Report Wizard displays different parameters. Many of the parameters are used for multiple report types, and they appear in different combinations for each type.

---

**Note:** If you find that you need information presented differently than it is presented in the default reports, you can create custom reports. Use the Custom Wizard button in the Report Wizard to open the Custom Report Wizard.

---

The following topics describe the default reports that you can use to display enterprise-specific information:

- Using default reports
- Specifying the scope and time frame of reports
- Customizing an existing report

- Saving data in a report
- About Report Wizard parameters

Before you begin working with the default reports, you should have understanding of the following:

- About report types
- About report formats

## About changes in the default / canned reports UI

Until Veritas Backup Reporter 6.5, when you clicked on a default report, report wizard page was displayed, where you had to select report parameters to generate a report. In VBR 6.5.1 and later versions, when you click on a default report, a report with default parameters is displayed. You do not have to go through the report wizard to view a report. You can edit this report as required.

Instead of a wizard for each chart type of a default report, VBR 6.5.1 and later versions provide a separate link for each chart type. For example, when you expand Job Size folder under Activity Planning report category, following chart type links are made available:

- Historical
- Rankings
- Distribution

Click any of these chart types to view the corresponding default report in the right-hand side pane.

## Loading sample reports

The first time you use Veritas Backup Reporter, after installation, you should load the default reports. After the reports are loaded, they remain available to you indefinitely.

### To load the sample reports

- 1 Click **Reports > My Reports**.
- 2 In the My Tools list (in the task pane), click **Generate Sample Reports**.

The sample reports are categorized as follows:

Operations Dashboard	<ul style="list-style-type: none"><li>■ Error Codes in Last 24 Hours</li><li>■ Backup Size by Server</li><li>■ Size of Backups + Number of Clients</li><li>■ Number of Files by Policy Type</li></ul>
Risk Dashboard	<ul style="list-style-type: none"><li>■ Recovery Point by Client</li><li>■ Least Successful Backups by Servers</li><li>■ Risk Dashboard Daily Success Rate for Last Week</li></ul>
Drive Analysis Dashboard	<ul style="list-style-type: none"><li>■ Drive Utilization for Last Two Weeks</li><li>■ Drive Throughput for Last Two Weeks</li></ul>
Device and Media Dashboard	<ul style="list-style-type: none"><li>■ Status of Media</li><li>■ Volume Pool Media Distribution</li><li>■ Media Retention Level</li><li>■ Storage Type by Week</li></ul>

## Specifying the report scope and time frame

You can use the Report Wizard to create a report that is based on a default report.

### To specify the scope and time frame for a default report

- 1 Select a report subject from the menu bar on the My Reports page (for example, Backups).
- 2 Expand a tree in the task pane, and then click the report subject (for example, Asset - Client Count.).
- 3 If you are prompted, select the report format (for example Stacked Bar), and then click **Continue**.
- 4 In the Report Wizard, define the report's scope by doing the following:
  - From the Within View drop-down list, select an object view category.
  - From the Aggregate at drop-down list, select the view level to be appear the report.
  - If you want to filter the report to include only the data for a particular set of objects (instead of the data for all objects in the view), select the view level of the filtered objects from the Filter drop-down list.
  - If you selected a Filter at value, select one or more objects whose data you want to include in the report in the Select specific items list box.
- 5 Define the report time frame by doing either one of the following:

- Click **Relative Date** to configure a relative time frame. Then from the Show Last drop-down lists, select number of hours, days, months or years. The report displays data collected within the specified time period, for example, data of the last 3 months.
  - Click **Absolute Date** to configure an absolute time frame. In the From drop-down lists, select month, day, year, and start and end time. The report displays data from the time period between the start and end dates.
- 6 Select values for one or more report parameters, depending on the category and type you clicked for your report.
  - 7 Click **Run**.  
Click a hypertext link in the report (such as North America) to view the same report for the next lowest level (such as Canada).
  - 8 To return to the Report Wizard and make changes to the report, click **Edit**.

## Customizing an existing report

You can customize an existing report by modifying the report parameters, which you can save.

---

**Note:** If the report you have selected is generated by running a custom SQL query, when you click the Edit link on the report, the Edit Sql Statement for the Report page appears. You can edit the related SQL query on this page and run the query to view the updated report.

---

### To customize an existing report

- 1 Open a report in the Veritas Backup Reporter console.
- 2 Click **Edit**.
- 3 Modify the report parameters.  
To access additional features for report data, click **Custom Wizard**.
- 4 Click **Run**.

## About Report Wizard parameters

The Report Wizard displays a set of parameters that varies depending on the report type and the report format. The following topics describe each parameter that is available on a report:

- About the Report Grouping parameters  
See [“About the Report Grouping parameters”](#) on page 352.
- About Report Time Frame parameters  
See [“About Report Time Frame parameters”](#) on page 353.
- About Report Time Frame grouping parameters  
See [“About the Report Time Frame Trendline parameter”](#) on page 354.
- About the Report Time Frame Trendline parameter  
See [“About the Report Time Frame Trendline parameter”](#) on page 354.
- About Filter options  
See [“About Filter options”](#) on page 354.
- About Forecast parameters  
See [“About Forecast parameters”](#) on page 355.
- About the Retries Restriction parameter  
See [“About the Retries Restriction parameter”](#) on page 355.
- About the Target Performance parameter  
See [“About the Target Performance parameter”](#) on page 355.
- About the Cost Formula parameter  
See [“About the Cost Formula parameter”](#) on page 355.
- About Display Option parameters  
See [“About Display Option parameters”](#) on page 355.
- About the Define Viewable Columns parameter  
See [“About the Define Viewable Columns parameter”](#) on page 356.
- Defining Exception Condition parameters  
See [“Defining Exception Condition parameters”](#) on page 356.

### About the Report Grouping parameters

Use the Report on parameters to define the report scope.

You can select up to four different values:

Report on	Select report grouping attribute from the drop-down list, which you want to view reports for. For example: Views, Backup Job Attributes, or Backup Image Attributes
Within view	Select a view. The report displays data for objects in the selected view.
Aggregate at	<p>Select the level at which to group data in the report. This setting determines the way data is grouped and labeled in the report.</p> <p>For example, when reporting on the client count view, you can aggregate data at the top level and the report displays data for all servers as a single unit. If you aggregate data at the client level, the report displays data for each client individually.</p> <p><b>Note:</b> The Aggregate at field is not available for some report types that only display data at the Top level of the object view.</p>
Filter at	Select one or more objects within the specified view to limit the amount of data that is collected for the report. Data is collected only for the specified object type.
Select specific item(s)	<p>You can further limit the amount of data collected by selecting individual objects within the filtered scope, such as file systems on a host. Objects in this list may be “real” objects such as hosts and file systems, or they may be user-created nodes in the view, depending on the view level at which you set the filter.</p> <p>For example, when reporting on the Client Count view, you can filter the report at the Client level and select individual clients to include in the report. This does not mean that the clients appear individually in the report (your selection in the Aggregate at field determines that); it means that only data from those clients is included in the report.</p> <p><b>Note:</b> After you select a Report On parameter, wait for the console screen to refresh before clicking additional parameters.</p>

## About Report Time Frame parameters

Use the Report Time Frame parameters to define the beginning and end of the time interval to be covered by the report. You can choose either absolute dates (for example, March 1 to April 1) or relative dates (for example, the last 3 months).

If you plan to save reports for later viewing or for scheduled distribution by email, it is best to choose a relative time frame so that the report always represents the most recent data relative to the time the report is accessed or emailed.

It is best to configure trending and forecast reports with absolute time frames. If you chose a relative time frame, such as “the last 6 months,” the database would

probably contain incomplete data for the present month, and the last bar in the graph would be shorter as a result. This would skew trend lines and forecast lines downward, giving a false result. If you decide to use a relative time frame, choose a granular time period such as hours or days to minimize the skew.

## About Report Time Frame grouping parameters

You use the Report Time Frame Grouping parameters to display and filter report data.

### To display data in the Report Time Frame Grouping

- ◆ Use the drop-down lists in Report Time Frame Grouping to select the unit of time (hours, days, weeks, months or years) in which the report displays its data.

For example, if you want your report to show long-range usage statistics for all NetBackup clients, you might select 1 Month or 3 Months. The report data is grouped by 1-month or 3-month intervals.

As another example, to display statistics for a single client over the most recent week, you could select 1 Day to see day-by-day information for the client.

## About the Report Time Frame Trendline parameter

Use the Report Time Frame Trendline parameter to specify whether the report should include a trendline, and the length of the interval between points on the trend line (in days).

## About Filter options

Filter options enable you to narrow the scope of your report beyond the selections you made in using the Report On parameters. For example, you can filter a backup report to include data for full backup jobs, incremental jobs, or all jobs.

For some report types, you can use drop-downs in the Report Wizard window to click filter options. For example, the Backup Level Filter option specifies the type of backup job level (full backup, incremental backup, or both) that the report should include in its data. Attempt Status specifies whether to display data for backup jobs or attempts.

Expand Show Advanced Filters at the bottom of the window to click additional filtering criteria for the report display. The list of available criteria depends on the report format and type.

For disk-based data protection reports, you have new advanced filters, such as disk pool name, disk pool master server, or disk pool status.

## About Forecast parameters

You can use Forecast Parameters to select the length of a report's forecast line in periods. The length of a period is determined by the Report Time Frame Grouping parameter. If this parameter is set to group data by month, for example, you can specify six forecast periods to generate a 6-month forecast line.

## About the Retries Restriction parameter

You can use the Retries Restriction parameter to specify whether the jobs counted for the report should include only the last tried job or all tries for a given backup host.

## About the Target Performance parameter

You can use the Target Performance parameter to click where a report draws the target line, to which you compare the actual performance shown.

## About the Cost Formula parameter

You can use the Cost Formula parameter, (applicable only for cost reports) to click the cost formula you want to use to calculate chargeback costs for the report.

## About Display Option parameters

You can use the following Display Options parameters to control the way data is labeled in the report display:

- Use the Display Unit parameter to select the size units for reports that display quantities of storage capacity. You can choose from KB, MB, GB, and TB.
- For rankings reports, use the Display Top Rankings parameters to click the number of items to display in the ranking, and the order in which to display them.  
Examples: 5 Descending, 10 Ascending
- Use the Alias X-Axis Name and Alias Y-Axis Name parameters to provide labels for the axes in a bar chart, distribution, or trending report. If you leave these fields blank, default labels are provided.
- Use the Report Description field to provide an optional text description. This is useful when you plan to distribute the report by email. A default description is provided for almost all reports.
- Use the Table Rows Per Page drop-down list to specify how many rows display in each page of a tabular report.

## About the Define Viewable Columns parameter

You can use the Define Viewable Columns parameter to click the columns that display in a tabular report. In the Available Columns list box, click a column you want to include in the tabular report and then click the right single-arrow button to move the column to the Selected Columns list box. You can also move all columns from one box to the other simultaneously using the double-arrow buttons. To configure the order of report columns, in the Selected Columns list box, click a column and then click the up or down arrow to move its position in the list. The first column in the list appears on the left end of the report while the last column appears on the right end.

## Defining Exception Condition parameters

In the Exception Conditions section of the Report Wizard window, specify exception conditions for notification. Exception conditions represent potential problems, for example an unusually high percentage of backup job failures or an unusually low quantity of data being backed up.

Each exception condition is defined by assigning threshold values for a particular metric, such as Success Rate or Total Backup Job Size. You can set a low threshold, a high threshold, or both.

After you specify your conditions, you can configure Veritas Backup Reporter so that when a condition is true, an alert is triggered or an email notification is sent, or both.

As an example, you can define a backup report with the following conditions:

- **Success Rate: Low threshold 80%**  
The condition is met whenever the success rate falls below 80 percent.
- **Total Backup Job Size: Low threshold 500 GB, high threshold 1000 GB**  
The condition is met whenever the total quantity of backed-up data falls outside the range of 500-1000 GB.

### To define report conditions

- 1 In the Add Condition To field, select a metric, and then click **Go**.
- 2 Set threshold values for the metric using the following fields:

Scale	If applicable, select the scale in which to measure, for example a storage size (like GB) or a time period (like days).  The label on this field corresponds to the metric you selected in step 1.
Low Threshold	Specify the low threshold. When a measurement falls below this value, the condition is met.
High Threshold	Specify the high threshold. When a measurement exceeds this value, the condition is met.  <b>Warning:</b> Avoid setting ranges (in other words, both low and high threshold values) for measurements that might return non-numeric data.
Invert	Switch the Low Threshold and High Threshold values.

- 3 Repeat steps 1-2 to create additional conditions.  
To delete a condition, select **Delete**.

## Generating backup reports

This section provides information on generating a number of backup reports

---

**Note:** For description about each of the default / canned backup reports, refer to *Veritas Backup Reporter Report Description White Paper* posted at the following location:

<http://support.veritas.com/docs/320685>

---

## Generating Client Risk Analysis report

The Client Risk Analysis report displays backup clients that are at risk. The following details about the clients that are at risk are displayed on the report:

---

**Note:** You get accurate report output when you generate this report against NetBackup data. This is because these reports are designed mainly for NetBackup.

---

- Client Name
- Master Server Name
- Policy Name
- Last Successful Backup
- Last Full Job Run
- Last Incremental Job Run

**To generate the Client Risk Analysis report**

- 1 In the Veritas Backup Reporter console, click **Reports > Backups > Risk Analysis > Client Risk Analysis**.
- 2 On the report wizard, select the following parameters:

- |                   |  |
|-------------------|--|
| Report Grouping   | Select a view from the Within View drop-down list.   |
| Report Time Frame | Select number of months or number of days. For example, if you selected 1 month, the report shows all clients that were not backed up since a month.   |
| Display Options   | Type report description.<br>Select number of rows you want to be displayed on a single page.<br>Select job status, such as Success or Partial Success.<br>Select True or False from the Host is Active drop-down list. If you select True, the report shows all clients which are active and being backed up.<br>Select backup level, Full, Incremental, or All.<br>Select a master server to specifically check if that master server is at risk. |

- 3 Click **Run**.

## About Advanced Success Rate reports

Advanced Success Rate reports reside in the Advanced Success Rate report category in the Backup reports section. Success Rate reports are described as follows:

- Success Rate - Line This report is a graphical representation of the success rates of master servers.

Summary Dashboard	This is a tabular report that displays summary of job status of master servers.
Detailed Report (Failed Jobs)	A tabular report that displays details of jobs that have failed.
Consecutive Failures	A tabular report that displays jobs that have consecutively failed for number of times, for example, 1, 5, or 10.

In addition to Report Grouping, Report Time frame, and Report Time Frame Grouping filters, the following set of filters is provided on all success rate reports, which are specific to this report category:

**Metric Type** Select a metric type for example, client or job. For example, if you select client as a metric type, the success rate of a master server is calculated on the number of clients that were successfully backed up.

**Aggregation Level** Select any of the following aggregation level:

- **First Job Success Rate** - Select this option to view the success rate of a master server depending on the number of jobs that were successful at their first attempts.
- **All Job Success Rate** - Select this option to view the success rate of a master server depending on the number of jobs that were successful.
- **Last Job Success Rate** - Select this option to view the success rate of a master server depending on the number of jobs that were successful at their last attempts.

The success rate of a master server may differ depending on the metric type you have selected. Consider the following example:

Metric Type: Client

Aggregation Level: First Job Success Rate

Number of clients for the selected master server: 2

Number of jobs run for client 1: 6, number of jobs successful at the first attempt: 6

Number of jobs run for client 2: 4, number of jobs successful at the first attempt: 0

The success rate of the master server is = Number of clients that ran all jobs successfully at the first attempt / Number of clients = 1 / 2

The success rate of the master server is = 50 %

**Increment days** Select a day when you want to schedule a recurring incremental backup.

Increment Window Parameters	Select a time when you want to start incremental backup on the specified day and number of hours for which you want to run the backup.
Full days	Select a day when you want to schedule a recurring full backup.
Full Window Parameters	Select a time when you want to start full backup on the specified day and number of hours for which you want to run the backup.

## About Drive Analysis reports

Drive Analysis reports reside in the Drive Analysis report category in the Backup reports section. Drive Analysis reports are described as follows:

Drive Throughput - Line Shows average throughputs for all drives.

Drive Queue Time - Line Shows queue time for drives.

Drive Utilization - Line Show average utilization of drives. This is the time for which the drive is in use.

## About viewing Drive Utilization and Drive Throughput reports in a heat chart format

In Veritas Backup Reporter, you can view Drive Utilization - Line and Drive Throughput - Line reports using the line chart. However in a large environment with dozens of drives, it becomes difficult to interpret these reports using the line chart.

In Veritas Backup Reporter, you can view the following reports in a heat chart format:

- Drive Utilization
- Drive Throughput

Heat charts are an efficient and intuitive means of displaying many data points. Heat charts are a color-coded representation of the data values contained in a data set. The different color codes let you quickly interpret and analyze the heat chart.

**Note:** In case you have saved Drive Utilization - Line and Drive Throughput - Line reports in earlier releases and upgraded to VBR 6.6, these reports automatically open in a heat chart format after the upgrade.

## About the Drive Utilization report

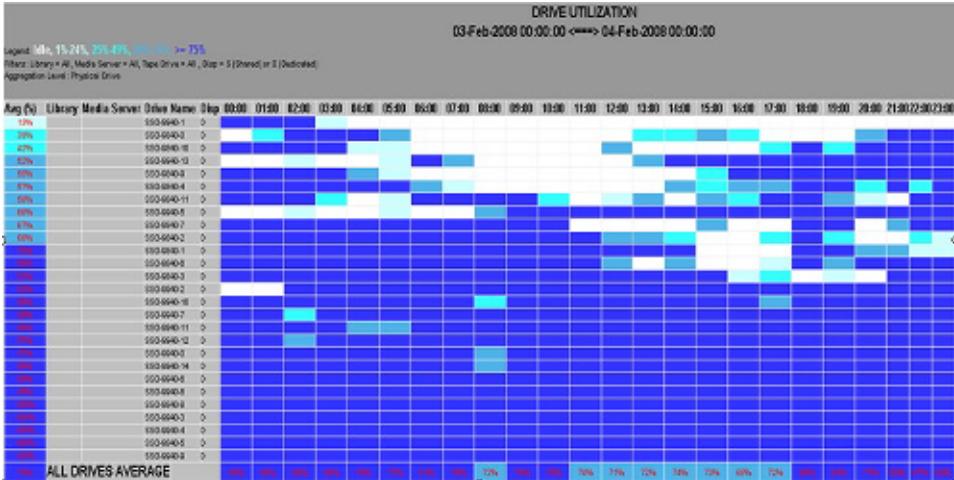
The Drive Utilization report shows the drive utilization across your environment by hour of the day as well as day of the week. The report decomposes actual usage data to determine usage and not a simple polling to detect if the drive is in use. Averages are weighed to ensure a balanced and accurate representation.

The Heat chart format lets you quickly identify the drives that are idle/underutilized. The heat charts can also show the average drive utilization for drives associated with specific media servers or specific tape libraries.

These reports can help you make decisions, help increase drive utilization, and put off unnecessary purchase of new drives.

Figure 9-1 shows a sample report view.

Figure 9-1 Drive Utilization report



The Legend (displayed at the top of the report on the left corner) shows what the different colors in the heat chart stand for. For example in this report, white color means that the drive is idle while dark blue color means that the drive utilization is  $\geq 75\%$ . The other colors depict intermediate ranges of drive utilization. You can set the range for each color code as per your preference. The colors shown in the report are variations of blue and cannot be customized. This report also shows the average drive utilization in your environment. The value in the last cell of

Avg (Kb/sec) column (left of ALL DRIVES AVERAGE) is the average drive utilization in your environment. For example, the average drive utilization in Figure 1-1 is 78%.

---

**Note:** To know the average drive utilization in your environment, run this report across all the drives (aggregated at Tape Drive level) for a sufficiently long time period (say a month to smooth out any fluctuations).

---

See [“Customizing the Drive Utilization or Drive Throughput report”](#) on page 364. to know more about how to set the parameters.

The report also shows the different filter parameters that are set. These parameters are listed just below the Legend.

See [“Customizing the Drive Utilization or Drive Throughput report”](#) on page 364.

---

**Note:** The Disp column shown in the report can take either of the two values - S (Shared) or D (Dedicated). S or Shared means that the drive is shared between two or more media servers. D or Dedicated means that the drive is associated only with one media server.

---

## About the Drive Throughput report

The Drive Throughput report describes the performance of the drives in units of KiloBytes/second. The Heat chart format allows you to quickly identify drives that are not performing well.

The heat charts can also show you the drive throughput for drives associated with specific media servers or specific tape libraries.

[Figure 9-2](#) shows a sample report view.



The report also shows the different filters/parameters that have been set. These parameters are listed just below the Legend.

---

**Note:** The Disp column shown in the report can take either of the two values - S (Shared) or D (Dedicated). S or Shared means that the drive is shared between two or more media servers. D or Dedicated means that the drive is associated only with one media server.

---

## Running the Drive Utilization or Drive Throughput report

Use the following procedure to run the Drive Utilization and Drive Throughput report.

### To run the Drive Utilization or Drive Throughput report

- 1 Click **Reports > Backups** in the Veritas Backup Reporter console.
- 2 Click **Tape Devices** in the Reports pane.
- 3 Click one of the following reports:
  - Drive Utilization
  - Drive Throughput
- 4 After running the report, you can edit, email, or print the report using the links displayed at the top of the report. You can also save the report using the Save As link.

Detailed procedure for editing and customizing these reports is listed.

See [“Customizing the Drive Utilization or Drive Throughput report”](#) on page 364.

## Customizing the Drive Utilization or Drive Throughput report

Use the following procedure to customize the Drive Utilization or Drive Throughput report.

---

**Note:** This procedure must be followed after running these reports.

---

### To customize and run the Drive Utilization or Drive Throughput report

- 1 Click **Edit** to customize the report.
- 2 On the Report Wizard, modify the following report parameters:

Report Time Frame	<p>Define the report time frame by doing either of the following:</p> <ul style="list-style-type: none"><li>■ Click <b>Relative Date</b> to configure a relative time frame. From the Show Last drop-down list, select number of days or months. The report displays data collected within the specified time period, for example, data of the last 3 months.</li><li>■ Click <b>Absolute Date</b> to configure an absolute time frame. In the From drop-down lists, select month, day, year, start and end time. The report displays data from the time period between the start and end dates.</li></ul> <p><b>Note:</b> Always select timeframes in which data collection is valid and current.</p>
Report Time Frame Grouping	<p>Select the time interval by which you want to group the records. This can have the following values:</p> <ul style="list-style-type: none"><li>■ Hours of the day (Average)</li><li>■ Days of the Week For example, if you select Hours of the day (Average), the report shows 24 columns with records grouped by each hour.</li></ul>
Display Options	<p>Display options let you control how the report looks.</p>
Color code ranges	<p>Specify three numerals in ascending order in the three fields. These numerals are automatically translated into ranges. Each range is associated with a specific color code.</p> <p>For the Drive Utilization reports, specify three numerals (in ascending order) that fall between 0 - 100%.</p> <p>For example if you type 10, 50, 75 as the color code ranges, it translates into the following ranges: 0% (Idle), 1%-9%, 10%-49%, 50%-74%, &gt;= 75%</p> <p>For the Drive Throughput report, you can specify three throughput values (KB/sec) in ascending order.</p> <p>For example if you type 5000, 10000, 20000, it translates into the following ranges:</p> <p>0 (Idle), 1 - 4999, 5000 - 9999, 10000 - 19999, &gt;= 20000 KB/sec.</p> <p><b>Note:</b> The values entered as color code ranges must be numeric and must be in ascending order. This applies to both Drive Utilization and Drive Throughput reports.</p>

Aggregation Level	<p>Select the level at which to group data in the report. This setting determines the way data is grouped and labeled in the report.</p> <ul style="list-style-type: none"><li>■ Select <b>Default</b> to aggregate data at the logical drive level. A drive may be configured across media servers and libraries in many different ways. When you aggregate at the Default level, each logical drive is represented by a single row in the report.</li><li>■ Select <b>Media Server</b> to aggregate data at the media server level. There is one row for each media server in the report.</li><li>■ Select <b>Tape Library</b> to aggregate data at the library level. There is one row for each tape library in the report.</li><li>■ Select <b>Tape Drive</b> to aggregate data at the physical drive level. There is one row for each physical drive in the report.</li><li>■ Select <b>Drive Type</b> to aggregate data on the basis of drive type (like SDLT, DLT, LTO etc.). There is one row for each drive type.</li></ul>
Sort order	<p>You can define the sort order for the columns. This can take three values - Default, Ascending, or Descending.</p> <ul style="list-style-type: none"><li>■ Select <b>Default</b> to sort the contents of Library/Media Server/Tape Drive columns in alphabetical order.</li><li>■ Select <b>Descending</b> to sort the content of Avg (%)/Avg (KB/sec) columns in the Drive Utilization/Drive Throughput reports respectively in descending order.</li><li>■ Select <b>Ascending</b> to sort the content of Avg (%)/Avg (KB/sec) columns in the Drive Utilization/Drive Throughput reports respectively in ascending order.</li></ul>
Report Description	<p>Enter a description for the report.</p>
Filter Options	<p>Filter options allow you to select or limit data that is collected by the report. Data is collected only for the specified objects.</p>
Media Server	<p>Select one or more media servers from the drop-down list box. The report shows data only for the specific media servers.</p>
Tape Library ID	<p>Select one or more Tape Library ID's from the drop-down list box. The report shows data only for the specific tape libraries.</p>
Drive Name	<p>Select one or more drives from the drop-down list box. The report shows data only for the specific drives.</p>

Backup Level	You can specify one of the following values for Backup Level: <ul style="list-style-type: none"><li>■ All - The report shows data for all backup levels</li><li>■ Full - The report shows data only for Full backup level</li><li>■ Incremental - The report shows data only for Incremental backup level</li></ul>
Job Type	Specify a job type from the drop-down list. The report shows data only for the specific job type.
Backup Job Policy	Select one or more backup job policies from the drop-down list box. The report shows data only for specific backup job policies.

---

**Note:** The Aggregation Level is controlled by the Tape Library ID, Media Server and Drive Name filter options. For example, if you select a Tape Library ID from Filter Options and also set Aggregation Level to Tape Library, the report shows only one row (for the selected Tape Library). If no filters are selected for Tape Library ID, Media Server and Drive Name, and you set the Aggregation Level to Tape Library, the report shows one row for each library from which data is being collected.

---

### 3 Click **Run**.

## About Capacity Planning reports

Capacity Planning reports help you manage your tape media inventory by helping you to determine the optimal number of tapes in accordance to your needs. With these reports, you can avoid situations like shortage of tapes or delay in backups. These reports allow you to compare the supply and demand in your environment and also forecast the supply and demand in the near future. This helps you to decide how many tapes need to be bought and when you should buy them.

---

**Note:** Tapes that are full are not taken into account while generating Capacity Planning reports.

---

Veritas Backup Reporter provides the following Capacity Planning reports:

- Historical Size
- Forecasted Size

---

**Note:** The Capacity Planning reports show only NetBackup data. They do not contain data collected from other backup products such as, Backup Exec or Tivoli Storage Manager.

---

## About Historical Size reports

This report lets you compare the available space on tapes (supply) and amount of data to be written on tapes (demand) in your environment.

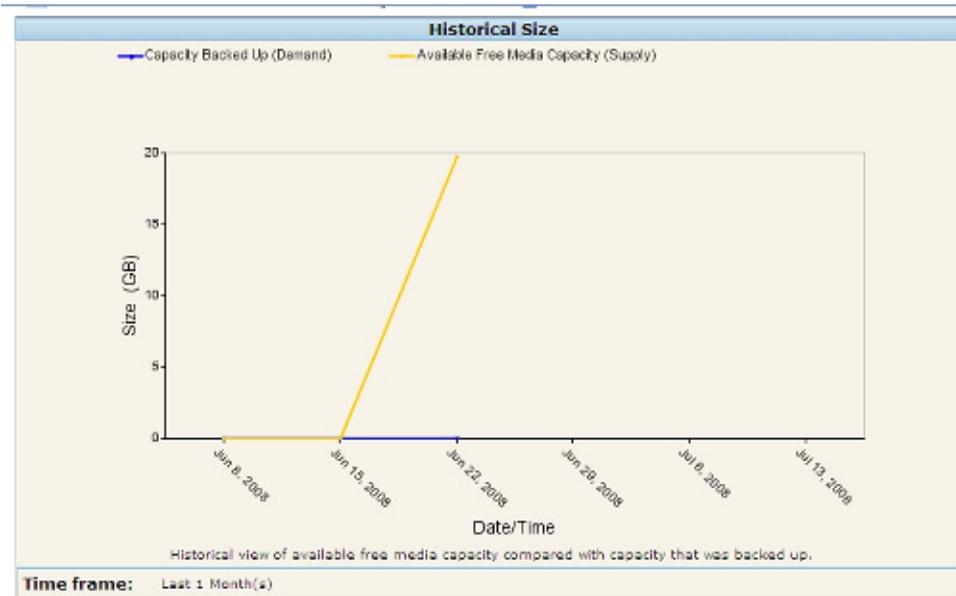
Supply = Total Capacity of Tapes - Used Space

Demand is the sum total of all backup image fragment sizes stored on the tape. This includes all data written to tapes including duplicate copies and data that was initially staged to disk and now moved to tape.

The report shows two trendlines out of which one represents supply and the other represents demand. If supply is greater than the demand, then the gap between the two trendlines shows unused capacity of the tapes in your environment. If demand is greater than supply, then you must increase the number of tapes in your environment.

Figure 9-3 shows a sample report view.

**Figure 9-3** Historical Size report



## About Forecasted Size reports

This report forecasts about available space on tapes (supply) and amount of data to be written on tapes (demand).

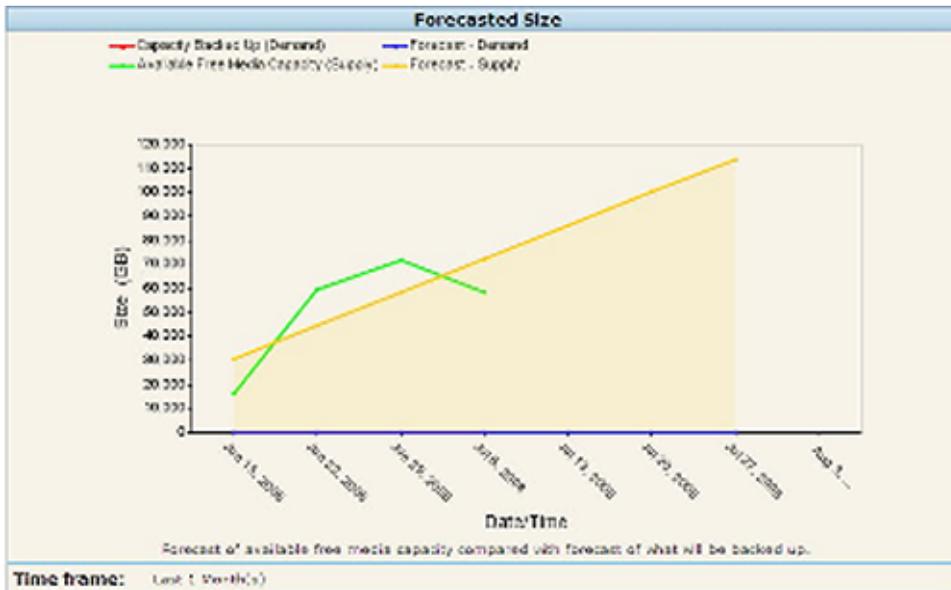
The report shows four trendlines - one represents supply and the other represents demand (same as Historical Size report). In addition, there are two forecast lines, one for demand and one for supply. The forecasting is based on a linear regression formula.

By using this report, you can predict when the demand is going to exceed the supply. If the supply is greater than the demand, and you see the two forecast lines intersecting at a future date, it implies that the demand will exceed the supply on this date, which means you will need more tapes on this date.

If forecasted supply is greater than the forecasted demand as shown in the following figure, the extra media can be put to some other use.

Figure 9-4 shows a sample report view.

Figure 9-4 Forecasted Size report



## About running Capacity Planning reports for the first time

After installing Veritas Backup Reporter and configuring data collector for NetBackup data collection for the first time, media data collection must happen successfully at least twice before you run Capacity Planning reports.

---

**Note:** The following procedure must be followed if you install Veritas Backup Reporter for the first time and then configure NetBackup data collector also for the first time. In setups where NetBackup data collector was already collecting media data and was upgraded to a new VBR version, you can run Capacity Planning reports immediately. This is because multiple media data collection events would have happened successfully already.

---

The first media data collection happens immediately after configuring the data collector (with Media event enabled). The second successful media data collection can be achieved by doing either of the following:

- Media data is collected for the second time when the media event runs after the collection interval. The media data collection interval can be specified while configuring the data collector. Thus you must run Capacity Planning reports only after the specified media data collection interval.
- Force poll media event to collect media data for the second time. Thus after collecting media data by force poll method, you can run Capacity Planning reports.

See [“Collecting data by the force poll method”](#) on page 196.

See [“Running the Capacity Planning reports”](#) on page 370.

## Running the Capacity Planning reports

Use the following procedure to run the Historical Size and Forecasted Size report.

---

**Note:** Also review Known Issues before running Capacity Planning reports.

---

### To run Capacity Planning reports

- 1 Click **Reports > Backups** in the Veritas Backup Reporter console.
- 2 Expand Activity Planning in the Reports pane and click **Capacity Planning**.
- 3 Click any of the Capacity Planning reports:
  - Historical Size
  - Forecasted Size
- 4 After running the report, you can edit, email, or print the report using the links displayed at the top of the report. You can also view the report data in a tabular format or export the report in a CSV (comma separated value), TSV (tab separated value), or an XML format. You can also save the report using the Save As link.

## Customizing the Capacity Planning reports

Use the following procedure to customize the Capacity Planning reports.

---

**Note:** This procedure must be followed after running these reports.

---

### To customize and run the Capacity Planning reports

- 1 Click **Edit** to customize the report.
- 2 On the Report Wizard, modify the following report parameters:

Report Time Frame	<p>Define the report time frame by doing either of the following:</p> <ul style="list-style-type: none"><li>■ Click <b>Relative Date</b> to configure a relative time frame. From the Show Last drop-down list, select number of days or months. The report displays data collected within the specified time period, for example, data of the last 3 months. The default time frame for the Inventory Management reports is Last 1 month.</li><li>■ Click <b>Absolute Date</b> to configure an absolute time frame. In the From drop-down lists, select month, day, year, start and end time. The report displays data from the time period between the start and end dates.</li></ul> <p><b>Note:</b> Always select timeframes in which data collection is valid and current.</p>
Report Time Frame Grouping	<p>Select the time interval by which you want to group the records. This can have the following values:</p> <ul style="list-style-type: none"><li>■ Hours of the day (Average)</li><li>■ Days of the Week For example, if you select Hours of the day (Average), the report shows 24 columns with records grouped by each hour.</li></ul> <p><b>Note:</b> The default time frame grouping period is 1 week.</p>
Display Options	<p>Display options let you control how the report looks.</p>
Display Unit	<p>Use the Display Unit parameter to select the size units. You can choose from KB, MB, GB, and TB.</p> <p>The default unit for the Inventory Management reports is MB.</p>
Alias X-Axis Name	<p>Use the Alias X-Axis Name parameter to provide a label for the X-axis. The default label is Date.</p>

Alias Y-Axis Name	Use the Alias Y-Axis Name parameter to provide a label for the Y-axis. The default label is Size.
Report Description	Enter a description for the report.
Forecast Parameters	Forecast parameters allow you to define the forecast.
Number of forecast periods	<p>You can select a forecast period from the available options.</p> <p>If you are generating the report from say June 2'nd to June 5'th and the Group By parameter is hours, selecting 1 as the forecast period means you will see the forecast 1 hour from the end date and time.</p> <p>In a similar way, if you are generating a report on June 9'th, 2008 for the last 1 month grouped by 1 month and the number of forecast periods is 1, then you will see the forecast 1 month from June 9'th (means till July 9'th).</p>
Filter Options	<p>Filter options allow you to select or limit data that is collected by the report.</p> <p><b>Note:</b> All filters are applied on supply value. Data is collected only for the specified objects.</p>
Backup Media Role	Select a Backup Media Role from the drop-down list.
Backup Media Type	Select a media type (like SDLT, DLT etc.) from the drop-down list.
Backup Media Volume Pool Name	Select the volume pool name from the available options.
Backup Media Volume/EMM Database server	Select an option from the drop-down list.
Backup Media Product	Select a Backup media product from the available options.
Backup Media Agent Server	Select the backup media agent server from the available options.
Tape Library Manufacturer	Select a tape library manufacturer from the available options.
Tape Library Serial Number	Select a tape library serial number from the available options.

**3** Click **Run**.

## About Media reports

Media reports is a new report category that contains some useful media-related reports. All media reports can also be generated from the Custom category by selecting appropriate parameters. Having these reports under the Media report category makes them easily accessible from the Veritas Backup Reporter console.

You can analyze the media reports to plan your backup environment in a better way.

The Media reports are as follows:

- [About Tape Count reports](#) Tape Count report
- [About Tape Used Capacity by Retention Level reports](#) Tape Used Capacity by Retention Level report
- [About Tapes Expiring Now reports](#) Tapes Expiring Now report
- [About Tapes Expiring in next 7 days reports](#) Tapes Expiring in the next 7 days report

## About Tape Count reports

The Tape Count report folder contains the following reports:

- Tape Count Distribution by Volume Pool
- Tape Count Trends by Volume Pool
- Tape Count Distribution by Tape Type
- Tape Count Distribution by Retention Level
- Tape Count Trends by Retention Level

---

**Note:** Both, Tape Count Distribution by Volume Pool and Tape Count Trends by Volume Pool reports show the same data but in different formats. Similarly, Tape Count Distribution by Retention Level and Tape Count Trends by Retention Level reports show the same data but their representation is different.

---

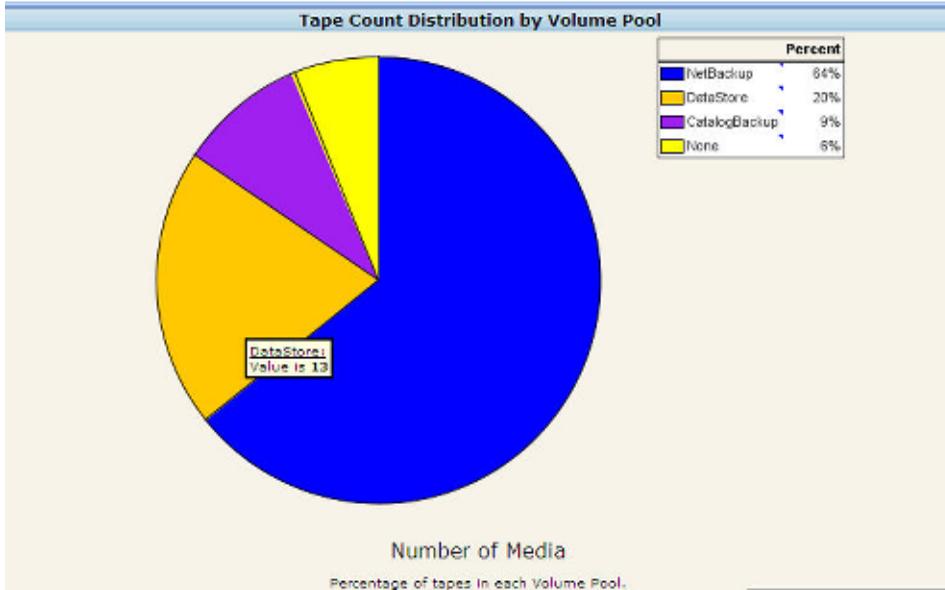
## About Tape Count Distribution by Volume Pool reports

This report shows the number of tapes associated with each volume pool in the form of a pie chart. This lets you identify the volume pools that have maximum or minimum tapes in a glance.

Each volume pool is represented by a specific color. Placing the mouse on each color segment shows the volume pool name and the number of tapes associated with it. The report also lists the tape distribution for each volume pool in percent on the right-hand side.

Figure 9-5 shows a sample report view.

Figure 9-5 Tape Count Distribution by Volume Pool report



### About Tape Count Trends by Volume Pool reports

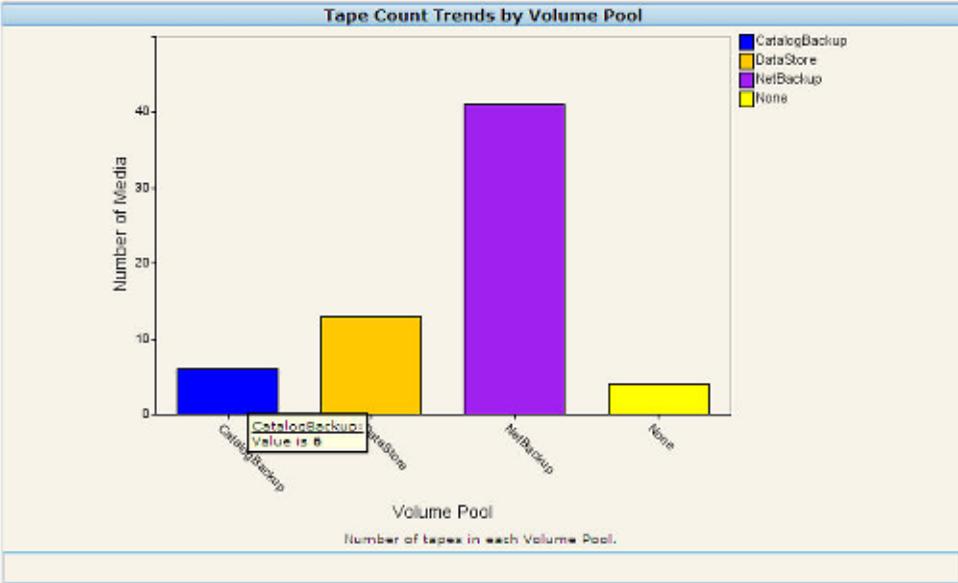
This report shows the number of tapes associated with each volume pool in a trending format. This lets you identify the volume pools that have maximum or minimum tapes in a glance.

Each volume pool is represented by a specific color, which is shown on the right-hand side.

Placing the mouse on each colored bar shows the volume pool and the number of tapes associated with the volume pool.

Figure 9-6 shows a sample report view.

Figure 9-6 Tape Count Trends by Volume Pool report



**About Tape Count Distribution by Tape Type reports**

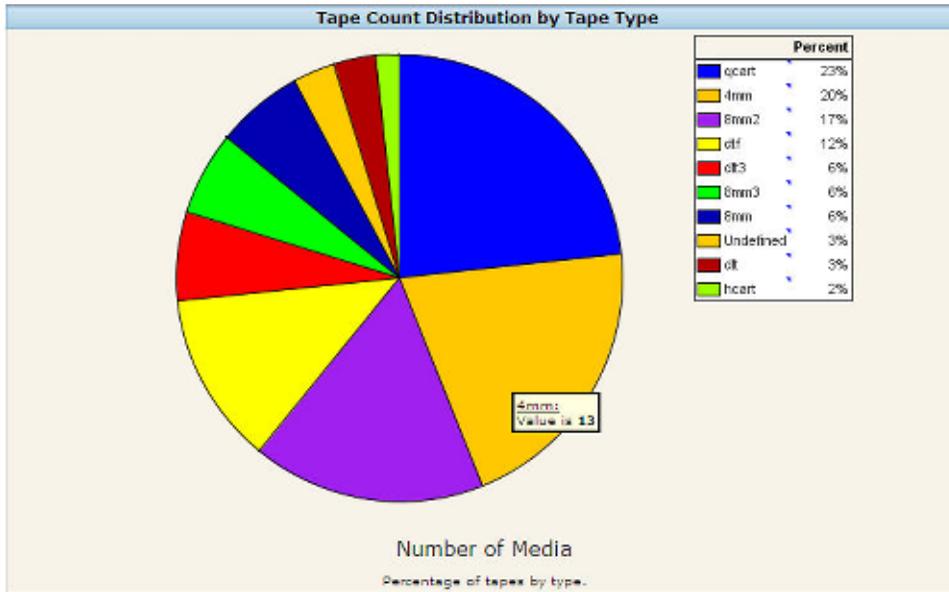
This report lets you track the distribution of different types of tapes in your environment. For example, this report tells you that the number of 4mm tapes in your environment is 13 and number of DLT tapes is 2.

Placing the mouse on each color segment shows the number of tapes associated with each tape type.

The report also lists the tape distribution for each tape type in percent on the right-hand side.

Figure 9-7 shows a sample report view.

**Figure 9-7** Tape Count Distribution by Tape Type report



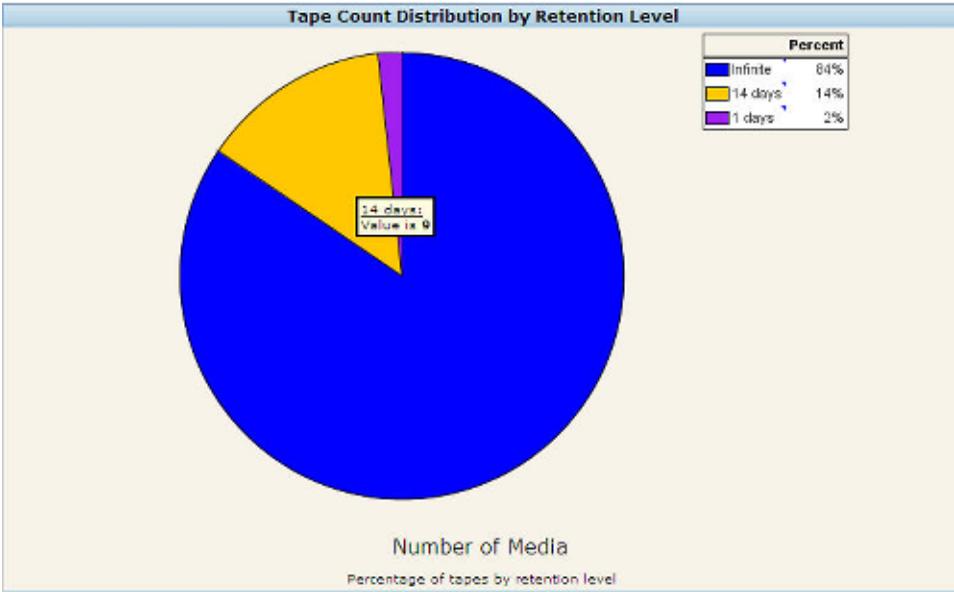
### About Tape Count Distribution by Retention Level reports

This distribution report shows the number of tapes having specific retention levels. Placing the mouse on each color segment shows the number of tapes associated with a specific retention level. For example, this report shows that 54 tapes have an infinite retention level while 9 tapes have a retention level of 14 days.

The report also lists the tape distribution for specific retention level in percent on the right-hand side.

[Figure 9-8](#) shows a sample report view.

**Figure 9-8** Tape Count Distribution by Retention Level report



**About Tape Count Trends by Retention Level reports**

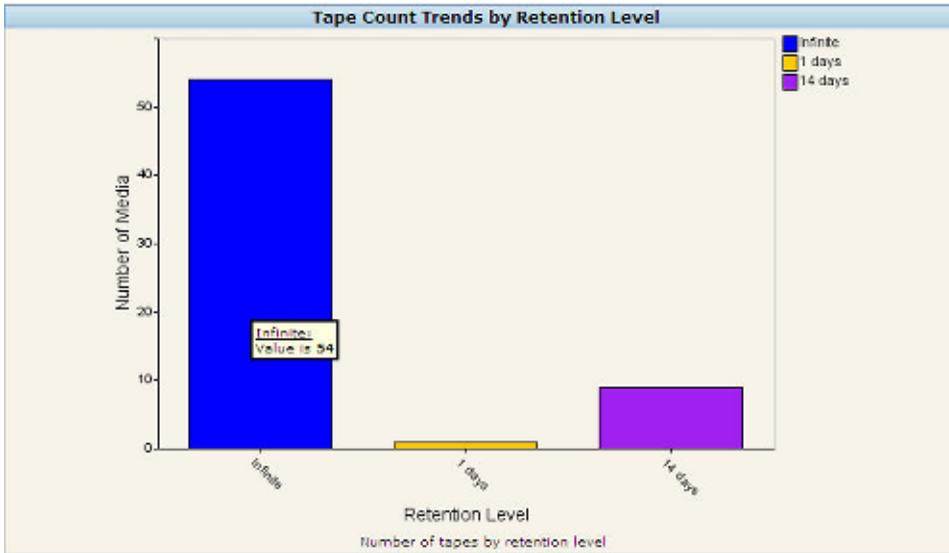
This trending report shows the number of tapes having specific retention levels.

Placing the mouse on each colored bar gives the number of tapes with a specific retention level. For example, this report tells you that 54 tapes in your environment have an infinite retention level while 9 tapes have a retention level of 14 days.

Each retention level is represented by a unique color. This is shown on the right-hand side.

Figure 9-9 shows a sample report view.

**Figure 9-9** Tape Count Trends by Retention Level report



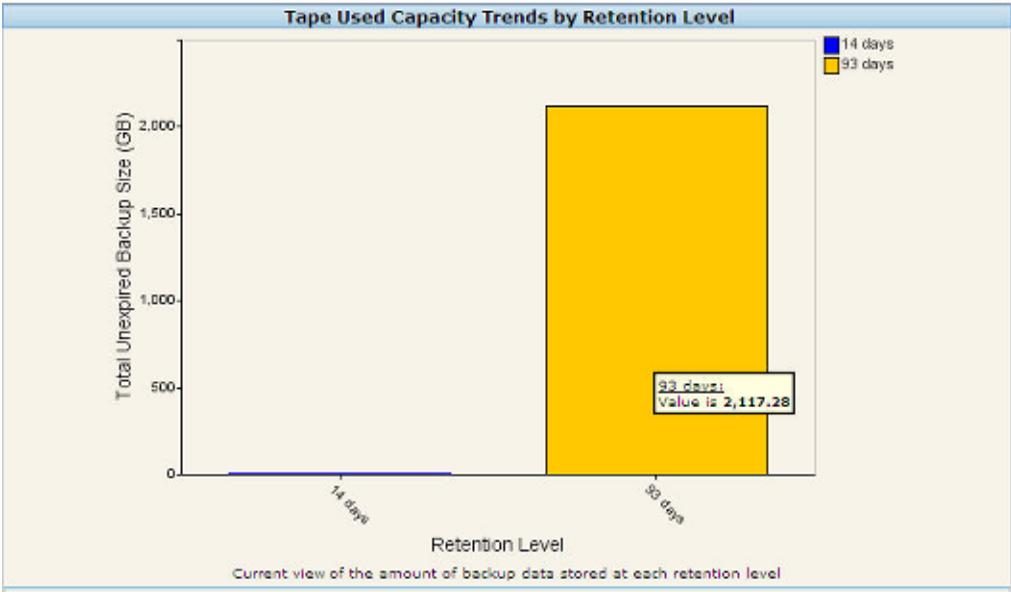
### About Tape Used Capacity by Retention Level reports

This report shows the total tape capacity used by media having specific retention levels. Using this report, you can see the overall tape used capacity trend based on the retention level in your environment.

For example, the report can tell you that a total capacity of around 2117.28 GB is being used by media having a retention level of 93 days.

[Figure 9-10](#) shows a sample report view.

**Figure 9-10** Tape Used Capacity by Retention Level report



**About Tapes Expiring Now reports**

This tabular report shows details for the tapes expiring now. This includes the tapes expiring between 12 a.m. today (the day when you run the report) and 12 a.m. of the next day. This is shown by default.

You can also configure the time frame to see the tapes that are expiring in the near future or tapes that have expired in the past time frame.

Figure 9-11 shows a sample report view.

**Figure 9-11** Tapes Expiring Now report

Tapes Expiring Now				
Volume/EMM Database Server	Volume Pool Name	Media ID	Backup Media Barcode	Backup Media Expiration Time
ocs-nln-qe-7	RetBackup	A00004	0	Jun 25, 2008 13:52:01
ocs-nln-qe-7	RetBackup	A00005	0	Jun 25, 2008 15:52:01
ocs-nln-qe-7	RetBackup	A00006	0	Jun 25, 2008 17:00:01
ocs-nln-qe-7	RetBackup	A00007	0	Jun 25, 2008 23:12:01

4 Total Rows    Pages: [Navigation icons]

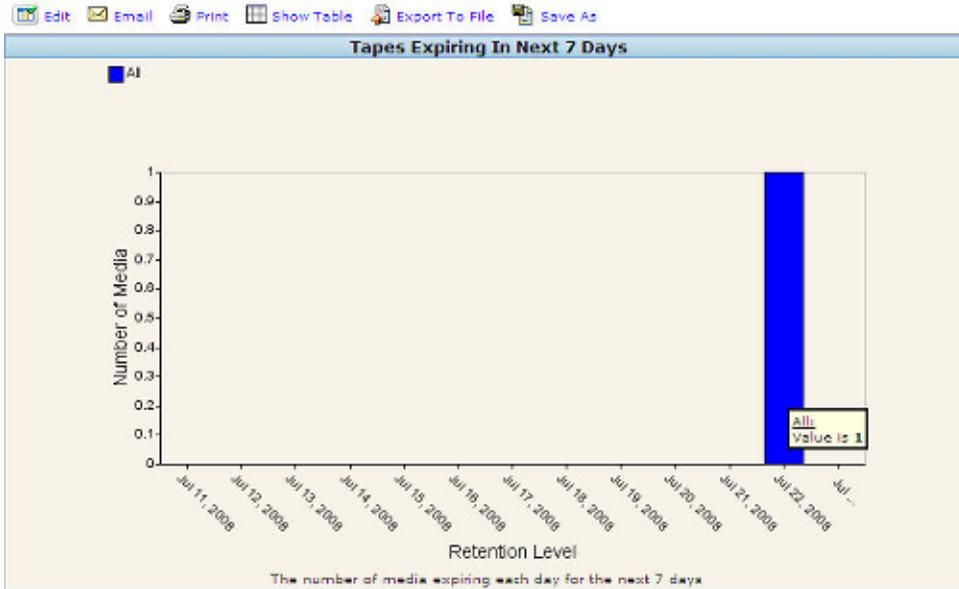
Time frame: Next 1 Day(s)

**About Tapes Expiring in next 7 days reports**

This report shows trends for tapes expiring in the next seven days. It shows the number of tapes expiring on each of the seven days.

Figure 9-12 shows a sample report view.

Figure 9-12 Tapes Expiring in next 7 days report



## Running Media reports

Use the following procedure to run media reports.

### To run Media reports

- 1 Click Reports > Backups in the Veritas Backup Reporter console.
- 2 Expand Media in the Reports pane.
- 3 Click any of the Media reports:
  - Tape Count
  - Tape Used Capacity by Retention Level
  - Tapes Expiring Today
  - Tapes Expiring in the next 7 days

---

**Note:** Click **Tape Count** to run the various reports under the Tape Count report folder.

---

- 4 After running the report, you can edit, email, or print the report using the links displayed at the top of the report. You can also view the report data in a tabular format or export the report in a CSV (comma separated value), TSV (tab separated value), or an XML format. You can also save the report using the Save As link.

Detailed procedure for editing and customizing this report is listed.

See [“Customizing the Media reports”](#) on page 381.

## Customizing the Media reports

Use the following procedure to customize media reports.

---

**Note:** This procedure must be followed after running these reports.

---

### To customize and run the Media reports

- 1 Click **Edit** to customize the report.
- 2 On the Report Wizard, modify the following report parameters: (All these parameters may not be available for all media reports)

Backup Media Expiration Time	<p>Select any of the following:</p> <ul style="list-style-type: none"><li>■ Click <b>Relative Date</b> to configure a relative time frame. In the Day window, you can select a specific time interval using From and To drop-down lists. Select Last/Next, number of hours, days, weeks, months, quarters, or years. The report shows data which lies in the selected time frame. The report displays data collected within the specified time period, for example, tapes expired in the last 3 months. Do not select the To Date check box if you want to view data for the entire period specified. For example: The current date is 13th June 2008. If you selected the period as Last 1 Month and not selected the To Date check box, the report shows data from 14th May 2008 to 13th June 2008. If you selected the To Date check box, the report shows data from 1st June 2008 to 13th June 2008. Select Include Infinite Values if you want to see details of media whose expiration time is set as Infinite Retention. Select Only Infinite Values if you want to see details of media whose expiration time is set as Infinite Retention.</li><li>■ Click <b>Absolute Date</b> to configure an absolute time frame. In the From drop-down lists, select month, day, year, and start and end time. The report displays data from the time period between the start and end dates.</li></ul>
Report Grouping	This option allows you to group records in the report.
Report on	The media reports report on a specific parameter hence there is no need to select any option.
Display Options	Display options let you control how the report looks.
Display Unit	Use this parameter to select the size units. You can choose from KB, MB, GB, and TB.
Alias X-Axis Name	Use this parameter to provide a label for the X-axis.
Alias Y-Axis Name	Use this parameter to provide a label for the Y-axis.
Report Description	Enter a description for the report.
Table rows per page	Select the number of rows/records you want to see on a single page of the report.
Filter Options	Filter options allow you to select or limit data that is collected by the report. Data is collected only for the specified objects.

Backup Level	Select one of the following values for Backup Level: <ul style="list-style-type: none"><li>■ All - The report shows data for all backup levels.</li><li>■ Full - The report shows data only for Full backup level.</li><li>■ Incremental - The report shows data only for Incremental backup level.</li></ul>
Disk Pool Name	Select a disk pool from the drop-down list box.
Backup Media Role	Select a Backup Media Role from the drop-down list box.
Backup Media Type	Select a media type (like SDLT, DLT etc.) from the drop-down list box.
Backup Media Volume Pool ID	Select an ID from the available options.
Backup Media Volume Pool Name	Select the volume pool name from the available options.
Backup Media Status	Select the media status from the available options.
Backup Media Volume/EMM Database server	Select an option from the drop-down list.
Backup Media Product	Select a Backup media product from the available options.
Backup Media Agent Server	Select the backup media agent server from the available options.
Tape Library Manufacturer	Select a tape library manufacturer from the available options.
Tape Library Serial Number	Select a tape library serial number from the available options.

### 3 Click **Run**.

## About the Client Coverage report

The Client Coverage report tells you whether all clients in your environment are being backed up or not. VBR can only report on clients that have already been defined and configured for backups. This report helps you to identify the clients that are a part of your environment but are not known to Veritas Backup Reporter. These clients may not be getting backed up because of backup software not being installed or the clients not being configured for backups.

To run this report, you must specify a CSV file (comma-separated value) that contains a complete and authoritative inventory of all servers across the enterprise.

Some of the independent sources of server inventory across the enterprise which can be used to generate a CSV file are the following:

- Configuration Management Database (CMDB)
- Asset Management System
- Domain Name System (DNS)
- Homegrown databases
- Spreadsheet

See “[About CSV formats](#)” on page 385. for more information.

Veritas Backup Reporter imports data from the CSV file and compares the list of clients (available in CSV) with the clients known to VBR. The clients which are present in CSV but not in VBR can be easily identified from this report.

[Figure 9-13](#) shows a sample report view.

**Figure 9-13** Client Coverage report

Client Coverage				
External Client*	Backed Up Client	Message	Backup Product	Full Policy
pinacolada	PTIACOLADA.vindia.veritas.com	Match - FQDN vs Short Name	Backup Exec	Backup 00004
pinacolada	PTIACOLADA.vindia.veritas.com	Match - FQDN vs Short Name	Backup Exec	Backup 00004
harshap	HARSHAP.vindia.veritas.com	Match - FQDN vs Short Name	Backup Exec	Backup 0000-Duplicate Backup Sets 0000
6dd.vindia.veritas.com		In External List And Not In Backup		
scgqacl2		In External List And Not In Backup		
scs-wing-3.vindia.veritas.com	scs-wing-3.vindia.veritas.com	Match - Direct	Backup Exec	Backup 00010
scs-wing-1	scs-wing-1.VERTS.vindia.veritas.com	Match - FQDN vs Short Name	Backup Exec	Test Backup
scs-wing-33		In External List And Not In Backup		
ASWA.vindia.veritas.com		In External List And Not In Backup		
alb.vindia.veritas.com		In External List And Not In Backup		

**Note:** The CSV file must be located on the machine from where you are running the Client Coverage report.

See “[About comparison of clients listed in CSV and VBR](#)” on page 386. for more information on how the comparison takes place.

The following table provides details on each field of the report:

External Client	Name of the client that appears in the CSV file. <b>Note:</b> A client may be known by multiple names and all the names may be documented in the CSV file. The name that appears in the External Client column is the first name that is documented in the CSV file. For example, if a CSV file lists multiple names for a client such as, myhost, myhost.symantec.com, myhost.veritas.com, then myhost appears in the External Client column.
Backed Up Client	Name of the backed up client in Veritas Backup Reporter.
Message	The result of comparison. The following are the possible messages: <ul style="list-style-type: none"><li>■ Match - Direct</li><li>■ Match - FQDN vs. Short name</li><li>■ In External List And Not In Backup</li></ul> The Client Coverage report helps you to identify these clients which are present in your environment but are not known to Veritas Backup Reporter. You must verify if these clients are being backed up. See <a href="#">“About comparison of clients listed in CSV and VBR”</a> on page 386. for more details.
Backup Product	A list of backup products used for backing up the client, such as, NetBackup, Backup Exec, or Tivoli Storage Manager.
Full Policy	The backup policy associated with the client when the last full backup was successful.
Last Full Job Time	This is the time when the last full backup was successful for the specific client.
Incremental Policy	The backup policy associated with the client when the last incremental backup was successful.
Last Incremental Job Time	This is the time when the last incremental backup was successful for the specific client.

### About CSV formats

The CSV file required as an input to the Client Coverage report can be created using a text editor or Microsoft Excel application.

A typical CSV file format is as follows:

```
Host1_name1,Host1_name2,Host1_name3,Host1_name4
```

```
Host2
```

```
Host3
```

---

**Note:** Host1\_name1,Host1\_name2,Host1\_name3,Host1\_name4 are multiple names of the same machine. Multiple names for the same machine may exist due to many reasons like because of a machine having multiple Network Interface Cards etc.

---

**Note:** Each host machine exists in a new line. For example, Host1, Host2, and Host3 all exist in three separate lines.

---

Here is a sample CSV format:

```
css-bin3,css-bin3.symantec.com
macy.symantec.com,macy,macy.veritas.com
css-bin10.symantec.com
```

---

**Note:** There is no space after the comma in the CSV file.

---

### About comparison of clients listed in CSV and VBR

VBR imports data from the CSV file and compares the list of clients (available in CSV) with the clients known to VBR.

The Client Coverage report shows any or all of the following outcomes after comparison:

Client is in  
External Client  
and Backed Up  
Client list

This means that a client exists in both the CSV file and VBR database.

**Note:** In case multiple names for a machine are present in CSV and VBR, then all the names present in CSV are compared with each name in VBR till a match is obtained.

The comparison results in this case may be one of the following:

- **Match - Direct:** This happens when the host name in CSV is exactly the same as the host name in VBR. For example, myhost.symantec.com in CSV and myhost.symantec.com in VBR.
- **Match - FQDN vs. Short Name:** This happens when the host name is an FQDN in CSV and a short name in VBR or a short name in CSV and an FQDN in VBR. For example, if the CSV file contains myhost.veritas.com and VBR contains myhost, then the comparison result is Match - FQDN vs. Short Name. Similarly, if the CSV file contains myhost and VBR contains myhost.veritas.com, then the comparison result is Match - FQDN vs. Short Name.

In External List  
And Not In Backup

The Client Coverage report helps you to identify these clients which are present in your environment but are not known to VBR. You must verify if these clients are being backed up.

**In Backup And Not In External List** This happens when the host name is known to VBR but not present in the CSV file. This may be due to several reasons like machine not being available in the network or machine not registered in the DNS, and so on.

## Running a Client Coverage report

Use the following procedure to run the client coverage report.

---

**Note:** The Client Coverage report cannot be saved, emailed, printed, or exported.

---

### To run the Client Coverage report

- 1 Click **Reports > Backups** in the Veritas Backup Reporter console.
- 2 Expand Risk Analysis and then click **Client Coverage**.
- 3 On the Report wizard, select the following parameters:

**Report Grouping** You can define the report's scope by doing the following: Select a view from the Within View drop-down list. This can be done to view the report for a specific location, department etc.

If you want to filter the report to include only the data for a particular set of objects (instead of the data for all objects in the view), select the view level of the filtered objects from the Filter at drop-down list.

If you selected a Filter at value, select one or more objects whose data you want to include in the report in the Select specific items list box.

**Note:** In case you select the Report Grouping parameters, you must create the CSV file that contains the clients in the particular view only. For example, if you want to see the Client Coverage report for HR department in Canada, then the CSV file must contain the client list specific to the HR department in Canada.

**External List of Clients** Type the path of the CSV file. You can also browse to the CSV file.

You must specify the CSV file for running the Client Coverage report.

**Note:** The CSV file must be located on the machine from where you run the Client Coverage report.

See "[About CSV formats](#)" on page 385. to know about the CSV format.

**Host Name Wild Card (Optional)** You can specify a part of the backed up client name so that the report shows data only for the specific backed up clients that are of your interest. For example, to see details of all backed up servers running Oracle which are known to have a string "ora" somewhere in the host name, you can type the following:

- %ora% - Include or exclude all backed up clients with 'ora' anywhere in the host name
- ora - Include or exclude all backed up clients named ora.
- ora% - Include or exclude all backed up clients whose names start with ora.
- %ora - Include or exclude all backed up clients whose names end with ora.

Similarly, you can specify multiple search strings as follows:

- %ora%, %syb% - Include or exclude all Veritas Backup Reporter hosts with Ora or Syb anywhere in the backed up client name.

**Note:** This search is applicable only for Backed Up clients and not the External Clients.

**Note:** The search is not case-sensitive. For example, if you search for Ora, you may find results like ora, Ora, oRa, and so on.

**Display Options** Type report description.  
Select the number of rows you want displayed on a single page.

4 Click **Run**.

## Generating recovery reports

You can generate recovery reports through the Backup section.

### To generate a recovery report

- 1 In the Veritas Backup Reporter console, log on to the Veritas Backup Reporter Management Server.
- 2 In the console, click **Reports > Backups**.
- 3 On a report, click **Edit**.
- 4 On the Report Wizard page, in the Filter Options section, from the Job Type drop-down list, select **Restore** to generate a recovery report.
- 5 Select other filter parameters.
- 6 Click **Run**.

## Generating the library capacity forecast report

Veritas Backup Reporter provides the Library Capacity Forecast report that shows the backup trend for future dates depending on maximum tape capacity.

### To generate the Library Capacity Forecast report

- 1 Click **Reports > Backups** in the Veritas Backup Reporter console.
- 2 Click **Tape & Media Reports** in the Reports pane.
- 3 Click **Library Capacity Forecast**.
- 4 On the Report Wizard, select the following:

Report Time Frame	<p>Select time frame to view the report data.</p> <p>Using the Relative Date option, you can specify the time interval in hours, days, weeks, months, years, for which you want to view the data. For example, if you selected 5 days in the Show Last field, the report shows all records that were stored in the last 5 days.</p> <p>Using the Absolute Date option, you can specify the date range for which you want to view the data. Select the date and time from the From and To fields. The resultant report shows all records falling between the specified date range.</p>
Report Time Frame Grouping	<p>Select the time interval by which you want to group the records. For example, if you selected 1 month as the Report Time Frame and 10 days as the Group By interval, the report shows records in three chunks of data grouped by 10 days.</p>
Display Options	<p>Select display options.</p> <p>Select unit for the data to appear on the report, for example, KB, MB, GB, or TB.</p> <p>Select total capacity of the tape library as a reference against which you want to view the actual tape library usage. Select Maximum, Average, Minimum, or User Defined.</p> <p>You can select the User Defined option when you have the exact tape library information with you. You can either enter the actual values or the percentage values for slot count and maximum library capacity.</p>

User Defined Values	<p>If you selected the User Defined option from the Total Capacity Operation, select the user defined values for the following:</p> <ul style="list-style-type: none"><li>■ Media type or name</li><li>■ Maximum tape capacity</li><li>■ Number of slots in a tape library</li><li>■ Alias x-axis</li><li>■ Alias y-axis</li></ul> <p>Select the Use as percentage as slots check box to enter the percentage values of the slot counts and maximum library capacity.</p>
Forecast Parameters	<p>Select filter parameters for forecasting, for example, Backup Media Type, or Tape Library Manufacturer.</p>
Exception Conditions	<p>Select condition, either Total Backup Media Used Capacity or Average Backup Media Total Capacity.</p>

5 Click **Run**.

### About total capacity operation

When you generate the Library Capacity Forecast report, the maximum tape library capacity is calculated depending on the following total capacity operations:

- Maximum
- Average
- Minimum
- User Defined

## Reporting on scheduled jobs data

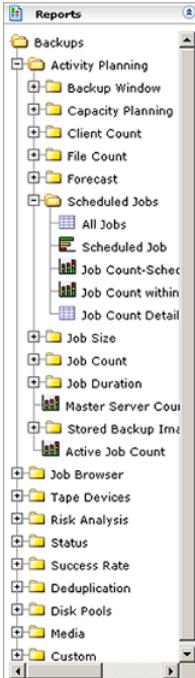
Veritas Backup Reporter (VBR) provides additional information about NetBackup Policies, Schedules, and Jobs. You can generate reports about these details.

See [“About Policy and Scheduled Jobs data collected in VBR 6.6”](#) on page 198.

In Veritas Backup Reporter 6.6, a new backup report category called ‘Scheduled Jobs’ is added. These reports provide information about jobs that are scheduled to run in future.

[Figure 9-14](#) shows a list of new reports in the Scheduled Jobs report category.

Figure 9-14 Scheduled Jobs reports



---

**Note:** The Scheduled Jobs reports are available only for NetBackup.

---

The Scheduled Jobs report category contains the following new reports.

See “[About Policy and Scheduled Jobs data collected in VBR 6.6](#)” on page 198.

- |          |   |
|----------|---|
| All Jobs | <p>This tabular report shows details of all Scheduled Jobs and actual jobs.</p> <p>Scheduled Jobs are the jobs that are scheduled to run in future.</p> <p>Actual jobs are jobs that have already been run. They may be either of execution type ‘Manual’ or ‘Scheduled’.</p> <p><b>Note:</b> Actual job count does not include jobs that do not have policy associated with them, such as Image Cleanup or Restore jobs. Actual job count includes jobs of type Backup and Archive.</p> <p>See “ <a href="#">About the All Jobs report</a>” on page 392.</p> |
|----------|---|

Scheduled Jobs	<p>This ranking report shows the Scheduled Job count for top clients, policies, schedules, and master servers.</p> <p>See <a href="#">“About the Scheduled Jobs report”</a> on page 393.</p>
Job Count-Scheduled Vs Actual	<p>This historical report shows the comparison between Scheduled Job count and Actual Job count.</p> <p>Actual jobs are those jobs that are already executed. These jobs may be of execution type ‘Manual’ or ‘Scheduled’.</p> <p><b>Note:</b> The Actual Job count include only backup and archive type of jobs.</p> <p>See <a href="#">“About the Job Count-Scheduled Vs Actual report”</a> on page 394.</p>
Job Count Within Backup Window	<p>This historical report shows Scheduled Job count and Actual Job count, within a backup window.</p> <p>See <a href="#">“About the Job Count Within Backup Window report”</a> on page 396.</p>
Job Count Details-Scheduled Vs Actual	<p>This tabular report shows the comparison between Scheduled Job count and Actual Job count.</p> <p>See <a href="#">“About the Job Count Details-Scheduled Vs Actual report”</a> on page 397.</p>

## About the All Jobs report

This canned report shows jobs in a tabular form, which include the following:

Manual Jobs	<p>These jobs are initiated manually, by NetBackup admin at his or her discretion. Therefore, these jobs do not have schedule time associated with them.</p> <p><b>Note:</b> While generating the Job Count-Scheduled Vs Actual report, you have an option to exclude the manual jobs from the actual job count and show only those jobs that are of execution type ‘Scheduled’.</p> <p>See <a href="#">“About the Job Count-Scheduled Vs Actual report”</a> on page 394.</p>
-------------	---

**Scheduled Jobs**

These jobs are scheduled to run in future. Each Scheduled Job information comprises a client, policy, schedule, and schedule time. VBR stores this information historically. Each Scheduled Job when run on the specified schedule time becomes an actual job of execution type 'Scheduled'. Thus, a Scheduled Job has a corresponding actual job entry in VBR database. This particular Scheduled Job can be identified by the unique combination of client, policy, schedule, and schedule time. You can compare the schedule time of this Scheduled Job with the corresponding Job Start Time to determine whether that job was run on scheduled time or not.

Figure 9-15 shows a sample All Jobs report.

**Figure 9-15** All Jobs report

Jobs that do not have schedule associated are Manual Jobs.

These Scheduled Jobs do not have Job Start Time and End Time, which implies that they are yet to run.

These Scheduled Jobs have Job Start Time and End Time, which implies that they were run on the specified schedule.

All Jobs										
Client	Master Server	Policy	Schedule	Schedule Start Time	Level	Job Status	Job Id	Job Start Time	Job End Time	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Failure	2915	2009-02-25 17:41:12.0	2009-02-25 17:49:21.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	2920	2009-02-25 18:25:24.0	2009-02-25 18:36:31.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	2917	2009-02-25 18:01:49.0	2009-02-25 18:02:11.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	2916	2009-02-25 18:01:48.0	2009-02-25 18:02:01.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	2913	2009-02-25 17:49:17.0	2009-02-25 18:02:01.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Failure	3072	2009-02-27 09:59:13.0	2009-02-27 10:02:00.0	
pmwin17	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	3075	2009-02-27 10:02:44.0	2009-02-27 10:08:33.0	
gsk	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Failure	3073	2009-02-27 09:59:13.0	2009-02-27 10:02:00.0	
gsk	pmwin17	Multistream	No schedule associated	Job was not scheduled	Full	Success	3076	2009-02-27 10:02:44.0	2009-02-27 10:03:43.0	
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-03-04 11:16:42.603						
ccs-sol-qe-13	ccs-sol-qe-13	SS00-DiskPool-Stugrp	Full	2009-03-05 06:00:00.760						
ccs-sol-qe-13	ccs-sol-qe-13	Pol_Tape_ccqasol2	Full	2009-03-04 21:23:38.866						
ccs-sol-qe-13	ccs-sol-qe-13	Pol_Disk_ccqasol2	Full	2009-03-05 00:00:00.573						
ccs-sol-qe-13	ccs-sol-qe-13	Pol_Disk_ccqasol2	Full	2009-03-05 00:00:00.573						
ccs-sol-qe-13	ccs-sol-qe-13	Pol_Disk_ccs-sol-qe-13	Full	2009-03-05 00:00:00.573						
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-02-26 19:14:26.696	Full	Success	1345	2009-02-22 19:12:36.0	2009-02-22 19:12:48.0	
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-02-26 19:14:26.696	Full	Success	1349	2009-02-22 21:12:38.0	2009-02-22 21:12:49.0	
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-02-26 19:14:26.696	Full	Success	1350	2009-02-22 22:12:39.0	2009-02-22 22:12:49.0	
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-02-26 19:14:26.696	Full	Success	1352	2009-02-22 23:12:40.0	2009-02-22 23:12:49.0	
ccs-sol-qe-13	ccs-sol-qe-13	Test_Pol_Sche_1hr	Test_Sched_1hr	2009-02-26 19:14:26.696	Full	Success	1358	2009-02-23 01:12:42.0	2009-02-23 01:12:59.0	

181 Total Rows Pages: 1 2 3 4 5 6 7 8 9 10 |> |< |

Tabular report showing jobs executed within window , outside window , jobs with no schedules and jobs that are currently scheduled. This report is valid only for Veritas NetBackup.

**About the Scheduled Jobs report**

This report is available in ranking report view, which depicts how many jobs have been scheduled to run in future. You can view the Scheduled Jobs per schedule, policy, master server, or client.

**Note:** By default, the Scheduled Jobs report shows job count per policy. If you want to view the job count for clients, schedules, or master servers, change the report parameters.

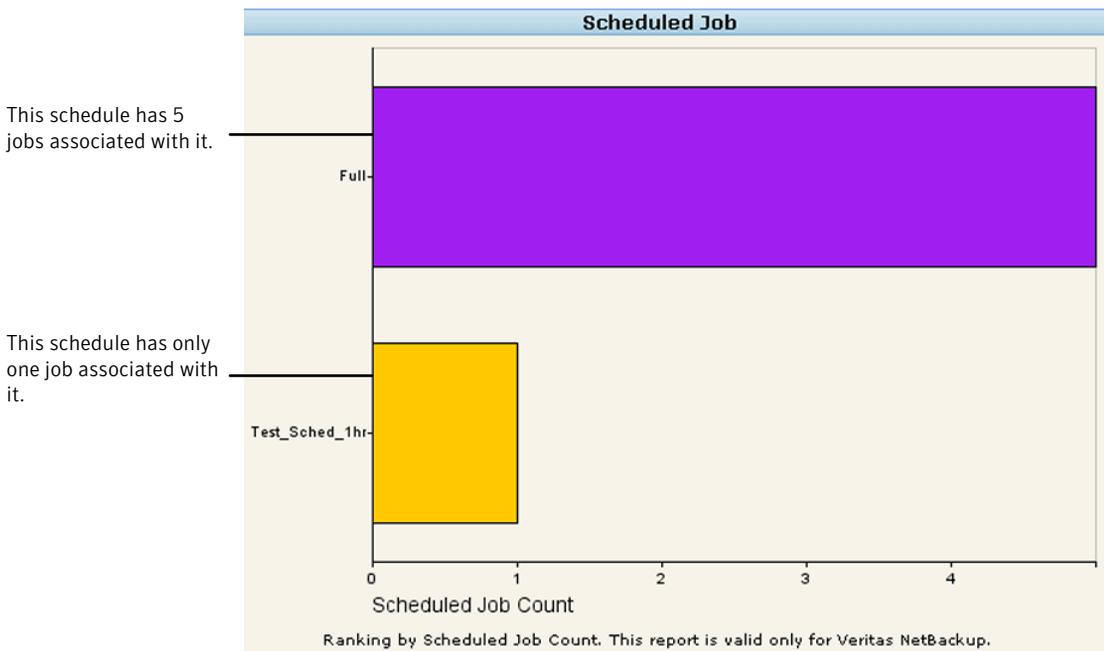
### To change the report parameters

- 1 On the Scheduled Jobs report, click the **Edit** link.
- 2 On the Report Wizard, from the Report On drop-down list, select a Scheduled Job attribute. For example: Client, Master Server, Policy, or Schedule Name.
- 3 Click **Run**.

**Note:** To view job count for a specific client, policy, master server, or schedule, click **Show Advanced Filters** and select name of the client, policy, master server, or schedule, for which you want to view job count.

Figure 9-16 shows a sample Scheduled Jobs report. Here each horizontal bar corresponds to a schedule and the X-axis shows Scheduled Job Count for each of these schedules.

Figure 9-16 Scheduled Jobs report



### About the Job Count-Scheduled Vs Actual report

This historical report depicts how many jobs were scheduled to run in future and how many jobs have actually been run. The report essentially shows the comparison between Scheduled (Future) Job Count and Actual Job Count.

Using this report you can determine whether jobs that were scheduled to run in future have been run on schedule.

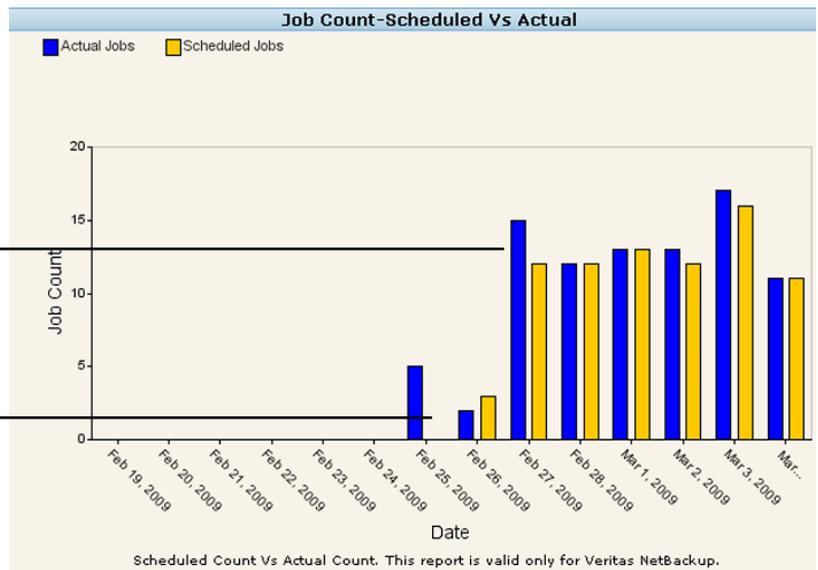
By default the Actual Job Count includes manual jobs, which were initiated manually by NetBackup admin. To exclude manual jobs from the Actual Job count, and view only those jobs that have execution type as 'Scheduled', do the following:

**To exclude manual jobs from the actual jobs**

- 1 On the Job Count-Scheduled Vs Actual report, click the **Edit** link.
- 2 On the Report Wizard, in the Filter Options section, select "Yes" from the Exclude Manual Jobs drop-down list.
- 3 Click **Run**.

Figure 9-17 shows a sample Job Count-Scheduled Vs Actual report. The Actual Jobs include Manual Jobs that have already been run.

**Figure 9-17** Job Count-Scheduled Vs Actual report - including Manual Jobs



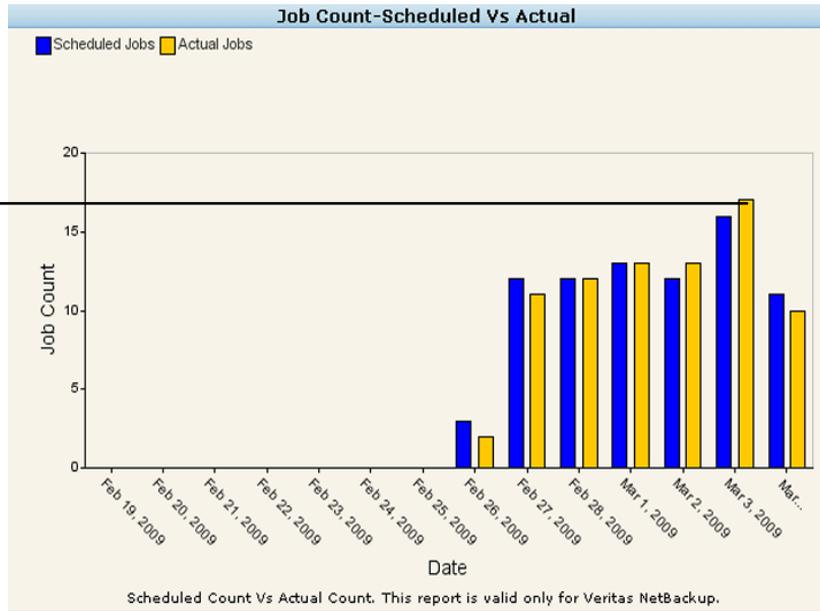
The blue bars show the number of jobs that were run (actual jobs) on a particular day. In this report: Actual Jobs include jobs of execution type 'Scheduled' and 'Manual'.

By looking at this report and the following one, it can be implied that, this is a manual job which was run on 25<sup>th</sup> Feb. Because this job is not present in the following report, which excludes manual jobs from the actual job count.

Figure 9-18 shows a sample Job Count-Scheduled Vs Actual report. Actual Jobs do not include Manual Jobs. This report shows comparison between the number of Scheduled Jobs and the number of jobs that have already been run.

**Figure 9-18** Job Count-Scheduled Vs Actual report - excluding Manual Jobs

The yellow bars show the number of jobs that were run (actual jobs), on a particular day. While generating this report, manual jobs have been excluded. Therefore, in this report: Actual Jobs = Jobs of execution type 'Scheduled'



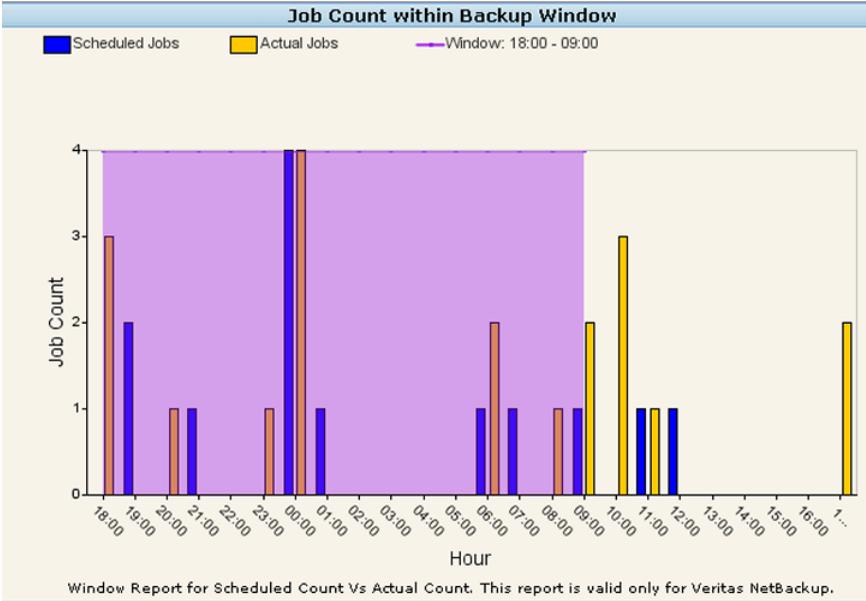
### About the Job Count Within Backup Window report

This historical report depicts how many jobs were scheduled and how many jobs have been run within the specified backup window. The report essentially shows the comparison between Scheduled (Future) Job Count and Actual Job Count, during the backup window.

Use this report to determine whether your backup windows are appropriate and are being properly utilized.

Figure 9-19 shows a sample Job Count Within Backup Window report.

Figure 9-19 Job Count Within Backup Window report



### About the Job Count Details-Scheduled Vs Actual report

This tabular report shows the comparison between Scheduled Job count and Actual Job count for each of the combinations of clients, policies, and schedules, for each day.

**Note:** By default, the Job Count Details-Scheduled Vs Actual report shows job count per policy. If you want to view the job count per client or master server, change the filter parameters.

#### To change the report parameters

- 1 On the Job Count Details-Scheduled Vs Actual report, click the **Edit** link.
- 2 On the Report Wizard, in the Define Viewable Columns section, select a column name (Client or Master Server) from the Available Columns list.
- 3 Click >> button.
- 4 Click **Run**.

**Note:** To view job count for a specific client, policy, master server, or schedule, click **Show Advanced Filters** and select name of the policy, master server, or schedule, for which you want to view job count.

By default the jobs that were run (Actual Job Count) include manual jobs, which do not have any schedule time associated with them as they are initiated manually. You can exclude manual jobs from the actual job count, and view only jobs that are of execution type 'Scheduled'.

**To exclude manual jobs from the actual jobs**

- 1 On the Job Count Details-Scheduled Vs Actual report, click the **Edit** link.
- 2 On the Report Wizard, in the Filter Options section, select Yes from the Exclude Manual Jobs drop-down list.
- 3 Click **Run**.

Figure 9-20 shows a sample Job Count Details-Scheduled Vs Actual report.

**Figure 9-20** Job Count Details-Scheduled Vs Actual report

Job Count Details-Scheduled Vs Actual					
Date (DD/MM/YYYY)*	Policy	Client	Master Server	Scheduled Count	Actual Count
4/3/2009	NBU1	pmwin17	prwin17	0	1
4/3/2009	S3OD-DiskPael-Sbugrp	ccs-sol-qe-13	ccs-sol-qe-13	1	1
4/3/2009	Test_Pol_sche_1hr	ccs-sol-qe-13	ccs-sol-qe-13	6	5
4/3/2009	Pol_Disk_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	1	1
4/3/2009	Pol_Disk_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	1	1
4/3/2009	Pol_Type_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	1	1
3/3/2009	Pol_Type_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	2	2
3/3/2009	Pol_Disk_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	1	1
3/3/2009	Pol_Disk_ccsqasol3	ccs-sol-qe-13	ccs-sol-qe-13	1	1
3/3/2009	S3OD-DiskPael-Sbugrp	ccs-sol-qe-13	ccs-sol-qe-13	1	1
3/3/2009	Pol_Disk_ccs-sol-qe-13	ccs-sol-qe-13	ccs-sol-qe-13	1	1
3/3/2009	Test_Pol_sche_1hr	ccs-sol-qe-13	ccs-sol-qe-13	10	11
28/2/2009	Pol_Disk_ccsqasol2	ccs-sol-qe-13	ccs-sol-qe-13	1	1
28/2/2009	Test_Pol_sche_1hr	ccs-sol-qe-13	ccs-sol-qe-13	8	8
28/2/2009	Pol_Disk_ccsqasol3	ccs-sol-qe-13	ccs-sol-qe-13	1	1
28/2/2009	S3OD-DiskPael-Sbugrp	ccs-sol-qe-13	ccs-sol-qe-13	1	1
28/2/2009	Pol_Disk_ccs-sol-qe-13	ccs-sol-qe-13	ccs-sol-qe-13	1	1
27/2/2009	Multiclient	pmwin17	pmwin17	0	2
27/2/2009	Multiclient	gek	pmwin17	0	2
<b>38 Total Rows</b>				<b>Pages:</b> 1   2   11	
Scheduled Count Vs Actual Count by Policy , Master server and Client. This report is valid only for Veritas NetBackup.					
<b>Time frame:</b>		Last 7 Day(s)			

This particular record shows that on 3/3/2009, Scheduled Job count is 10 and Actual Job count is 11

The Actual Job count includes jobs that were run and which are of execution type 'Scheduled' and 'Manual'.

The Job Count Details-Scheduled Vs Actual report shows comparison between Scheduled Job count and Actual Job count. The Actual Job count includes Manual Jobs.

**About new NetBackup-specific filter parameters**

In Veritas Backup Reporter 6.6, a new set of filter parameters / attributes have been added: Scheduled Jobs, Backup Schedule, and Backup Policy. Using these filters you can view specific data related to the new policy and job data collected from NetBackup. The following table lists all these new filter parameters / attributes and their navigation.

**Table 9-3** New parameters in custom reports

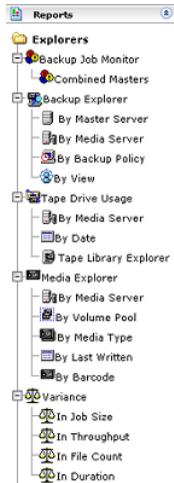
Data type	Navigate to
Job - Scheduled Jobs	<ul style="list-style-type: none"> <li>■ Click <b>Reports &gt; Custom</b>.</li> <li>■ From the Category drop-down list, select the new attribute Scheduled Jobs and Report Type and click <b>Next</b>.</li> </ul> <p>On the parameters page, in the Report On, Y-axis, and X-axis parameters, new Scheduled Jobs attributes have been added.</p> <p>In the Filter parameters, in the Backup Schedule, new attributes are available.</p> <hr/> <ul style="list-style-type: none"> <li>■ Click <b>Reports &gt; Custom</b>.</li> <li>■ From the Category drop-down list, select Backup/Job/Image/Media.</li> <li>■ Select Tabular from the Report Type drop-down list and click <b>Next</b>.</li> </ul> <p>On the parameters page, in the Available Columns parameter, following filter attributes have been added:</p> <ul style="list-style-type: none"> <li>■ Backup Job Attributes &gt; Job Execution Type</li> <li>■ Backup Job Attributes &gt; Job Scheduled Time</li> <li>■ Backup Job Attributes &gt; Window Closing Time</li> <li>■ Schedule Attributes</li> </ul>
Policy	<ul style="list-style-type: none"> <li>■ Click <b>Reports &gt; Custom</b>.</li> <li>■ From the Category drop-down list, select the new attribute Scheduled Jobs and click <b>Next</b>.</li> </ul> <p>On the parameters page, in the Filter parameters, new Backup Policy filter attributes have been added.</p> <p>In the Filter parameters, new Backup Policy filter attributes have been added.</p>

## Viewing explorer reports

In VBR 6.6, reports under Monitors tab have been moved to Reports > Explorers section.

[Figure 9-21](#) shows a list of report available in the Explorers section.

Figure 9-21 Explorer reports tree



## Viewing backup jobs for hosts by object views

You can monitor backup jobs that are organized by object view categories, for example Geography or Application.

### To view backup jobs for hosts in an object view category

- 1 In the Veritas Backup Reporter console, click **Reports > Explorers**. The console displays a menu of tools for monitoring and tracking backup jobs.
- 2 In the task pane tree view, expand Backup Job Monitor, and then click **Combined Masters**.
- 3 Do one of the following:
  - Select a backup job ID to view additional details for that job, including skipped files and job log entries.
  - Select a backup job's status. For example, a status code of 0 means the job completed without errors.

## Viewing backup jobs by host

You can monitor the backup jobs for hosts on a specific master server or media server, or within a specific object view category.

### To view backup jobs for hosts

- 1 In the Veritas Backup Reporter console, click **Reports > Explorers**. The console displays a menu of tools for monitoring and tracking backup jobs.
- 2 In the task pane tree view, expand Backup Explorer.
- 3 Select one of the following:
  - By Master Server
  - By Media Server
  - By backup Policy
  - By View

A table of master servers or media servers displays, showing the number of backup jobs, last backup, and oldest backup for each one.

- 4 Select the server whose backup jobs you want to view.

The Backup Summary table displays, showing backup jobs for each host in the indicated server. Each host's backup jobs display in a single row sorted by date, the most recent jobs appearing in the leftmost columns. Mouse over an individual job to see a tool tip that includes details like the job ID, the exact time the job completed, and the job's status.
- 5 Click a host name to view the Host Backup Jobs table, which contains a more detailed list of that host's backup jobs.
- 6 Do one of the following:
  - Select a backup job ID to view additional details for that job, including skipped files and job log entries.
  - On the Format drop-down list, select a time frame and intervals. Examples: 4 Hours at 15 minute intervals
  - To include statistics on tape drive usages associated with backup jobs, select Include Tape Drive Use, and then click **Go**. Using this option will probably increase the time it takes to populate the table with data. The table refreshes to display data based on your selections. Select the name of a master server to display more detailed information about backup jobs for that server.

### Viewing tape drive utilization history

Veritas Backup Reporter collects log data from your backup media servers and compiles it into a history of tape drive utilization. Use the Tape Drive Usage tool to view detailed information about a drive's usage in percentage. This tool helps

the administrator evaluate whether tape drives are being used efficiently and whether there is a need to add more drives.

#### To view tape drive utilization history

- 1 In the Veritas Backup Reporter console, click **Reports > Explorers**. The console displays a menu of tools for monitoring and tracking backup jobs.
- 2 In the task pane tree view, click **Tape Drive Usage**. The Tape Drive Usage table displays a list of master servers and media servers, showing the most recent sample, number of samples, and utilization percentage for each server.
- 3 In the Tape Drive Usage table, click the server whose tape drive usage history you want to view.

A table displays the utilization history of the server's individual tape drives. Each column in the table represents a snapshot of the drive utilization, with 15 minute intervals between each sample. Mouse over a table field to see the exact time the snapshot was taken, and which media server was writing to the drive at that time.

## Viewing backup tape media status

Veritas Backup Reporter collects log data from Veritas NetBackup and BackupExec and compiles status information for the backup media into its database. You can view recent writes, availability, and status for your backup media.

#### To view backup media

- 1 In the Veritas Backup Reporter console, click **Reports > Explorers**. The console displays a menu of tools for monitoring and tracking backup jobs.
- 2 In the task pane tree view, click **Media Explorer**.  
  
A table of master servers and media servers displays, showing the number of media (usually tapes) and the images they contain, along with the date and time they were last updated, and the total amount of data on media (in GB) for each server.
- 3 Click the server host whose backup media you want to view. A table displays data about all of the server's backup media, organized by status. Each row displays the number of media devices, the total number of images they contain, and the total amount of data (in GB).

- 4 In the Master Media Explorer table, select a status, such as Active or Full.  
A table displays summary information for each backup medium reporting the selected status. For each medium, the table displays its volume pool, number of images, when it was last updated, the oldest expiration date, its density, and the total amount of data (in GB).
- 5 Click an individual media ID to view detailed information for that medium.

## Viewing backup data with infinite retention periods

In Veritas Backup Reporter, you can view records that have infinite retention period.

### To view backup data with infinite retention period

- 1 In the Veritas Backup Reporter console, click **Reports > Custom**.
- 2 On the Select Report Category and Type page, select any of the following categories:
  - Backup Job/Image
  - Backup Media
- 3 Select report type as Tabular.
- 4 Click **Next**.
- 5 Select report parameters, such as View, Viewable Columns, and Time Frame.
- 6 In the Time Frame section, select any of the following parameters depending on the report category you have selected.
  - Job Expiration Time
  - Backup Image Expiration Time
  - Backup Media Expiration Time
  - Backup Media Physical Expiration TimeOther expiration time related filters, such as Backup Image Copy Expiration Time and Backup Image Fragment Expiration Time are available in the Filter > Backup Images section.

- 7 When you select the expiration time, the following fields are displayed in the Time Frame section.

**Include Infinite Values** Select this check box to display all records, which include records with fixed as well as infinite expiration time.

**Only Infinite Values** Select this check box to display only those records that have expiration time set as infinity.

- 8 Click **Run**.

The resulting report displays all relevant records. The jobs, images, or media that have infinite expiration time are marked 'Infinite Retention'.

## Viewing backup data with future expiration dates

In Veritas Backup Reporter, you can view jobs, images, and media that are expiring in future.

### To view backup data with future expiration date

- 1 In the Veritas Backup Reporter console, click **Reports > Custom**.
- 2 On the Select Report Category and Type page, select any of the following categories:
  - Backup Job/Image
  - Backup Media
- 3 Select report type as Tabular.
- 4 Click **Next**.
- 5 Select report parameters, such as View, Viewable Columns, Time Frame and so on.
- 6 In the Time Frame section, click **Relative**.
- 7 Select any of the following parameters depending on the report category you have selected:
  - Job Expiration Time
  - Backup Image Expiration Time
  - Backup Media Expiration Time
  - Backup Media Physical Expiration Time

Other expiration time related filters, such as Backup Image Copy Expiration Time and Backup Image Fragment Expiration Time are available in the Filter > Backup Images section.

- 8 When you select the expiration time, the following fields are displayed in the Time Frame section:

A drop-down list with Last and Next as values to be selected

- Select **Last** from the drop-down list to view jobs, images, and media that have already expired.
- Select **Next** from the drop-down list to view jobs, images, and media that are expiring in future.

Select Include Infinite Values or Only Infinite Values check box if you want to view records that have expiration time set as infinity.

See [“Viewing backup data with infinite retention periods”](#) on page 403. for more details.

- 9 Click **Run**.

## Reporting on archive data

Veritas Backup Reporter 6.6 has been integrated with Enterprise Vault to provide reports based on the archive data pertaining to Microsoft Exchange Server (MS Exchange Server or Exchange Server).

See [“About data collected from Enterprise Vault”](#) on page 238.

See [“About versions supported by Veritas Backup Reporter”](#) on page 240.

In Veritas Backup Reporter 6.6, a new report category called Archives is added.

The Archives report category contains a number of new reports that are generated based on the archive data pertaining to MS Exchange Server, which is collected from Enterprise Vault. For example, Original Size, Count of Items, or Original Size Vs. Archive Size.

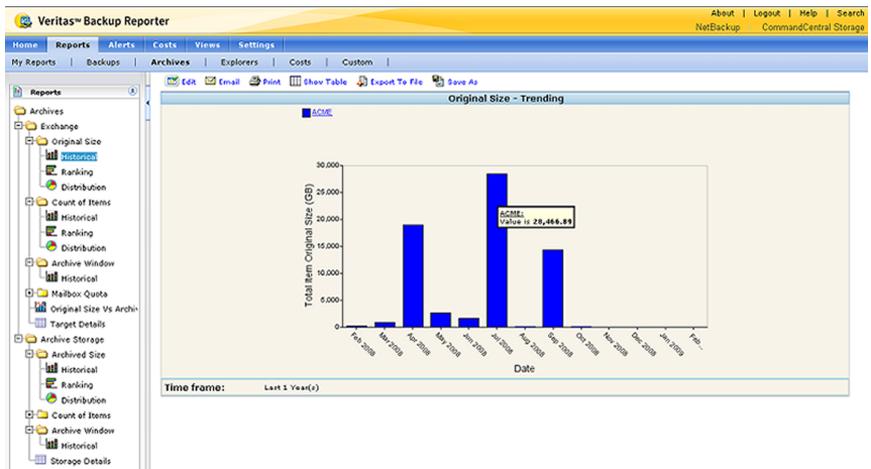
---

**Note:** Cost reports are not available for Enterprise Vault / archive data.

---

[Figure 9-22](#) displays a sample archive report.

Figure 9-22 Archive reports

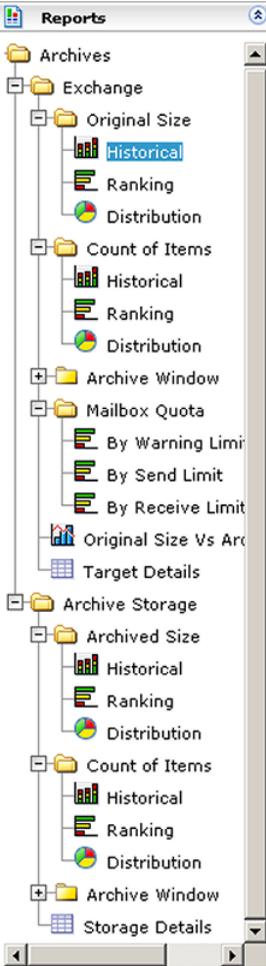


## About archive report categories

Archive reports have two categories: Exchange and Archive Storage

Figure 9-23 displays the archive report tree.

**Figure 9-23** Archive report categories



## Exchange

The Exchange report category contains the following reports:

- Original Size
- Count of Items
- Archive Window
- Mailbox Quota
- Original Size Vs Archived Size
- Target Details

This archive report category comprises reports that mainly provide Exchange Servers-specific information. For example, Original Size, Mailbox Quota, Original Size Vs Archived Size, or Target Details reports

The Exchange reports can be drilled down to further levels. Depending on the Report On parameter that you have selected while generating an Exchange report, the drill-down paths change.

If you have selected Archive Site as the Report On parameter, the drill-down path is as follows: Archive Site > Exchange Servers > Provisioning Groups

On an Exchange report, you can select an archive site to view details of the Exchange Servers within that site, select an Exchange Server to view the details of its provisioning groups.

If you have selected Enterprise Vault Server as the Report On parameter, the drill-down path is as follows: Enterprise Vault Server > Vault Store > Vault Partition

If you have selected Target Server as the Report On parameter, the drill-down path is as follows: Exchange Servers > Provisioning Groups

If you have selected Vault Store as the Report On parameter, the drill-down path is as follows: Vault Store > Vault Partition

## Archive Storage

The Archive Storage report category contains the following reports:

- Archived Size
- Count of Items
- Archive Window
- Storage Details

This archive report category comprises reports that mainly provide storage-specific information. For example, Archived Size or Storage Details reports

The Archive Storage reports can be drilled down to further levels. Depending on the Report On parameter that you have selected while generating an Archive Storage report, the drill-down paths change.

If you have selected Archive Site as the Report On parameter, the drill-down path is as follows: Archive Site > Enterprise Vault Server > Vault Store > Vault Partition

On an Archive Storage report, you can select an archive site to view details of the Enterprise Vault Server within that site. Select an Enterprise Vault Server to view the details of its Vault Stores. Select a Vault Store to view the details of its Vault Partitions.

If you have selected Enterprise Vault Server as the Report On parameter, the drill-down path is as follows: Enterprise Vault Server > Vault Store > Vault Partition

If you have selected Vault Store as the Report On parameter, the drill-down path is as follows: Vault Store > Vault Partition

---

**Note:** The Count of Items and Archive Window reports are available in both archive report categories.

All archive reports provide drill-down reports depending on the archive report category - Exchange or Archive Storage - that you have selected.

---

## About filter parameters specific to Enterprise Vault

In Veritas Backup Reporter 6.6, a new set of filter parameters called Archive Attributes and is added under the Report On parameter. Use these attributes to filter the Enterprise Vault / archive data.

Additionally, following Advanced Filters are provided in Veritas Backup Reporter 6.6, which you can use to filter your Enterprise Vault / archive data:

[Figure 9-24](#) displays filter parameters specific to Enterprise Vault.

Figure 9-24 Enterprise Vault filter parameters

The screenshot shows the 'Report Wizard' interface with the following sections and parameters:

- Report Grouping:** Report on: Archive Site (dropdown menu open showing options: Select..., Views, View Groups, Archive Attributes, Archive Site, Archive Vault Partition Name, Archive Vault Store Name, Archive Vault Store Vault Server, Provisioning Group, Target Server).
- Report Time Frame:** Relative Date (selected) / Absolute Date. Show Last: (dropdown menu).
- Report Time Frame Grouping:** Group by: 1 Day(s).
- Display Options:** Display Unit: GB. Alias X-Axis Name: (text field). Alias Y-Axis Name: (text field). Report Description: (text field).
- Report Time Frame Trendline:** Include Trendline?: Yes (selected) / No. If yes, Moving Average Period: 3. Hide Advanced Filters: (dropdown arrow).
- Archive Site:** ACME Default Domain.
- Archive Vault Store:** EU Dom Journal VS Dual3, EU Dom Journal VS Dual5, EU Dom Mailbox VS Dual3.
- Archive Vault Server:** vtsn01.acme.local, vtsn02.acme.local, vtsn03.acme.local.
- Exchange Server:** (text field).
- Archive Vault Store Partition:** EU Dom Journal VS Dual3 Ptn1, EU Dom Journal VS Dual5 Ptn1, EU Dom Mailbox VS Dual3 Ptn1.
- Buttons:** Run, Cancel.

These filter parameters are described in detail in the following section.  
See [“Generating an archive canned report”](#) on page 410.

## Generating an archive canned report

Veritas Backup Reporter 6.6 provides a set of archive reports that are based on Exchange Server data. These archive reports are available in the new report category called Archives.

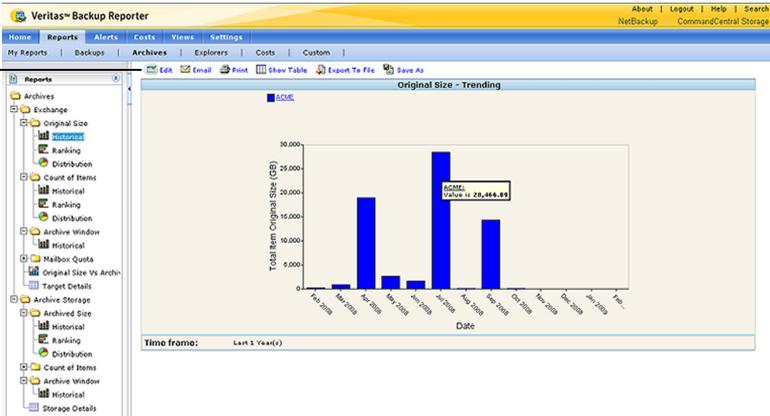
This section provides the procedure for generating an archive or Enterprise Vault report. The following sections explain each archive report in detail. The steps to generate all these reports is the same.

**To generate an archive or Enterprise Vault report**

- 1 In the Veritas Backup Reporter console, click **Reports > Archives**. The following screen is displayed.

Click the Edit link to change the report parameters.

Click the Show Table link to view the archive data in a tabular form.



- 2 In the Reports tree, navigate to the report that you want to generate, by expanding the Exchange or Archive Storage report folders.  
See [“About archive report categories”](#) on page 406.

- 3 Select the name of the report for example, Original Size > Historical or Count of Items > Distribution.

It generates a default (or canned) report with default filter parameters on, in the report area at the right-hand side, in the report view (Historical, Ranking, Distribution, or Tabular) that you have selected. All of these report views are not available for all archive reports. Some are only tabular reports, some are historical, and a few can be displayed in all graphical report views (Historical, Ranking, and Distribution).

Each of these report views has the option to view the report data in tabular form. Click the **Show Table** link to view the data in a table.

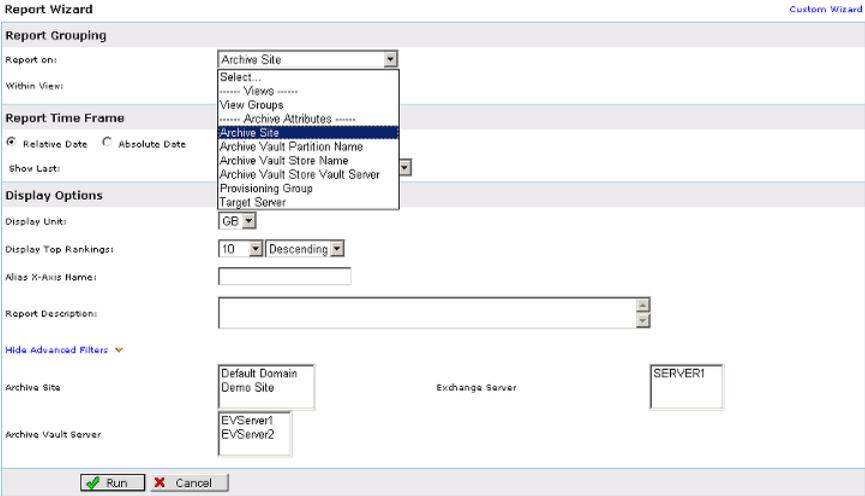
The report views are described as follows:

Historical	<p>This report view depicts report data using stacked bars. Multiple stacks of data are represented using different colors.</p> <p>Use this report view if you want to compare two or more sets of data.</p> <p>For example: You have 5 Exchange Servers in your setup and you want to know the original size of the archived data for each Exchange Server, for the last one month. Generate a historical report. The report output shows multiple vertical bars in 5 different colors, each representing one of the 5 Exchange Servers. The height of the stacked bars represent the original size of the archived data pertaining to the Exchange Servers. If the data of multiple Exchange Servers was archived on the same day, this is represented by a vertical bar having multiple stacks of different colors, one above the other.</p>
Ranking	<p>This report view depicts report data using horizontal bars. Multiple sets of data are represented using different colors of bars.</p> <p>Use this report view to determine the sets of data that exceed others in numbers.</p>
Distribution	<p>This report view depicts report data using a pie chart. Multiple sets of data are represented using different colors.</p> <p>Use this report view to determine the percentage of each set of data.</p>
Tabular	<p>This report view displays the records of data in a table.</p>

- 4 Click the **Edit** link in the report area. This opens the Report Wizard where you can select filter parameters to filter the report as you wish.

**5** In the Report Wizard page, select any of the following Report On parameters:

**Note:** In Veritas Backup Reporter 6.6, a new set of attributes - called Archive Attributes - is added in the Report On filter parameter. Use these attributes to filter the Enterprise Vault / archive data.



**Archive Site**

Select this filter attribute to view data pertaining to various archive sites available in the Enterprise Vault environment.

For example: Your Enterprise Vault setup comprises three archive sites (or domains) namely Site A, Site B, Site C. These sites consist of multiple Enterprise Vault Servers that archive Exchange Server data. If you want to know the size of the data which was archived for each archive site for the last one month, do the following:

- Click Reports > Archives > Archive Storage > Archived Size > Historical or Ranking or Distribution.
- Select Archive Site from the Report On drop-down list and 1 Month from the Report Time Frame drop-down list.
- Run the report.

The report shows the total size of data that was archived by Enterprise Vault Servers residing in each archive site.

**Archive Vault Partition Name**

Select this filter attribute to view archive data stored in vault partitions of various Enterprise Vault Servers.

Archive Vault Store Name	Select this filter attribute to view archive data pertaining to vault stores of various Enterprise Vault Servers.
Archive Vault Store Vault Server	Select this filter attribute to view archive data pertaining to various Enterprise Vault Servers.
Provisioning Group	Select this filter attribute to view archive data pertaining to various Provisioning Groups.
Target Server	Select this filter attribute to view archive data pertaining to various MS Exchange Servers.

**6** Select a view from the Within View drop-down list, of which you want to view details.

**7** Select any of the following Report Time Frame options:

**Relative Date** Select this time frame option if you want to view data for a specific period of time in the past starting from the current date.

For example, if you want to view the data for last 10 months, select the Relative Date option and select 10 Month(s) from the Show Last drop-down list.

You can view data for last several hours, days, weeks, months, or years. For example: 60 hours, 20 days, 10 weeks, 5 months, 1 year, and so on.

**Absolute Date** Select this option if you want to view data for the days between two specific dates. Select From and To dates from the drop-down lists available.

For example, if you want to view how much data was archived since 1st January 2009 to 1st February 2009, select the Absolute Date option and select JAN 1 2009 12:00 AM from the From drop-down list and select FEB 1 2009 12:00 AM from the To drop-down list.

**8** In the Report Time Frame Grouping section, select the Group by option . Depending on the purpose of the report, the Group by options vary.

- If you want to generate the Original Size, Archived Size, or Count of Items, you can select Group by options like 10 Hours, 5 Days, 1 Week, 4 Months, 5 Years and so on.

For example: If you want to view original size of the archived data in Historical view for the period between 1st Jan 2009 to 1st Feb 2009 in

groups, each of one week, select 1 Week from the Group by drop-down list. On the report, you can see data in four stacked bars, one per week.

- If you are generating a window type of a report, for example Archive Window, you can select any of the following Group by options: Hour of the Day (Total) or Hour of the Day (Average).

If you have selected 4 Hours of the Day (Total) as a group by option, the size of archive data displayed is the summation of size of data for each hour. If you have selected 4 Hours of the Day (Average), the size of archive data for is the average of the data for each hour.

**9** This step is specific to Window reports.

If you are generating the Archive Window report, the Window Setting options are available on the Report Wizard page. Select a specific window, within which you want to determine how much data was archived. Select time of the day from the drop-down list, for example: 4 AM to 4 PM.

**10** Select Display Options, which vary depending on the report view / report type that you have selected.

- In case of the Historical type of a report, you have the following Display Options to select:

**Display Unit** Select a unit for size of the data that you want to display on the report. Select KB, MB, GB, or TB.

This display option is available wherever relevant. It is not available for selection if you are generating the Count of Items report.

**Alias X-Axis Name** Enter the X-axis variable name that you want to be appeared on the report output, for example, 'Week in a month'. If you do not enter anything, the report shows the default X-axis variable name, which is Date.

**Alias Y-Axis Name** Enter the Y-axis variable name that you want to be appeared on the report output. For example, you can enter the following text if you are generating the Original Size Vs Archived Size report against an archive site called 'Roseville': Savings for Roseville site.

If you do not enter anything, the report shows the default Y-axis variable name, for example, Total Item Original Size (GB).

**Report Description** Enter the text that describes this report.

For example, if you are generating the Count of Items report, you can enter the following text in this text box: This report depicts how many mailboxes pertaining to the Roseville archive site have been archived in the month of January 2009.

Select the Report Time Frame Trendline as follows:

**Include Trendline?**

If yes, Moving Average  
Period

- In case of the Ranking type of a report, you have the following Display Options to select:

**Display Unit** Select a unit for size of the data, which you want to display on the report. Select KB, MB, GB, or TB.

**Display Top Rankings** Select the number of horizontal bars that you want to display on the report, which should represent maximum of the available data in ascending or descending manner.

For example: If you have 7 Exchange Servers available in your setup, which contain size of data as follows: 100 GB, 20 GB, 30 GB, 50 GB, 70 GB, 500 GB, 600 GB and you have selected 5 and Ascending from the Display Top Rankings drop-down list, the report displays the horizontal bars representing the size of data as shown in the following order:

50 GB  
70 GB  
100 GB  
500 GB  
600 GB

**Alias X-Axis Name** Enter the X-axis variable name that you want to be appeared on the report output. For example, you can enter the following text if you are generating the Original Size Vs Archived Size report against an archive site called 'Roseville': Savings for Roseville site.

If you do not enter anything, the report shows the default Y-axis variable name, for example, Total Item Original Size (GB).

**Report Description** Enter the text that describes this report.

For example, if you are generating the Count of Items report, you can enter the following text in this text box: This report depicts how many mailboxes pertaining to the Roseville archive site have been archived in the month of January 2009.

- In case of the Distribution type of a report, you have the following Display Options to select:

**Display Unit** Select a unit for size of the data, which you want to display on the report. Select KB, MB, GB, or TB.

**Alias X-Axis Name** Enter the X-axis variable name that you want to be appeared on the report output. For example, you can enter the following text if you are generating the Original Size Vs Archived Size report against an archive site called 'Roseville': Savings for Roseville site.

If you do not enter anything, the report shows the default Y-axis variable name, for example, Total Item Original Size (GB).

**Report Description** Enter the text that describes this report.

For example, if you are generating the Count of Items report, you can enter the following text in this text box: This report depicts how many mailboxes pertaining to the Roseville archive site have been archived in the month of January 2009.

- In case of a tabular report, you have the following Display Options to select:

Report Description	Enter the text that describes this report.  For example, if you are generating the Count of Items report, you can enter the following text in this text box: This report depicts how many mailboxes pertaining to the Roseville archive site have been archived in the month of January 2009.
Table Rows Per Page	Enter the number of records that you want to view on the tabular report, per page.  For example: You have selected 10 from the Table Rows Per Page drop-down list and there are totally 50 records. The records are distributed across 5 pages, 10 records per page.

## 11 Select advanced filters.

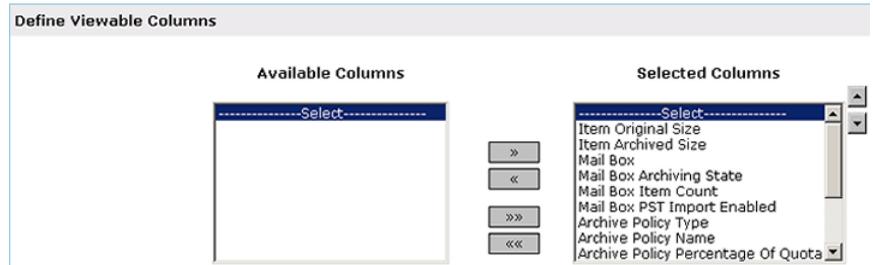
To select advanced filters, click **Show Advanced Filters**. It displays the available advanced filters.

Archive Site	Select a specific archive site to view the associated archive data.
Archive Vault Store	Select a specific Vault Store to view the associated archive data.
Archive Vault Server	Select a specific Enterprise Vault Server to view the associated archive data.
Exchange Server	Select a specific Exchange Server to view the associated archive data.
Archive Vault Store Partition	Select a specific Enterprise Vault Store Partition to view the associated archive data.
Provisioning Group	Select a specific Provisioning Group to view the associated archive data.

**12** This step is specific to tabular reports.

If the report is a tabular one for example, Target Details or Storage Details, the Define Viewable Columns section is available where you can select columns that you want to be appeared on the tabular report. By default all viewable columns are selected

In case of Target Details tabular report, the following columns are available for selection: Item Original Size, Mailbox Item Count, or Mailbox PST Import Enabled, and so on.



In case of Storage Details report, the following columns are available for selection: Archive Vault Name, Archive Vault Description, Archive Vault Store Name and so on.

Select viewable columns as follows:

In the Define Viewable Columns section, select a column name from the Selected Columns list, which you do not want to be visible on the report and click << arrow button. Thus, you can remove column names one by one from the Selected Columns list. The columns that you have removed from the Selected Columns list will be added to the Available Columns list. You can add any of these columns to the Selected Columns list by select that column and clicking the >> arrow button. The column names that are present in the Selected Columns list are visible in the report output.

Click << << arrow button to remove all column names from the Selected Columns list, at once.

Click >> >> arrow button to add all column names in the Available Columns list to the Selected Columns list, at once.

Use



or



buttons to change the sequence of the column names that you want to display on the report.

**13** Click **Run** to generate a report.

Click links on the report to drill it down to the next level.

## About the Original Size report

This report is available only in the Exchange report category. Generate this report if you want to determine the original size of the Exchange Server data that was archived. You can view the original size of the archived data for a specific archive site or Exchange Server. You can also determine how much was the original size of the data that was archived and has been stored in a specific Vault Store, Enterprise Vault Server, or Vault Store Partition. You can select these filters using the Advanced Filters option on the Report Wizard page.

See [“Generating an archive canned report”](#) on page 410.

The Original Size report is available in all three graphical views, Historical, Ranking, and Distribution.

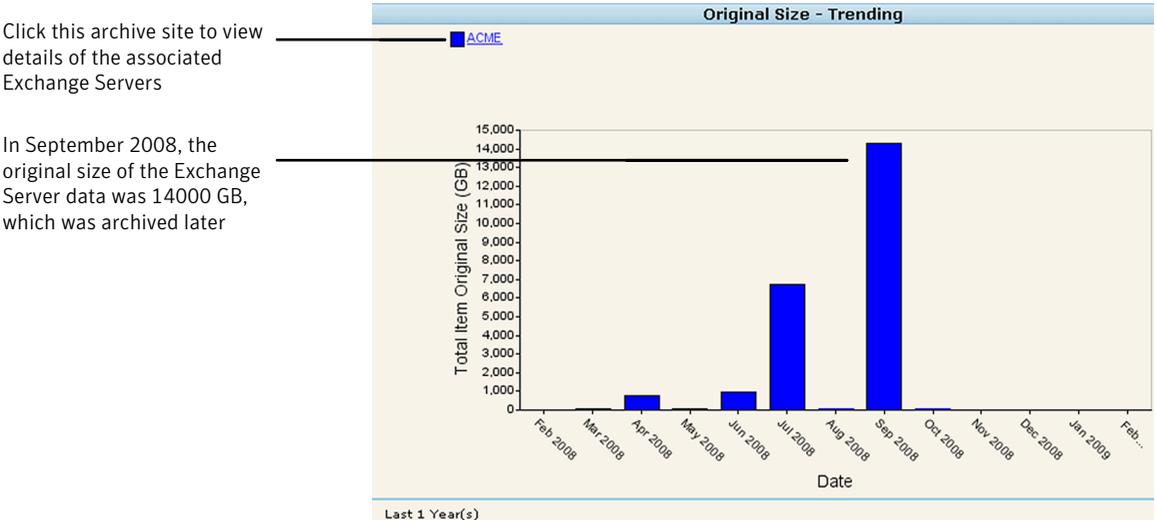
See [“About archive report categories”](#) on page 406.

The following example explains about the original size of the data that was archived:

- You have 100 MB of Exchange Server data, which is the total mailbox size
  - Out of 100 MB data you want to archive 30 MB, as per the definition in an archive policy
  - After archiving, the 30 MB data is compressed into 20 MB data
  - The Original Size of Exchange Server data was 30 MB and Archived Size is now 20 MB
  - The total savings are equal to the difference between the Original Size and Archived Size. Total Savings = 30 MB - 20 MB = 10 MB
- By archiving, you can save on huge amount of storage space.

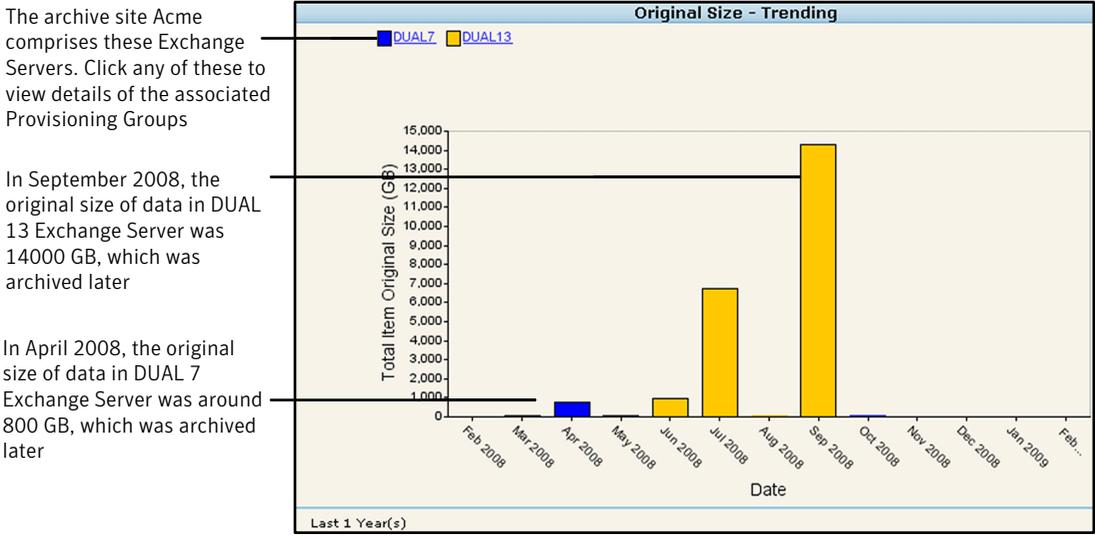
[Figure 9-25](#) shows a sample Original Size report in the historical view. Archive Site is selected as the Report On parameter. Therefore, the drill-down path is: Archive Site > Exchange Server > Provisioning Group.

**Figure 9-25** Original Size report



The report displays, in an archive site called 'Acme' how much was the original size of the Exchange Server data that has been archived since last one year.

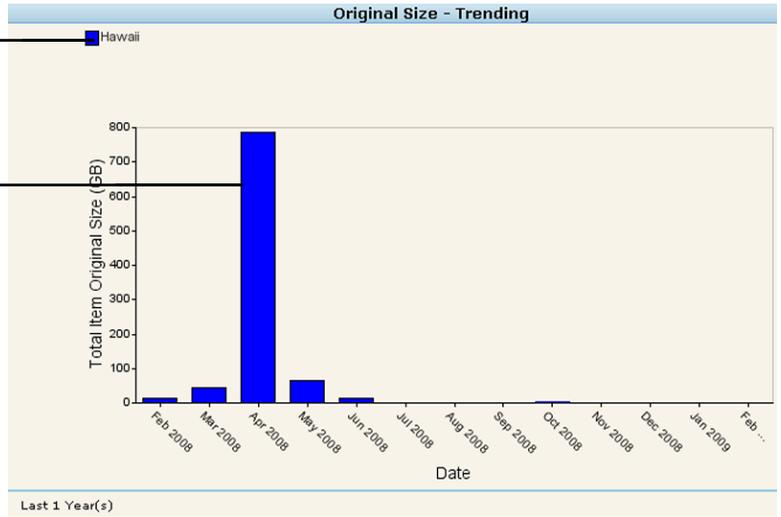
On the Original Size report click the archive site link to view details of the Exchange Servers it comprises.



The following is the drill-down report that depicts details about the Exchange Servers available in Acme archive site. Click any of the Exchange Server link to view the details about its Provisioning Groups.

Exchange Server DUAL 7  
comprises this provisioning  
group

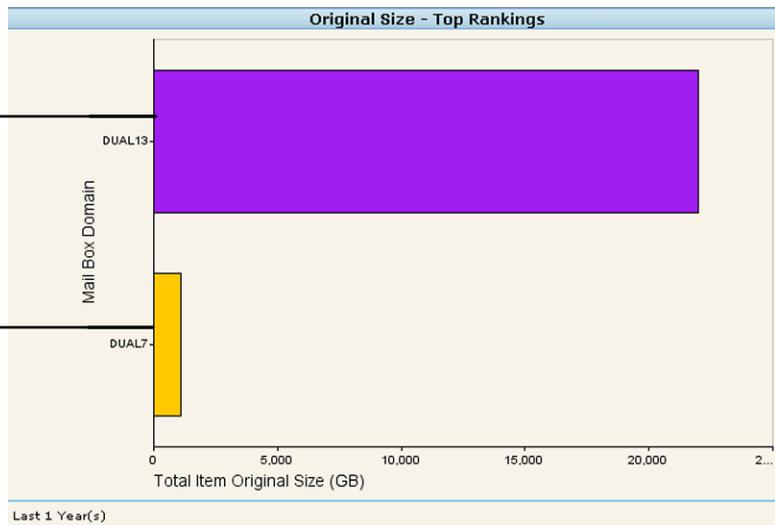
In April 2008, the original size of  
the DUAL 7 Exchange Server data  
was around GB, which was  
archived later



The following sample report depicts the ranking view of the Original Size report. Target Server (Exchange Server in this case) is selected as the Report On parameter. Therefore the drill-down path is: Target Server / Exchange Server > Provisioning Group

The Acme archive site contains  
top two Exchange Servers:  
DUAL 13 that stores totally  
22,000 GB of data, which was  
archived

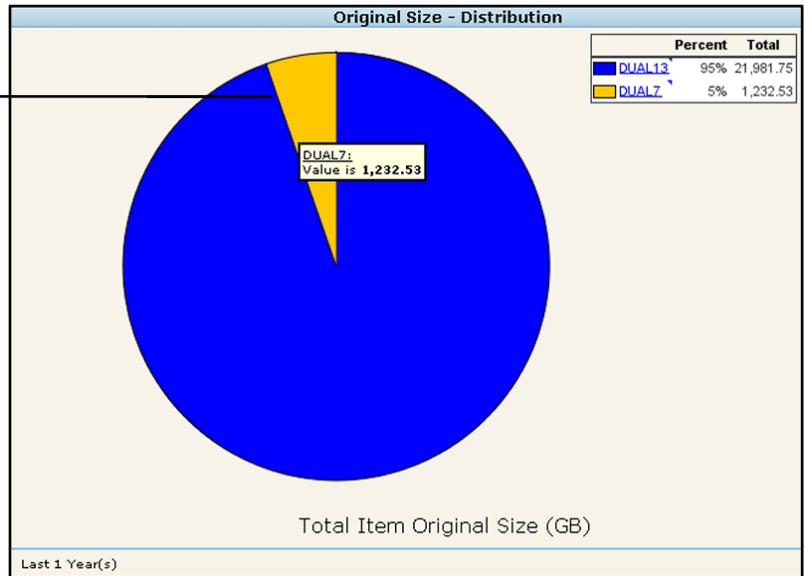
DUAL 7 that stores totally  
1,000 GB of data, which was  
archived



The following sample report depicts the distribution view of the Original Size report. Target Server (Exchange Server in this case) is selected as the Report On parameter. Therefore the drill-down path is: Target Server / Exchange Server > Provisioning Group

The pie chart (Distribution) view of the Original Size reports depicts the following:

The total size of data (around 25,000 GB) that was archived in the last one year, in the Acme archive site, is distributed between the two exchange servers - DUAL 13 (95 %) and DUAL 7 (5 %)



The Original Size Vs Archived Size report depicts the difference between the two size of Exchange Server data. The more the difference, the more efficient is your archival process.

See [“About the Original Size Vs Archived Size report”](#) on page 426.

## About the Count of Items report

This report is available in both archive report categories, Exchange and Archive Storage. Use this report to determine the number of emails or items in each Exchange Server in an Enterprise Vault environment.

See [“Generating an archive canned report”](#) on page 410.

The Count of Items report is available in all three graphical views, Historical, Ranking, and Distribution.

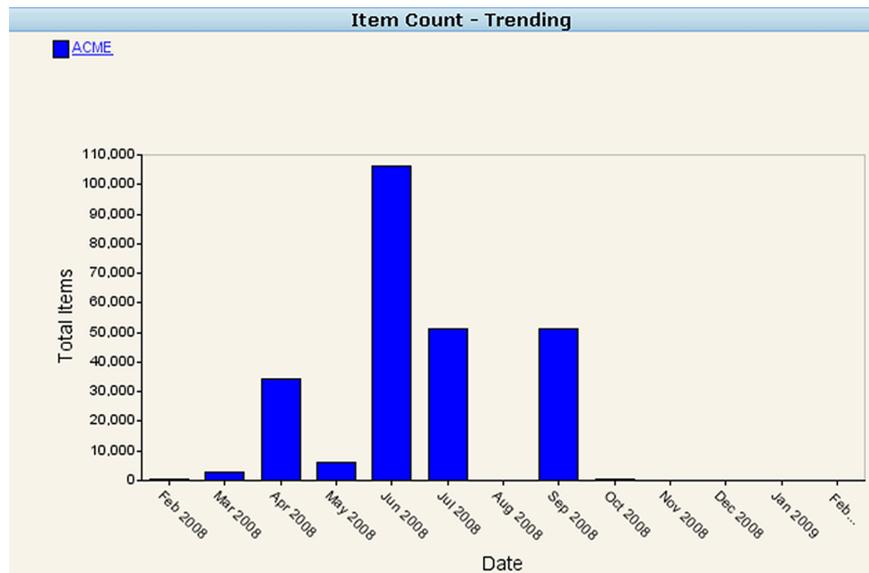
This report provides different drill-down reports depending on the archive report category that you have selected.

The Count of Items report is available in both archive report categories, Exchange and Archive Storage. The drill-down reports vary depending on the archive report category that you have selected.

See [“About archive report categories”](#) on page 406.

[Figure 9-26](#) depicts the sample Count of Items report.

**Figure 9-26** Count of Items report



Click the archive site to determine how many emails were archived in each Exchange Server available in this site.

## About the Archive Window report

This report is available in both archive report categories, Exchange and Archive Storage. Use this report to determine how much of data is being archived in a particular time frame that is archive window.

See [“Generating an archive canned report”](#) on page 410.

The Archive Window report is available only in Historical view.

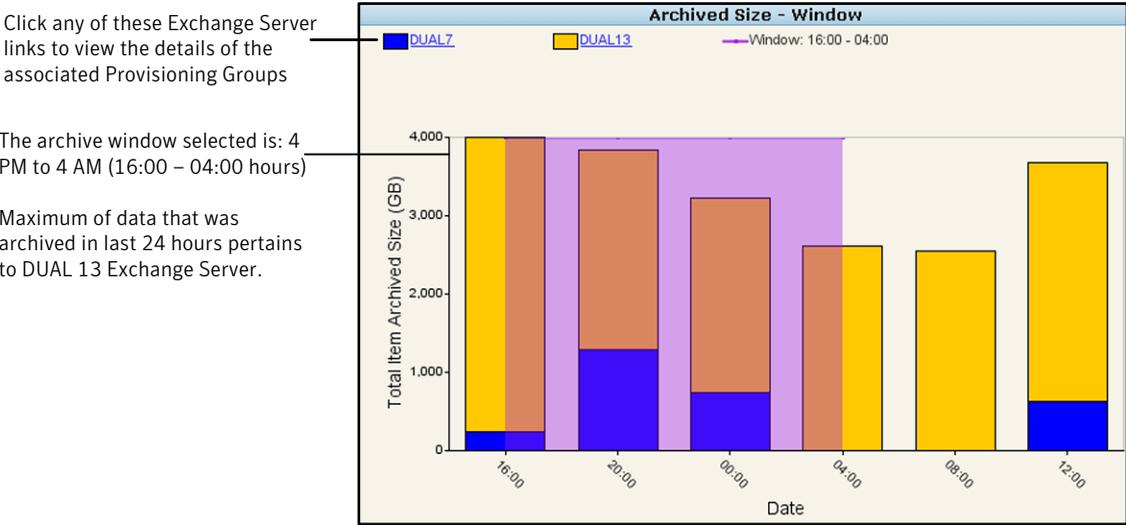
The Archive Window report is available in both archive report categories, Exchange and Archive Storage. The drill-down reports vary depending on the archive report category that you have selected.

See [“About archive report categories”](#) on page 406.

Figure 9-27 depicts how much data was archived during the selected archive window.

Enterprise Vault Server is selected as the Report On parameter and archive window is: 4 PM to 4 AM.

Figure 9-27 Archive Window report



The reports shows that two Enterprise Vault Servers are available: valtsrv04 and valtsrv05. valtsrv04 contains maximum archive data between the two.

During the period of 4 PM to 4 AM that is the selected archive window, maximum emails were archived. This implies that the schedule defined for archival process is appropriate and the archive window is being properly utilized.

Click valtsrv04 or valtsrv05 link to view the details of the Vault Stores associated with the selected Enterprise vault Server. You can further drill-down the Vault Store report to view the details of the Vault Partitions associated with it.

## About the Mailbox Quota report

The Mailbox Quota report displays the top mailboxes in Exchange Server, which have exceeded a particular mailbox size limit. This report is available in the Ranking report view.

See “Generating an archive canned report” on page 410.

There are three types of Mailbox Quota reports:

By Warning Limit	<p>This report shows mailboxes that have exceeded the Warning limit set in Exchange Server.</p> <p>The Warning limit is a limit set for mailboxes, which decides how much data mailboxes can contain.</p> <p>For example: The Warning limit for mailboxes is set to 256 MB. The By Warning Limit report displays all mailboxes that have exceeded 256 MB of data.</p>
By Send Limit	<p>This report shows mailboxes that have exceeded the Send limit set in Exchange Server.</p> <p>The Send limit is a limit set for mailboxes, which is greater than the Warning limit. If size of a mailbox exceeds this limit, emails cannot be sent from this mailbox.</p>
By Receive Limit	<p>This report shows mailboxes that have exceeded the Receive limit.</p> <p>If size of your mailbox exceeds the Receive limit, you cannot receive any emails.</p>

The Mailbox Quota reports are available in the Exchange report category.  
See [“About archive report categories”](#) on page 406.

## About the Original Size Vs Archived Size report

This report provides the comparison between original size and archived size of Exchange Server data. using the report, you can determine how much was the original size of the data that was archived later. The difference between original size and archived size is termed as savings. If the savings are more, it implies that data was archived in a very efficient way and thus, lesser storage space was required.

See [“Generating an archive canned report”](#) on page 410.

The Original Size Vs Archived Size report is available in the Exchange report category.

See [“About archive report categories”](#) on page 406.

Target Server is selected as the Report On parameter.

## About the Target Details report

The Target Details report shows details of all mailboxes in all Exchange Servers in an archive site. The word Target refers to individual mailboxes. The details in the report includes the name of a mailbox, original size of emails in a mailbox

(Item Original Size), archived size of emails (Item Archived Size), number of emails (Target Item Count), and so on.

See [“Generating an archive canned report”](#) on page 410.

The Target Details is available in the Exchange report category.

See [“About archive report categories”](#) on page 406.

Figure 9-28 shows a sample Target Details report.

**Figure 9-28** Target Details report

Tabular - Target Report													
Archive Target	Item Original Size (MB)	Item Archived Size (MB)	Target Archiving State	Target Item Count	Is Enabled for Import	Archive Policy Type	Archive Policy Name	archive Policy Percentage Of Quota	Provisioning Group	Is Provisioning Group Enabled	Retention Name	Category	Retention Period
US_Tex_Sale_494	3.34	3.34	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.42	3.42	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	2.27	2.27	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	2.12	2.12	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	84.17	84.17	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.28	3.28	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.35	3.35	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	1.82	1.82	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.35	3.35	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.40	3.40	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	1.83	1.83	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.33	3.33	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	2.26	2.26	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.30	3.30	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.29	3.29	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	1.82	1.82	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.43	3.43	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	2.34	2.34	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	3.30	3.30	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365
US_Tex_Sale_494	2.13	2.13	1	8	No	3	Default Exchange Mailbox Policy	20	Texas	true	US MBX EXCH DUAL4		365

9378809 Total Rows    Pages: 1 2 3 4 5 6 7 8 9 10 | H

## About the Archived Size report

This report is available only in the Archive Storage report category. Use this report if you want to determine the archived size of the Exchange Server data that was archived. You can determine how much is the size of the Exchange Server data that was archived and has been stored in a specific Vault Store, Enterprise Vault Server, or Vault Store Partition. You can select these filters using the Advanced Filters option on the Report Wizard page.

See [“Generating an archive canned report”](#) on page 410.

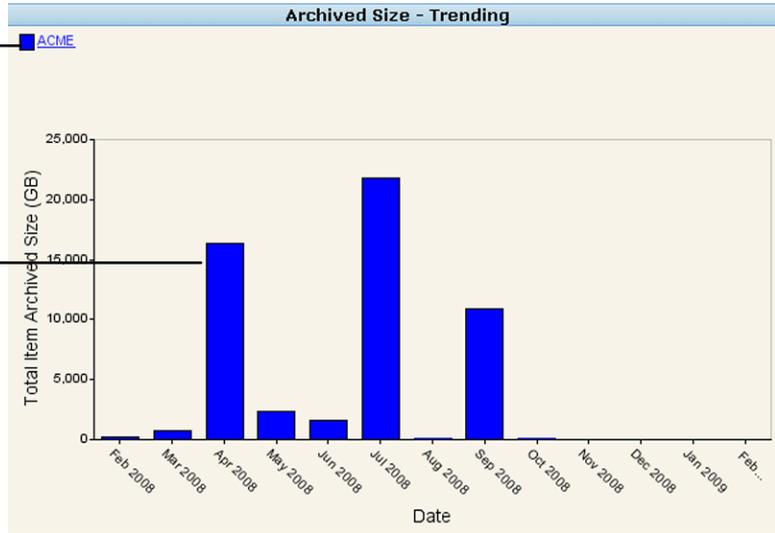
The Archived Size report is available in the Archive Storage report category.

See [“About archive report categories”](#) on page 406.

Figure 9-29 shows a sample Archived Size report in the historical report view. Archive Site is selected as the Report On parameter. Therefore, the drill-down path is: Archive Site > Enterprise Vault Server > Vault Store > Vault Partition. Archive Site is selected as the Report On parameter. The report depicts the data that was archived in the last one year, in an archive site called Acme.

**Figure 9-29** Archived Size report

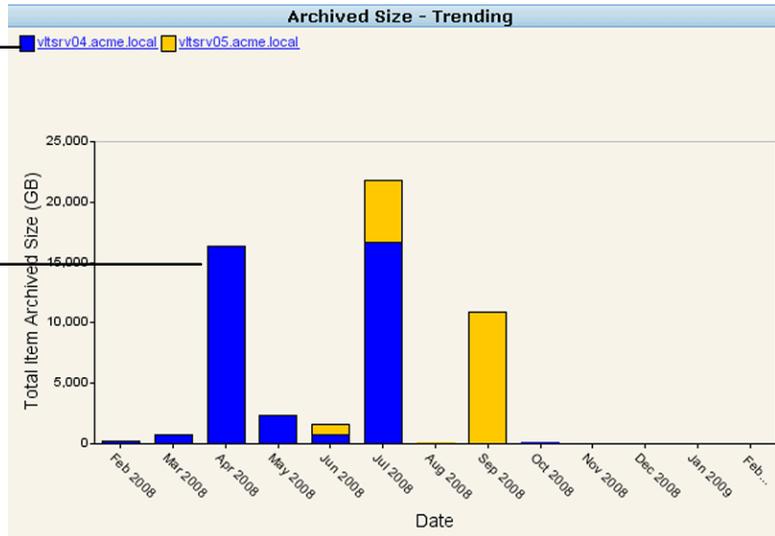
Click this archive site link to view the details of the associated Enterprise Vault Servers



This historical report shows that in the Acme archive site how much data was archived for the last one year.

Click the archive site link to view details about the Enterprise Vault Servers associated with the Acme archive site.

Click any of these Enterprise Server links to view the associated Vault Stores' details

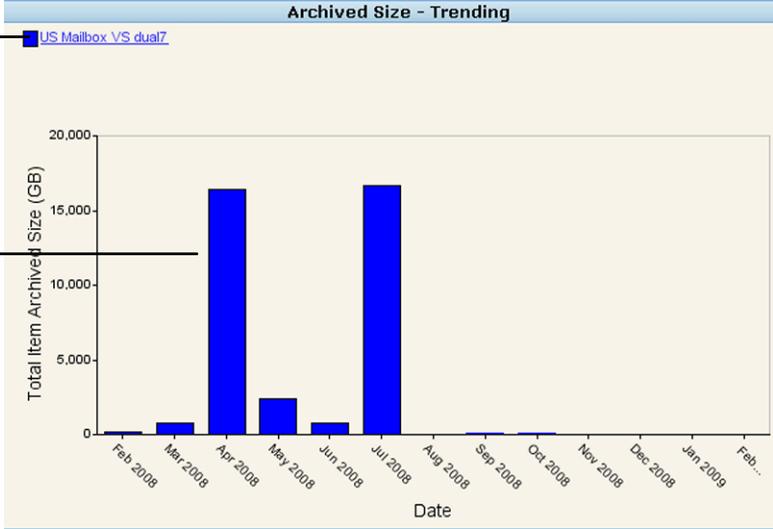


This historical report shows how much data was archived by two Enterprise Vault Servers, vltsrv04 (represented by the blue stack bar) and vltsrv05 (represented by the yellow stack bar) residing in the Acme archive site

The archive site comprises two Enterprise Vault Servers: vltsrv04 and vltsrv05. By clicking any of these Enterprise Vault Server links, you can view the details of the associated Vault Stores.

Click any of these Vault Store links to view the details of the associated Vault Partitions

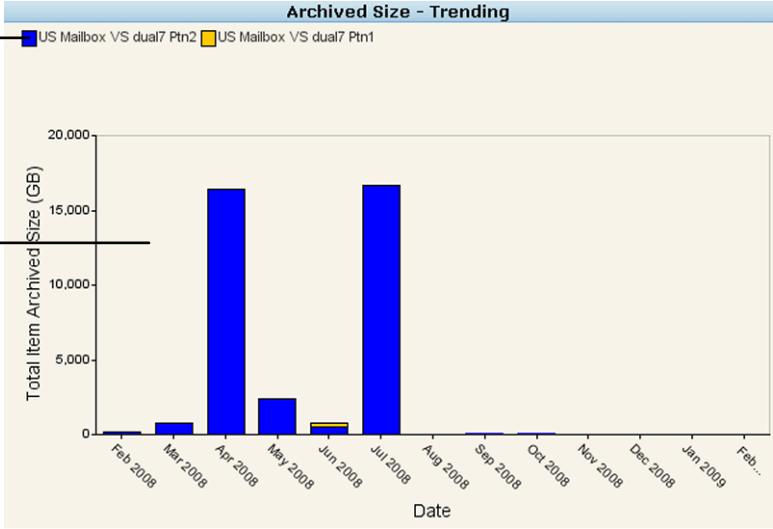
This historical report shows how much of the total archived data was stored in the US Mailbox VS dual7 vault store. This data was archived by the vltsrv04 Enterprise Vault Server



Click a Vault Store link to view the details of the associated Vault Partitions.

US Mailbox VS dual7 vault store comprises these two vault store partitions, where all data that was archived by the vltsrv04 Enterprise Vault Server Was stored.

This historical report shows how much of the total archived data was stored by each of the vault partitions, US Mailbox VS dual7 Ptn1 and US Mailbox VS dual7 Ptn2



The Original Size Vs Archived Size report depicts the difference between the two size of Exchange Server data. The more the difference, the more efficient is your archival process.

See [“About the Original Size Vs Archived Size report”](#) on page 426.



After creating a custom report, you can modify the report, print, save, and email it.

As you work with different report types, the Report Wizard displays different parameters. Many of the parameters are used for multiple report types, and they appear in different combinations for each type.

Before you begin creating custom reports, you should become familiar with the following topics:

- Report types
- Report formats

You can create a custom report by using the parameters that are available in the Custom Report Wizard.

---

**Note:** When you generate a report that correlates two types of data, you may not be able to view the expected data. For example: In a report that contains records correlating Jobs and their Attempts, the Jobs that do not have Attempts data do not appear in the report. Records containing Jobs and related Attempts appear in the report.

---

#### To create a custom report

- 1 Click **Reports > Custom** in the console.
- 2 Click **Custom Report** to start Custom Report Wizard.

**3** On the Select Report Category and Type page, from the Category drop-down list, select one of the following report categories:

Backup Job/Image/Media	Select to view job or image data. The associated filter parameters, such as Job Client or Job Error Code appear.
Backup Log	Select to view backup log data. The associated filter parameters, such as Backup Log Source Host or Agent Server appear.
Backup Media	Select to view Media Server data. The associated filter parameters, such as Media Size or Media ID appear.
Backup Tape Drive	Select to view tape drive data. The associated filter parameters, such as Tape Drive Device Host or Tape Drive Type appear.
Scheduled Jobs	This report category has been added in VBR 6.6. Generate reports on Scheduled Jobs using this category
Archive Target	This report category has been added in VBR 6.6. Using this category you can generate reports to display information of mailboxes / targets that were archived.
Archive Storage	This report category has been added in VBR 6.6. Using this category you can generate reports to display information on archive storage, such as Vault Store or Vault Partition.
Chargeback	Select to view chargeback or cost information. The associated filter parameters appear. To view the chargeback data, you must create cost formulas.
Savings	Select this category to view NetBackup PureDisk savings data. The associated filter parameters appear. To view the savings data, you must create the cost variable with Protected Job Size as the variable metric.
Agent Status	Select to view information specific to the agent. The associated filter parameters, such as Agent Host or Last Heartbeat appear.

**4** Select one of the following from the Report Type drop-down list:

Top ranking	Display data for the leading objects in the specified metric, for example, the hosts with the greatest number of successful backup jobs.
Trending	Display data as a graph that shows fluctuations over time and optionally, projects future trends.
Distribution	Display groupings or objects or resources in a pie chart, a graphical format.
Tabular	Display data in the form of a table.

**5** Click **Next**.

**6** In the second panel of the Custom Report Wizard, select values for one or more report parameters, depending on the report category and type you selected.

As you select parameters, the content pane may refresh to display additional selections. For example, when you select a view filter, you are then given a choice of items on which to filter the report display.

**7** Click **Run**.

**8** To return to the Custom Report Wizard and make changes to the report, click **Edit**.

## About Custom Report Wizard parameters

The Custom Report Wizard displays a set of parameters that varies depending on the report type. The following topics describe all the available parameters:

- Data selection parameters
- Data parameters
- Table columns
- Frame parameters
- Report conditions
- Filter parameters

### About Data Selection parameters

Use the Data Selection parameters to define the report scope.

You can select up to four of the following values:

Data Grouping	<p>The way in which report data is grouped or aggregated.</p> <p>Example: Status groups backup jobs according to their status.</p> <p>Example: Host: OS Type groups hosts according to host platforms such as Solaris and Windows.</p> <p>To use a different grouping from the ones listed, click <b>View Aggregation Level Node</b>, and then select a level from the Aggregate at drop-down list.</p> <p>For example, when reporting data in the Geography category, you can aggregate data at the Top level and the data appears for all servers as a single unit. If you aggregate at a lower level, data displays according to countries, cities, or even individual servers.</p>
Within View	<p>Select an object view category.</p> <p>Object view categories are defined by your system administrator and are the same ones used in the Views area of the console.</p> <p>Examples: Geography, Application</p>
Filter at	<p>Specify the hierarchical level, if any, for filtering the object view category.</p> <p>Examples: Level 1, Level 3</p>
Specific items	<p>When you select a filter, you are given a choice of items on which to filter the report display.</p> <p>Examples (with Geography and Level 2 selected): Japan, Canada</p> <p>Examples (with Line of Business and Level 1 selected): Finance, HR</p>

## About Data parameters

Use the data parameters to define the measurements to be collected for trending, ranking, and distribution reports.

---

**Note:** For ranking reports, the wizard displays data parameters under the heading Rank By. For trending reports, the wizard displays data parameters under the heading Y Axis Properties and enables you to pick two different sets of data to plot.

---

You can select from the following values:

Report On	<p>Define the report's scope using the drop-down lists:</p> <ul style="list-style-type: none"><li>■ The mathematical category Examples: Total, Minimum, Maximum, Average, Percent</li><li>■ The type of data Example: Backup Job Total Size</li><li>■ The backup job group ID (if multi stream jobs are grouped together) Example: BackupGroup1</li></ul>
Top	<p>The number of items to display in the ranking, and the order in which to display them.</p> <p>Available only for Top Ranking type</p> <p>Examples: Top 5 Descending, Top 10 Ascending</p>
Display Unit	<p>For numeric data types, such as Backup Job Total Size, the units in which to display the data.</p> <p>Examples: MB, GB.</p>
Chart Type	<p>The report format. Additional formats may be available depending on the values specified in Report Data.</p>
Target	<p>For trending reports, select the radio button and type a value in the text box to include a target level or threshold in the report display. The target value appears as a horizontal line, useful for making quick visual comparisons between the target value and the actual values being reported.</p>
Alias X-Axis Name or Alias Y-Axis Name	<p>A label for the graph axis that reflects quantity (as opposed to time). For trending reports, this is the vertical (Y) axis. For other reports it is the horizontal (X) axis. If you leave this field blank, a default label is provided.</p>
Report Description	<p>Description to display along with the report. If you leave this field blank, no description is provided by default.</p>

## Populating the table columns

Use the Viewable Columns parameters to establish the column titles for a tabular report.

### To populate the table columns

- 1 From the Available Columns list, select one or more values for table columns, for example, Host Name, Status, Backup Job Group ID.

The following columns are specific to NetBackup PureDisk reports:

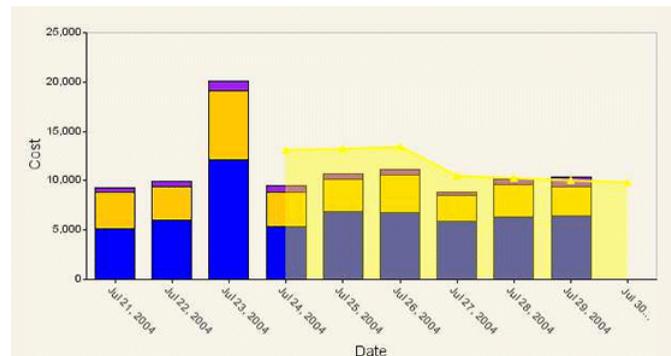
- Backup Job File Count SIS Factor
  - Backup Job File Count SIS Savings
  - Backup Job Pre SIS Size
  - Backup Job Size SIS Factor
  - Backup Job Size SIS Savings
- 2 From the Size Display Unit, select one of the following units:
    - KB
    - MB
    - GB
    - TB
  - 3 From the Duration Display Unit drop-down list, select one of the following time intervals:
    - Seconds
    - Minutes
    - Hours
    - Days
  - 4 From the Table Rows Per Page drop-down list, select number of rows of records that you want to display on one report page.
  - 5 Click **Add**.
  - 6 The columns selected from the Available Columns list are added to the pane, which you can rearrange as you want them to be displayed on reports using the following controls:
    - Sort order
    - Operation
    - Up
    - Down
    - Remove
  - 7 Top: The number of items or objects to appear in the table.  
Example: If the first column is Job Duration, the value 10 displays data for the 10 longest backup jobs in terms of duration

## Specifying trendlines

Use the Trendline and Forecast parameters to establish characteristics that are unique to trending reports. Using these parameters, your report can project future trends by averaging actual data from the recent past.

Figure 9-31 shows the trending report.

**Figure 9-31** Example of a trend report (trendline shown in yellow color)



### To specify trendlines

- 1 In Show trendline with moving average, select the checkbox and use the drop-down list to specify the number of data points to factor into the average.

At each interval on the graph, the trendline shows a moving average of the most recent data points.

Example: 3 displays a trendline that, at each interval, shows the average of the current data point and the two previous data points.

- 2 In Show forecast with forecast periods, check the checkbox and use the drop-down list to specify a number of forecast periods (intervals).

Example: 12 shows forecast data for the next 12 months (if the Group By is 1 month).

## Configuring frame parameters

You use the Time Frame parameters to define the report's overall time frame and the intervals for which data is reported.

---

**Note:** For trending reports, the wizard displays time frame parameters under the heading X Axis Properties.

---

You can select from the following values:

X Axis Type	<p>For trending reports, the metric used to define the graph's horizontal (X) axis.</p> <p>Examples: Backup End Time, Host Name</p>
Alias X-Axis Name	<p>For trending reports, a label for the horizontal (X) axis. If you leave this field blank, a default label is provided.</p>
Group By	<p>For trending reports, the unit of time into which measurements in X Axis Type are grouped.</p> <p>Example: 1 Day groups all measurements by one-day intervals. The default one-day interval runs from midnight to midnight.</p>
Time Basis	<p>The metric used for assigning a time to each item in the report, if not specified by the X Axis Type parameter.</p> <p>Example: The start time or the end time for each backup job.</p>
Time Shift	<p>Moves the starting point for a defined interval (such as minute, hour, day, or month) to one that more closely matches your own operations. Values includes days, hours, minutes, and seconds.</p> <p>Example: 30 seconds shifts the minute interval so that it begins at 30 seconds after the minute rather than exactly on the minute.</p> <p>Example: 14 days shifts the monthly interval so that it begins on the 15th day of the month rather than on the first day.</p> <p>Check <b>Backward</b> to move the starting point backward in time.</p> <p>Example: 6 hours Backward shifts the daily interval to 18:00 to 18:00. (18:00 is equivalent to 6:00 PM.).</p> <p>Use the Day Window value together with Time Shift to shorten the length of the daily interval from 24 hours.</p>
Day Window	<p>Specify the time interval that constitutes one day. Select values from the From and To drop-down lists.</p> <p>Example: 6:00 PM to 6:00 AM</p> <p>Example: 12:00 AM (midnight) to 12:00 PM (noon)</p>

Timeframe	<p>Define the beginning and end of the time interval to be covered by the report. You can choose either absolute dates, meaning that the report's contents remain static whenever you display it, or relative dates, meaning that the report always displays data collected over the most recent time interval.</p> <p><b>Note:</b> The Relative Date setting is especially useful for reports that you plan to generate on a regular basis. Such reports always show data collected over the most recent time interval.</p>
Last	<p>This parameter appears when you select the Relative time frame.</p> <p>Define the period in hours, days, weeks, months, quarters, or years for which you want to view data.</p> <p>Do not select the To Date check box if you want to view data for the entire period specified.</p> <p>For example: Thee current date is 13th April 2007.</p> <p>If you selected the period as 1 Month and not selected the To Date check box, the report shows data from 14th April 2007 to 13th April 2007.</p> <p>If you selected the To Date check box, the report shows data from 1st April 2007 to 13th April 2007.</p>

You can specify absolute or relative time frame for a report.

---

**Note:** If you specify relative time frame and select To Date, the report is configured to display data collected over the interval ending at the current date. This is effectively equivalent to specifying an absolute time frame; the report's contents remain static whenever you display it.

---

For backup history reports, you can have your report display data for the most recent eight-day period (rolling eight-day report). For example, if today is Monday, the display shows data about backup jobs ranging from last Monday through today.

### To configure an absolute time frame

- 1 On a report, click **Absolute Date**.
- 2 Select a start time (month, day, year, and time of day) using the From drop-down lists, and a end time using the To drop-down lists.

Alternatively, use the Unbounded check boxes to indicate an open-ended time interval. The report displays data from the time period between the start and end dates.

Example: From MAR 1 2004 12:00 AM to APR 30 2004 12:00 AM

Example: Unbounded to APR 30 2004 12:00 AM

### To configure a relative time frame

- 1 On a report, click **Relative Date**.
- 2 Select a time interval using the Last drop-down lists. The report displays data collected within the specified time period, up to the current time

Examples: Last 21 Days, Last 2 Quarters

## Defining report conditions

Expand **Conditions** in the Custom Report Wizard window to specify exception conditions for notification. Exception conditions represent potential problems, for example, an unusually high percentage of backup job failures or an unusually low quantity of data being backed up.

## Selecting and using filter parameters

You can use filter parameters to obtain additional filtering capability for the report you want to display. For example, you can filter on the following:

- Host Operating System
- Host Discovered Backup Client

### To specify additional filtering criteria

- 1 In the Custom Reports section, select report category and type. The respective parameters appear in the new Custom Report Wizard window.
- 2 Expand the **Filter** pane.  
The list of criteria depends on the report category and type you selected.
- 3 For each filtering criteria you want to use, check the criteria name, and then specify one or more values using the fields provided.

## Showing or hiding filter parameters

Veritas Backup Reporter provides the option to show or hide the filter parameters as required.

### To show or hide filter parameters:

- 1 On Custom Report Wizard window, click the arrow to expand the Filter pane. The list of filter parameters appears, which depends on the report category and type you selected.

For example, if you have selected Backup Job/Image as a report category, the following filter criteria appear in the Filter pane:

- Backup Job/Image
  - Backup Log
  - Backup Media
  - Backup Tape Drive
  - Chargeback
  - Savings
  - Agent Monitoring
- 2 Click the **Refresh/Get filter** arrow to display all parameters associated with the filter criteria. For example, if you expand Backup Job the parameters, such as Backup Job Size or Backup Job Start Time appear.
  - 3 Click **Hide** to hide all filter parameters. You cannot see the hidden filter parameters on the UI, but the parameter selections remain intact and the report is generated depending on the selected parameters. To reset the parameter selections, click the **Refresh/Get filter** arrow.
  - 4 Click **Show** to again display all filter parameters. You can modify the parameter selections as you want.

### About Agent Monitoring filter parameters

The following filter parameters are available for the Agent Monitoring reports:

Time Since Agent Last Heartbeat	Select the Time Since Agent Last Heartbeat check box to specify the time range in minutes and retrieve the agents that have not sent heartbeats within the specified time range.  Select the Exclude Range check box to invert the time range selection. All agents that have not sent the heartbeats outside the specified time range are retrieved.
---------------------------------	---

Agent Configuration ID	<p>Select the Agent Configuration ID check box to specify the Agent ID range and retrieve the agents that have IDs within the specified range. The Start parameter is a mandatory field, which must be 1 or above.</p> <p>Select the Exclude Range check box to invert the Agent ID range selection. All agents that have IDs outside the specified range are retrieved.</p>
------------------------	--

## Modifying a custom report

You can modify a custom report that you have already created.

### To create a new custom report

- 1 Display a custom report in the console.
- 2 Click **Edit**.  
The second panel of the Custom Report Wizard appears, with parameters for the current report selected.
- 3 Change parameters as needed to create the new custom report.
- 4 Click **Run**.
- 5 To return to the Custom Report Wizard and make more changes, click **Edit**.

## Saving report data

You can save the contents of reports you customized or new reports you created.

After you create or customize a report, you can save it for later viewing or for use in sending notifications to users.

After you create and save reports, you can use them in any of the following ways:

- View saved reports by selecting them from the task pane in the My <Subject> Reports page.
- Add saved reports to a portal page.  
See [“Editing sections on a portal page”](#) on page 345.
- Email saved reports to interested people on a regular basis.
- Trigger alerts to notify staff members of potential problems.

**To save data in a report**

- 1 Create and display a report.  
See [“Creating custom reports”](#) on page 430.
- 2 Click **Save As**.
- 3 On the Save Report page, in the Report Name text box, type a report name.
- 4 From the Save Under drop-down list, select a folder in which you want to save the report.
- 5 From Add to main portal section drop-down list, select a page to add the report to one of the report portal pages, in the .  
See [“Using the reports portal pages”](#) on page 343.
- 6 Select the checkbox to add a line break before the report.
- 7 Select the checkbox to overwrite any existing report that has the same name.
- 8 To schedule reports to be sent as emails, select a scheduled email in the Schedule report for email drop-down list.
- 9 Click **Save**.

## Exporting reports

You can also preserve report data in files or print the data. Veritas Backup Reporter provides two ways of preserving report data in files:

- Export the report you are currently viewing in the console window, using the procedure in this section.
- Arrange for a report to be archived at regularly scheduled intervals.

In both instances, the report data is exported to a file in either CSV (comma-separated values), TSV (tab-separated values), XML, or HTML format. You can then open the file using other applications, like a spreadsheet program or a text editor.

**To export a report**

- 1 Open a report in the console.
- 2 Click **Export to File**.
- 3 In the Export Report Options dialog box, in the Name field, type a name for the export operation.

The name should be descriptive enough that you can click it from a list.

- 4 Click **Enabled** to activate the export operation.  
Report data is exported at the next scheduled interval. (Cancel the selection if you want to defer the export operation until later.)
- 5 From the Schedule drop-down list, select a schedule.  
The schedule determines the time and days on which report data is exported.
- 6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
- 7 Select one of the following export file formats:

XML	Can be imported (using user-written scripts) by other programs like databases or billing applications.
CSV (comma-separated)	Use with spreadsheet programs.
TSV (tab-separated)	Compatible with word-processing applications and text editors.

The format you choose depends on how you want the data to be displayed and manipulated.

- 8 Click **Export**.
- 9 If prompted, specify whether you want to open the file or save it on your computer's file system.

## Printing reports

You can print the report you are currently viewing in the console window.

### To print a report

- 1 Display a report in the console.
- 2 Click **Print**.
- 3 In the Print dialog box, select a printer and adjust printer settings as required.
- 4 Click **Print**.

## Using custom SQL queries

In Veritas Backup Reporter, you can generate tabular reports by directly running SQL queries using the Custom Queries functionality. You can save or export the report using the available export options.

---

**Note:** Only administrator can access the Custom Queries functionality.

---

The Custom SQL Queries function lets you create and run custom queries and view related backup data. You can also save your custom queries that you plan to run frequently.

You can also run SQL queries from a command-line interface, using the `runstoredquery` utility.

`runstoredquery`

## Creating SQL queries

You can use the Custom SQL Queries tool to create and save database queries.

### To create a database query

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **Create New Query**.
- 3 On the Add Query screen, type the following:

Title	Enter the query title, for example UpdateQuery.
Category	Enter an existing or a new query category, for example, Backup Reports. If the category you specify does not exist, Veritas Backup Reporter creates a new category with that name. To add a new query under an existing category, you must type the category name exactly as it appears in the table of saved database queries.
Out File (optional)	Enter the directory path and name of the file in which results of the SQL query are stored.
SQL Statement	Enter the SQL query, for example: <pre>SELECT * FROM EVENTS WHERE LOCATION = 'TORONTO' AND STATE = 'RUNNING'</pre>
Description	A detailed description of the query, for example Events that are running on Toronto hosts.

- 4 Click **Add** to save the new query.

## Running SQL queries

You can run an existing or a saved SQL query or you can run an instant query without saving it. When you run a saved or an instant query, the output is displayed in a tabular report. You can perform the following operations on this report same as on any other report:

- Email
- Save
- Print
- Export

---

**Note:** The **Edit** link on a custom SQL query report lets you edit the related SQL query. You need to again run the modified query to view the changes in the report.

---

### To run a saved database query

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **All Saved Queries**.
- 3 Select the title of the query you want to run.

### To run an instant database query

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **Run Query**.
- 3 On the Run Query screen, enter the following information:

Title of Query	Enter the query title, for example UpdateQuery.
SQL Statement	Enter the SQL query, for example: <pre>SELECT * FROM EVENTS WHERE LOCATION = 'TORONTO'AND STATE = 'RUNNING'</pre>

- 4 Click **Run It**.

## About the options on Custom SQL query report

When you run a saved or an instant query, the output is displayed in a tabular report. The following options are available on a custom SQL query report.

Edit	Click to modify the related SQL query.
Email	Click to email the report.
Print	Click to print the report.
Export to File	Click to export the report in the available formats.
Save As	Click to save the report.
Output to HTML file	Click to save the output of a SQL query in the HTML format.
Output to comma delimited file	Click to save the output of a SQL query in the csv (comma separated value) format.
Output to text file	Click to save the output of a SQL query in a text file.

## Modifying saved SQL queries

You can modify existing SQL queries. You can also create new queries by copying or cloning existing queries and changing some of their attributes.

### To modify a saved database query

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **All Saved Queries**.
- 3 Click the **Modify** link corresponding to the query you want to modify, or select the ID of the query.
- 4 On the Modify Final Test screen, modify the field values.
- 5 To configure the query to prompt for user input when it runs, select one or more check boxes in the Prompt For area.
- 6 Do one of the following:
  - To create a new query and preserve the original query without modifications, click **Clone**.
  - To modify the original query, click **Modify**.  
If you click **Clone** without modifying the query name, the new copy of the query is saved as 'Copy of <QueryName>', where <QueryName> is the name of the original query.  
You can change this name by opening the Modify Final Test screen for the new copy.

## Viewing the list of saved SQL queries

You can view all saved database queries from the Veritas Backup Reporter console.

### To view saved database queries

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **All Saved Queries**.

## Deleting SQL queries

You can delete the SQL database queries that you no longer want. Deleting a saved query removes it permanently from the Veritas Backup Reporter database.

### To delete a saved query

- 1 In the Veritas Backup Reporter console, click **Report > Custom > Custom Queries**.
- 2 Click **All Saved Queries**.
- 3 Click the **Delete**.
- 4 On the confirmation message box, click **OK**.

## About reporting on restore jobs

Veritas Backup Reporter provides reports pertaining to restore jobs that are scheduled for a master server. You can view these reports in the **Reports > Custom > Custom Queries > All Saved Queries** section on the Veritas Backup Reporter UI. You can save these reports.

You can modify the associated SQL query.

Veritas Backup Reporter provides the following restore job reports:

Weekly Restore Job by Master Server	<p>This report shows the details about restore jobs that are run for a master server. The following details are displayed:</p> <ul style="list-style-type: none"><li>■ Master Server - Name of the master server</li><li>■ Restore Request Time - Difference in time (in weeks) between the executions of backup job and restore job</li><li>■ Count of Restore Jobs - Number of restore jobs scheduled for a master server</li></ul>
-------------------------------------	---

With these restore job details, you can derive the restore request trend that helps you set your data retention period.

**Average Image Retention Time Vs Restore Request Time** This report shows the average image retention period and restore request time with respect to a master server. The following details are displayed:

- Master Server - Name of the master server
- Average Image Retention Time - Average value of image retention periods
- Average Restore Request Time - Average value of restore request time

Restore request time is the difference in time between the executions of backup job and restore job

With these average values, you can derive the restore request trend that helps you set your image retention period.

**Weekly Restore Job by Applications** This report shows which applications cause maximum restores. This is a weekly report. The following details are displayed:

- Application - Name of application that was restored, for example Oracle
- Policy Type - Name of policy set in NetBackup, for example Standard or Oracle
- Restore request time (weeks) - Difference in time (in weeks) between the executions of backup job and restore job
- Count of Restore Jobs - Number of jobs that were run to restore applications



# Managing cost analysis and chargeback for services

This chapter includes the following topics:

- [About generating cost reports](#)
- [Estimating baseline \(chargeback\) costs](#)
- [Creating cost variables](#)
- [Modifying cost variables](#)
- [Managing cost formulas](#)
- [Generating a cost report](#)
- [Viewing a cost report with the currency of your choice](#)
- [Generating savings reports](#)

## About generating cost reports

Veritas Backup Reporter provides organizations with a tool to evaluate the cost of the IT services they consume, the Veritas Backup Reporter chargeback feature. You can create cost variables and formulas that enable you to run reports that show costs for different levels of your organization.

For example, a financial officer can run cost reports to do the following:

- Determine which divisions of the organization are the largest consumers of data recovery services
- Perform a cost-benefit analysis that compares different backup schedules
- Project future IT costs for budget planning

Using the chargeback feature in Veritas Backup Reporter, you can charge the organizations or IT departments based on the following aspects:

- Number of jobs that are backed up (Job Count)
- Size of jobs that are backed up (Job Size in GB)
- Media space that is occupied by the backup data (Daily Occupancy in GB)
- Size of jobs that are protected (Protected Job Size in GB)

---

**Note:** For generating NetBackup PureDisk savings reports, you must create a cost variable with the Protected Job Size (GB) metric.

See [“Generating savings reports”](#) on page 465.

---

You can do the following to generate cost reports:

- Create variables for assigning costs to the service types.  
To reflect changes in the rates for specific services, Veritas Backup Reporter offers the flexibility of creating more than one variable for a service type or of including more than one rate in a single variable.  
See [“Creating cost variables”](#) on page 455.
- Create formulas that apply one or more of these variables to determine the cost of a service.  
For example, you can create a Backup Service formula that uses two variables: cost per backup job and cost per backed-up GB. When you run a report using the formula, the report calculates both costs and represents the total in its graphical display.  
See [“Managing cost formulas”](#) on page 458.
- Generate a cost report.  
See [“Generating a cost report”](#) on page 460.

## Estimating baseline (chargeback) costs

The Formula Modeling Tool offers an easy way for you to estimate baseline rates for the IT services you provide. Using historical data, it provides you with an estimate of how much it costs your organization to provide a specific kind of service.

For example, suppose you anticipate spending \$500,000 over the next year to provide backup services throughout your enterprise. By inserting the metric Daily Occupancy into the tool, along with the amount \$500000, you can obtain an estimate per kilobyte that is based on the backup activity you performed last year.

**To estimate baseline (chargeback) costs using the Formula Modeling Tool**

- 1** On the console Costs tab, click **Formula Modeling Tool**.
- 2** Use the following Report Grouping parameters to define the model's scope:

Within View	Select a view category. Examples: Geography or Application
Filter at	Specify a parameter to filter the view category you have selected. Examples: Level 1, Country
Specific items	Select one or more individual items to filter the report. For example: If you have selected Geography as a view category, you can select Asia, Europe, or North America to filter the report.

- 3** Use the following Metric Selection parameters to specify the metric whose rate you want to estimate:

Select Metric	Select a metric, or category of service. Example: Daily Occupancy
Enter Amount	Specify the total amount of money, in dollars, you expect to charge for service within that category in a given time frame. Examples: \$50000, \$10000, or \$10000.00

- 4** Use the following Time Frame parameters to define the time intervals for which data is modeled:

Group By	The unit of time to be covered by your estimate. Example: 1 Day - Provides a cost estimate per day. The default one-day interval runs from 12:00 A.M. to 12:00 A.M.
----------	--

Time Shift	<p>Moves the starting point for a defined interval (such as minute, hour, day, or month) to one that more closely matches your own operations. Select a value from each of the drop-down lists: days, hours, minutes, and seconds.</p> <p>Example: 30 seconds shifts the minute interval so that it begins at 30 seconds after the minute rather than exactly on the minute.</p> <p>Example: 14 days shifts the monthly interval so that it begins on the 15th day of the month rather than on the first day.</p> <p>Check <b>Backward</b> to move the starting point backward in time.</p> <p>Example: 6 hours Backward shifts the daily interval from 12:00 A.M. to 12:00 A.M. to 6:00 P.M. to 6:00 P.M.</p> <p>Use the <b>Day Window</b> value together with <b>Time Shift</b> to shorten the length of the daily interval from 24 hours.</p>
Day Window	<p>Specifies the time interval that constitutes one day. Select values from the From and To drop-down lists.</p> <p>Example: 6:00 P.M. to 6:00 A.M.</p> <p>Example: 12:00 A.M. (midnight) to 12:00 P.M. (noon)</p>

**Timeframe** Defines the beginning and end of the time interval to be covered by the estimate. You can choose either absolute dates, meaning that the estimate's contents remains static whenever you display it, or relative dates, meaning that the estimate always reflects data collected over the most recent time interval.

Select one of the following:

- Click **Absolute** to configure an absolute time frame. Then select a start time (month, day, year, and time of day) using the From drop-down lists, and a stop time using the To drop-down lists. (Alternatively, use the Unbounded check boxes to indicate an open-ended time interval.) The estimate reflects data from the time period between the start and end dates.

Example: From MAR 1 2004 12:00 A.M. to APR 30 2004 12:00 A.M.

Example: Unbounded to APR 30 2004 12:00 A.M.

- Click **Relative** to configure a relative time frame. Then select a time interval using the Last drop-down lists. The estimate reflects data collected within the specified time period, up to the current time.

Examples: Last 21 Days or Last 2 Quarters

The Relative setting is especially useful for estimates that you plan to generate on a regular basis. Such estimates always reflects data collected over the most recent time interval.

- 5 Expand the Filter section at the bottom of the Formula Modeling Tool window to select additional filtering criteria for the model.

The list of criteria depends on the metric you have selected.

Following are some examples of the ways in which you can filter the model:

- Host Discovered Backup Client
- Host Operating System

- 6 Click **Next**.

- 7 Click **Back to Formula Modeling Tool** to input different values into the model, or to run a new model.

## Creating cost variables

Cost reports in Veritas Backup Reporter are based on user-defined variables that define the cost of various services.

Typically, each service is represented by one variable that reflects the cost of the service, for example \$1.00 per backup job. However, you can account for rate changes in one of two ways: by creating two variables for the same service (which you can include in a single cost formula later) or by incorporating both rates into a single variable. For example, a single variable can incorporate the rate of \$1.00 per backup job until 31 December 2004 and the rate of \$1.25 per backup job starting on 1 January 2005.

---

**Note:** To generate PureDisk savings reports, you must create a cost variable with the Protected Job Size (GB) metric.

---

To set up Veritas Backup Reporter to run cost reports, you need to create the variables that define the cost of various services.

**To create a cost variable**

- 1 On the console Costs tab, click **Step 1 - Create Cost Variables**.
- 2 In the content pane, click **Create** at the top of the list.
- 3 In the Create Cost Variables dialog box, type a name for the variable in the Variable Name field.
- 4 Select a metric from the Variable Metric drop-down list, for example Job Count or Job Size (GB).

For generating NetBackup PureDisk savings reports, you must create a cost variable with the Protected Job Size (GB) metric.

- 5 If necessary, select additional parameters to refine the metric you selected. For Backup Job Count and Backup Job Size, select the following:

Job Type	Measure costs for a specific type of job, for example Backup or Restore. The default is Archive.
Job Policy Type	Measure costs for jobs that use a specific policy type. In NetBackup, the policy type determines the type of clients that can be part of the policy and, in some cases, the types of backups that can be performed on the clients. Examples include DB2, Sybase, and MS-Exchange-Server. The default policy type is Standard.
Job Transport Type	Measure cost for a specific transport type for example, LAN (Local Area Network) or SAN (Storage Area Network).
Job Storage Type	Measure cost for a specific storage type for example, tape or disk. Veritas Backup Reporter supports NetBackup's disk-based data protection feature, which enables you to select disk as a storage type, while creating a cost variable.

- 6 Add one or more date ranges and associated rates using the drop-down lists for Month, Day, Year, and Time and by typing a cost per service unit (such as backup jobs or backed-up GB) in the Rate field.

You only need one date range.

- 7 Optionally, to add more date ranges, click **Add New Range**.

This can be useful for defining multiple date ranges to represent historical—or future—changes in service costs. You can also modify the variable later to add or delete date ranges as costs change.

- 8 Click **Save Variable**.

You can now use the variable you created to build formulas that form the basis for cost reports.

See [“Creating cost formulas”](#) on page 458.

## Modifying cost variables

You can update cost variables and formulas without having to recreate the reports that rely on them. For example, you can modify the name, date ranges and rates of a variable to reflect changing conditions in your enterprise.

You can also delete variables you no longer need. Deleting a cost variable removes it permanently from the database, and you must update any formulas that use the variable. To restore a deleted variable, you must recreate the variable manually.

#### To modify a cost variable

- 1 On the console Costs tab, click **Step 1 - Create Cost Variables**.
- 2 Click **Edit** to the right of the variable name.
- 3 In the Edit Cost Variable dialog box, do any of the following:
  - Change the variable's name by typing over text in the Variable Name field.
  - Change the variable's metric by selecting a different value in Variable Metric drop-down list.
  - Change date ranges and rates by replacing values in the various fields, or by using the Add New Range and Delete Selected buttons to add and delete date ranges.
- 4 Click **Save Variable**.

## Managing cost formulas

Based on cost variables you can create cost formulas, using which you can generate cost reports.

### Creating cost formulas

After you create cost variables, create formulas that define the cost of various services to run cost reports.

#### To create a cost formula

- 1 On the console Costs tab, click **Step 2 - Create Cost Formula**.
- 2 In the content pane, click **Create** at the top of the list.
- 3 In the Create Cost Formulae dialog box, type a name for the formula in the Formula Name field.
- 4 Add one or more cost variables to the formula.  
You only need to specify one variable to create the formula.

- 5 Optionally, to define formulas containing more than one variable, click **Add New Variable**.

You can also modify the formula later to add or delete variables and date ranges as the cost of the service changes.

- 6 Click **Save Formula**.

You now can use the formula to create cost reports with which you can evaluate the cost of services and make decisions about what to charge for performing those services.

See [“Generating a cost report”](#) on page 460.

## Modifying cost formulas

You can modify the name and variables of a cost formula that you have created.

You can update chargeback formulas without having to recreate the reports that rely on them. For example, you might want to update a formula called `RecoveryRate` to reflect a change in the hourly rate charged for recovery operations.

### To modify a cost formula

- 1 On the console Costs tab, click **Step 2- Create Cost Formulas**.
- 2 The content pane displays a list of cost formulas defined on the Server. The formulas are listed in alphabetical order.
- 3 In the content pane, click **Edit** to the right of the formula name.
- 4 In the Edit Cost Formula dialog box, do one or more of the following:
  - Change the formula’s name by typing over text in the Formula Name field.
  - Change variables and the factors associated with them by replacing values in the various fields, or by using the Add New Range and Delete Selected buttons to add and delete variables.
- 5 Click **Save Formula**.

## Deleting a cost formula

You can also delete formulas you no longer need. Deleting a cost formula removes it permanently from the database. To restore a deleted formula, you must recreate the formula manually.

#### To delete a cost formula

- 1 On the console Costs tab, click **Create Cost Formulas**.
- 2 In the content pane, check the checkbox next to the name of the formula you want to delete.
- 3 Click **Delete** at the top of the list.
- 4 In the confirmation message, click **OK**.

## Generating a cost report

Using cost variables and formulas you have defined, you can generate reports about backup and recovery operations. The Report Wizard guides you through the process of generating reports.

#### To generate a cost report

- 1 On the console Costs tab, click **Step 3 - Generate Cost Reports**.
- 2 On the My Cost Reports page, select a report type and format in the task pane (for example Costs - Rankings).
- 3 In the Report Wizard, select an object view category from the drop-down list in the Within View field.
- 4 Select the view level you want the report to display from the drop-down list in the Aggregate at field.

For example, when reporting on the Client Count view, you could aggregate data at the Top level (in which case the report displays data for all servers as a single unit) or at the Client level, in which case the report displays data for each client individually.

- 5 Filter the report results by objects, in the Filter text box.

Select the view level and then, in the Select specific items text box, select the relevant report objects.

The objects in the list box may be real objects such as hosts and file systems, or user-created nodes in the view, depending on the view level at which you set the filter.

- 6 Set the report time frame by doing one of the following:
  - Click **Relative Date** to configure a relative time frame. Then select a number of hours, days, weeks, months, or years using the drop-down lists in the Show Last field.

- Click **Absolute Date** to configure an absolute time frame. Then select a start date using the drop-down lists in the From field, and a end date using the drop-down lists in the To field.  
 If you plan to save reports for later viewing or for scheduled distribution by email, it is best to choose a relative time frame, so that the report always represents the most recent data relative to the time the report is accessed or emailed.
- 7 Define the parameter options when you select the report format in 2.
  - 8 Select a cost formula from the Choose Cost Formula drop-down list.
  - 9 The Choose Currency Symbol option is available if you have selected the Display Option in Wizard check box while selecting the default currency.

Report Grouping	
Report on:	Master Server ▾
Within View:	None ▾
Report Time Frame	
<input checked="" type="radio"/> Relative Date <input type="radio"/> Absolute Date	
Show Last:	2 ▾ Week(s) ▾
Display Options	
Display Top Rankings:	10 ▾ Descending ▾
Alias X-Axis Name:	<input type="text"/>
Report Description:	<input type="text"/>
Cost Options	
Choose Cost Formula	: F1 ▾
Choose Currency Symbol:	United States (English) \$/USD ▾
<a href="#">Show Advanced Filters ▸</a>	
<input type="button" value="Run"/> <input type="button" value="Cancel"/>	

See “[Setting the default currency](#)” on page 464.

- 10 Select the currency from the Choose Currency Symbol drop-down list. The chargeback is calculated depending on the currency you selected.
- 11 Click **Run**.  
 The report appears, showing the cost for the specified service, as defined by the formula you selected, over the specified time frame.
- 12 To make changes to the report (for example, adjusting the time frame or the filtering level), click **Edit**.  
 The Report Wizard appears. You can save the cost report for later use.

## Viewing a cost report with the currency of your choice

In Veritas Backup Reporter, you can set the currency that you want to appear on cost reports. The Veritas Backup Reporter administrator can set multiple global currencies, one of which can be set as the default currency.

You also have the option to overwrite this default currency while generating cost reports, provided you have selected the Display Option in Wizard check box while setting the default currency. You can view the cost reports with the currency of your choice.

---

**Note:** Setting the default currency gives you the flexibility to display the cost report values in the currency of your choice. However, Veritas Backup Reporter does not support conversion of currencies while generating cost reports.

---

[Table 10-1](#) provides the steps to execute to view a cost report with the currency that you want to be displayed.

**Table 10-1** Viewing a cost report with the currency of your choice

Step number	Step	Reference topic
1	Set global currencies using the Global Settings section. Navigate as follows: <b>Settings &gt; Global Settings &gt; Global Currency</b>	See <a href="#">“Setting global currencies”</a> on page 463.
2	Set one of the global currencies as the default currency using the User Settings section. Navigate as follows: <b>Settings &gt; User Settings &gt; User Currency Settings</b>	See <a href="#">“Setting the default currency”</a> on page 464.
3	Select the Display Option in Wizard check box to have the option of overwriting the default currency, while generating cost reports. Navigate as follows: <b>Settings &gt; User Settings &gt; User Currency Settings</b> <b>Note:</b> If you do not select the Display Option in Wizard check box, the cost values in the chargeback reports use the default currency that you have set.	See <a href="#">“Setting the default currency”</a> on page 464.

**Table 10-1** Viewing a cost report with the currency of your choice (*continued*)

Step number	Step	Reference topic
4	<p>While generating a cost report, select the currency from the Choose Currency Symbol drop-down list. The chargeback is calculated depending on the currency you have selected.</p> <p><b>Note:</b> The Choose Currency Symbol option is available if you have selected the Display Option in Wizard check box while setting the default currency. All the global currencies are available in the Choose Currency Symbol drop-down list.</p>	See <a href="#">“Generating a cost report”</a> on page 460.

## Setting global currencies

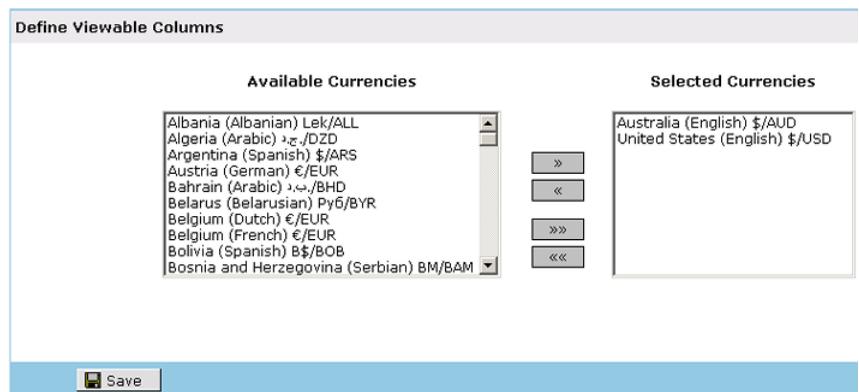
This section provides the procedure to set global currencies, one of which you can set as the default currency.

See [“Setting the default currency”](#) on page 464.

### To set the global currencies

- 1 In the Veritas Backup Reporter console, click **Settings > Global Settings > Global Currency**. The following page is displayed.

 **Select the currencies that will be available in the application**



- 2 On the Define Viewable Columns page, from the Available Currencies list box, select the currencies.

- 3 Click the right arrow. Use the arrow keys to add or remove currencies from the Selected Currencies list box. If you have already saved a currency, you cannot remove it from the Selected Currencies list box.
- 4 Click **Save**.

## Setting the default currency

In Veritas Backup Reporter, you can choose the currency you want to be displayed on cost reports. The Veritas Backup Reporter administrator can set multiple global currencies, one of which can be set as the default currency.

See [“Setting global currencies”](#) on page 463.

You also have the option to overwrite this default currency while generating cost reports.

See [“Generating a cost report”](#) on page 460.

The default currency that you have set is displayed with the cost report values.

---

**Note:** Setting the default currency gives you the flexibility of displaying cost report values in the currency of your choice. However, Veritas Backup Reporter does not support conversion of currencies.

---

### To set the default currency

- 1 In the Veritas Backup Reporter console, click **Settings > User Settings > User Currency Settings**. The following page is displayed.

**Set Default Currency**

Default Currency: United States (English) \$/USD

Currency Code(USD) or Currency Symbol(\$):  
 Currency Code  
 Currency Symbol

Display Option in Wizard:

**Save**

- 2 On the Set Default Currency page, in the Default Currency drop-down list, all global currencies that are set by the administrator are available for selection. Select a currency from the drop-down list.  
See [“Setting global currencies”](#) on page 463.
- 3 Select currency code or symbol. For example, for the currency US dollar, you can either select a currency code USD or symbol \$, which is displayed on chargeback reports.

- 4 Select the Display Option in Wizard check box to have the option of overwriting the default currency you have selected from the Default Currency drop-down list, while generating cost reports. If you do not select this check box, the cost values in the chargeback reports use the currency you have selected from the Default Currency drop-down list.  
  
See [“Generating a cost report”](#) on page 460.
- 5 Click **Save**.

## Generating savings reports

Savings reports are specific to NetBackup PureDisk backup product. The savings reports are saved in the Costs section.

Veritas Backup Reporter data collection from NetBackup PureDisk in addition to other backup products, such as BackupExec, NetBackup, or Tivoli Storage Manager. The Single Instance Storage (SIS) or deduplication technology of PureDisk can identify files and data segments that contain identical data and treats them as a single instance of the file, which it backs up only once.

For example, NetBackup has backed up 100 MB data, in which 20 MB of data is duplicate or identical. PureDisk protects the same data but eliminates the duplicacy using deduplication. Therefore, the data protected is 100 MB, but the actual data backed up by PureDisk is 80 MB, as 20 MB of data is duplicate data. This results in saving 20 MB of data. In other words, PureDisk saved 20 MB of data using deduplication. You can generate savings reports that show the amount you have saved using deduplication.

---

**Note:** For generating NetBackup PureDisk savings reports, you must create a cost variable with the Protected Job Size (GB) metric.

---

### To generate a savings report

- 1 On the console Costs tab, click **Step 3 - Generate Cost Reports**.
- 2 Select a report type and format in the task pane (for example Savings - Rankings).
- 3 In the Report Wizard, from the Report on drop-down list, select a report field.
- 4 Select an object view category from the drop-down list in the Within View field.
- 5 In the Filter text box, filter the report results by objects.
- 6 Set the report time frame by doing one of the following:

- Click **Relative Date** to configure a relative time frame. Then select a number of hours, days, weeks, months, or years using the drop-down lists in the Show Last field.
- Click **Absolute Date** to configure an absolute time frame. Then select a start date using the drop-down lists in the From field, and a end date using the drop-down lists in the To field.

If you plan to save reports for later viewing or for scheduled distribution by email, it is best to choose a relative time frame, so that the report always represents the most recent data relative to the time the report is accessed or emailed.

- 7 Select display options.
- 8 Select a cost variable from the Choose Cost Variable drop-down list.  
Cost variables of only Protected Job Size (GB) metric are available for the selection.
- 9 The Choose Currency Symbol option is available if you selected the Display Option in Wizard check box while selecting the default currency in the User Settings section. Select the currency from the Choose Currency Symbol drop-down list. The savings amount is calculated depending on the currency you selected.
- 10 Select Percentage Savings or Absolute Savings as required.
- 11 Select advanced filter by clicking on the **Show Advanced Filters** link.
- 12 Click **Run**.

# Performance tuning

This chapter includes the following topics:

- [Setting the max heap size](#)

## Setting the max heap size

In order to accommodate for additional Web applications along with Veritas Backup Reporter, you can increase the max heap size. On a production server, the max heap size can be set up to the recommended maximum values. For Windows, you can set the max heap size equal to or less than 1024 MB. On Solaris, you can set the max heap size equal to or less than 2560 MB.

On machines other than production servers, the max heap size can be set to 512 MB, or even to 1024 MB if there is enough physical RAM to support the configuration.

---

**Warning:** The VBR installer automatically sets the max heap size to 1024 MB. If your system requires a lesser max heap size to properly run all applications, set the max heap size to 512 MB.

---

**To set the max heap size**

- 1** Navigate to the following directory:

```
VRTSweb/bin
```

- 2** Run the following command to determine the existing size of your max heap:

```
webgui maxheap
```

- 3** Run the following command to increase the size of the max heap:

```
webgui maxheap 1024
```

You can set the max heap size to the value you want; the argument for the `webgui` command is in megabytes.

# Resolving Veritas Backup Reporter issues

This chapter includes the following topics:

- [Troubleshooting Veritas Backup Reporter issues](#)
- [About contacting the Veritas Backup Reporter support team](#)

## Troubleshooting Veritas Backup Reporter issues

This chapter provides you with the following troubleshooting information that you require in case of any issues while using the Veritas Backup Reporter application.

- [About troubleshooting Veritas Backup Reporter console issues](#)
- [About Veritas Backup Reporter log files](#)
- [About Veritas Backup Reporter status codes and recommended troubleshooting steps](#)
- [Gathering troubleshooting data with the support script](#)

### About troubleshooting Veritas Backup Reporter console issues

This section explains how to troubleshoot issues related to the Veritas Backup Reporter console such as logging in and viewing reports or other information.

#### About troubleshooting login issues

[Table 12-1](#) explains how to fix issues associated with logging on to the Veritas Backup Reporter.

**Table 12-1** Login issues

issues	Explanation	Recommended action
Users cannot log in to the console because the Domain drop-down list is blank.	The Veritas Backup Reporter Management Server host (Windows) is not configured with a fully-qualified domain name.	Check the configuration for the Server host and assign a fully-qualified domain name. For details, see Windows documentation.
Users cannot log on to the console because the Domain drop-down list is blank.	The Veritas Backup Reporter Management Server host (Windows) is not configured properly in Domain Name Service (DNS).	Check the configuration for the server host and ensure that it has a valid DNS name. For details, see Windows documentation.

## About troubleshooting viewing and reporting issues

[Table 12-2](#) explains how to fix issues associated with viewing information about backup resources and generating reports.

**Table 12-2** Viewing and reporting issues

issues	Explanation	Recommended Action
Status information and other data are not being updated for a NetBackup host.	The host alias may not match the name by which the host is known to the NetBackup explorer.	If necessary, change the host alias to match the name with which the explorer is attempting to collect data from the host.
A graphical report displays a legend but does not display the report itself.	If too many objects are defined for the report, the report cannot display.	Using the Report Wizard, change the number of objects in the report display. Do this by aggregating at a higher level, by using a filter, or by selecting specific objects within the report's scope.  Refer to the Reporting on backup and archive data section for more information about specifying the report scope and time frame.

**Table 12-2** Viewing and reporting issues (*continued*)

issues	Explanation	Recommended Action
Selecting links in the console produces no result.	Some links in the console open a new browser window. Pop-up blocker software can block this.	If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the Veritas Backup Reporter Management Server.
Running any graphical report from Veritas Backup Reporter throws a 'javax.servlet.ServletException' in Windows environment.	The Veritas Backup Reporter installation modified the PATH environment variable. The PATH environment variable does not take effect until the Veritas Backup Reporter Management Server reboots.	Reboot the Veritas Backup Reporter Management Server.
You encounter a decrease in View Builder performance when reporting on NBU Masters running Oracle RMAN or MS SQL Server.	View Builder performance is impacted by an exponential growth of file system objects in the Veritas Backup Reporter database when the Veritas Backup Reporter data collector is configured using BreakupJobs = True.	You must configure the Veritas Backup Reporter data collector using BreakupJobs = False (the default setting).

## About troubleshooting report refreshing issues

In Veritas Backup Reporter, temporary files that are generated with reports are stored in the `\temp\reports` directory instead of the `temp` directory as against in the earlier versions. The locations of the `reports` directory are as follows:

Solaris	<code>&lt;serverInstallDir&gt;/web/vbr/temp/reports</code>
Windows	<code>&lt;serverInstallDir&gt;\server\web\vbr\temp\reports</code>

After Veritas Backup Reporter upgrade, the existing reports do not properly display because of the new location of the directory that contains temporary files. You must refresh the reports to view them.

### About troubleshooting data collector configuration issues

If multiple Veritas Backup Reporter data collectors are configured to collect data from the same backup product server, duplicate data may be stored in the Veritas Backup Reporter database. To prevent the duplication of data, configure only one data collector to collect data from a single backup product server instance. If the backup product is clustered, specify the virtual IP address of the backup product server during the data collector configuration.

## About Veritas Backup Reporter log files

This section provides information about log files that VBR creates and which you can use for troubleshooting issues that you come across while using the VBR application.

**Table 12-3** lists locations of logs related to various VBR processes, on Windows and Solaris setups. For example, when an agent related process is running, the associated information is stored in the Agent logs at the given location.

These are all default locations.

---

**Note:** The log level of Agent and data collector can be set using the Agent and data collector configuration UIs.

---

**Table 12-3** Locations of logs for various VBR processes

VBR processes	Solaris	Windows
Agent related processes	<code>/opt/VRTSccsva/logs</code>	<code>c:\program files\symantec\veritas backup reporter\agent\logs</code>
CORBA Server related processes	<code>/var/VRTSccvs/log</code>	<code>c:\program files\symantec\veritas backup reporter\corbaserver\logs</code>

**Table 12-3** Locations of logs for various VBR processes (*continued*)

VBR processes	Solaris	Windows
Installation related processes	/opt/VRTS/install/logs	c:\documents and settings\all users\application data\symantec\veritas backup reporter and c:\documents and settings\all users\application data\veritas\vrtsweb
Management Server related processes	/var/VRTSccsvs/log	c:\program files\symantec\veritas backup reporter\server\logs
PBX related processes	/var/log/VRTSpbx	c:\program files\veritas\vxpbx\log
Web Server related processes	/var/VRTSweb/log	c:\program files\veritas\vrtsweb\log

[Table 12-4](#) lists the names of VBR log files and purpose of each log file. Use these log files while troubleshooting issues.

---

**Note:** 'X' indicates an incrementing log file number.

---

**Table 12-4** Log file names

VBR component	Log file name	Suggested troubleshooting purpose
Agent	agent_corba_client.log	CORBA issues
	agent_corba_server.log	CORBA issues
	core-0.log	Agent-server communication and data transmission errors
	err-0.log	All errors and exceptions details
	module-000-agentscheduler-<agent host>-X.log	Data collection scheduler issues
	module-001-agentalertposter-<agent host>-X.log	Agent related alert issues
	module-<data collector instance>-commvault-<agent host>-X.log	CommVault data collector log
	module-<data collector instance>-backupexec-<agent host>-X.log	NetBackup Exec data collector log
	module-<data collector instance>-enterprisevault-<agent host>-X.log	Enterprise Vault data collector log
	module-<data collector instance>-netbackup-<agent host>-X.log	NetBackup Enterprise data collector log
	module-<data collector instance>-networker-<agent host>-X.log	NetWorker data collector log
	module-<data collector instance>-puredisk-<agent host>-X.log	PureDisk data collector log
	module-<data collector instance>-tsm-<agent host>-X.log	TSM data collector log
	out-0.log	Message redirected to STDOUT
	summary-X.log	Agent spooler issues

**Table 12-4** Log file names (*continued*)

VBR component	Log file name	Suggested troubleshooting purpose
Management Server	err0.X.log	Database errors
	out0.log	Message redirected to STDOUT
	protocol_client0.X.log	Web application start/stop issues
	protocol_server0.X.log	Web application start/stop issues
	server_corba_client.log	CORBA issues
	server_corba_server.log	CORBA issues
	vbr-report0.X.log	Report issues
	vbr0.0.log	Exception errors and failed commands
Web Server	command0.X.log	Startup and shutdown messages
	hs_err0.X.log	Created if Java VM crashes
	jvm0.X.log	Memory issues
	ROOT0.X.log	Tracks logon access to webserver
	vbr-web0.X.log	License or logon issues

## About Veritas Backup Reporter status codes and recommended troubleshooting steps

This section provides detailed information about the status codes / error codes that you may come across while using the VBR application. This section provides recommended actions or troubleshooting steps that you need to take when you see a particular status code.

---

**Note:** VBR status codes are prefixed with 'A' when they originate from the agent and an 'S' when they originate from the server. For example, 'A217' is an agent error code. "S3003" is a server error code.

---

This information about VBR status codes is also available at the following location:

<http://seer.entsupport.symantec.com/docs/319722.htm>

**Note:** Additionally, Veritas Backup Reporter provides Knowledge Base of reference information for product error codes and commands. You can click an error code for say a failed job to view the Knowledge Base entry for that error code.

See [“About the Veritas Backup Reporter Knowledge Base”](#) on page 575.

If you come across any error while using VBR and cannot find a resolution in this section, record the status / error code and exact error message, provide this information to Symantec Technical Support.

<http://www.symantec.com/business/support/index.jsp>

Table 12-5 lists status codes related to VBR Management Server and recommended actions that you need to take when you come across these status codes.

**Note:** VBR Management Server status codes are displayed with an ‘S’ prefix.

**Table 12-5** VBR Management Server status codes

Status Code Range	Short Description	Recommended Action
0 - 999	Misc. / Debug	Dependent on circumstances. No specific recommendations.
100 - 1999	Authentication / Authorization	<ul style="list-style-type: none"> <li>■ Verify that the VBR agent is authenticated with the VBR server.</li> <li>■ Verify that the Symantec Product Authentication service is running.</li> </ul>
2000 - 2999	Fatal Database Exceptions	Review the CORBA server logs for more information
3000 - 3999	Non-fatal Database Exceptions	<ul style="list-style-type: none"> <li>■ Verify that the VBR database service is running.</li> <li>■ Verify that "db.portNumber" and other entries in server.conf are correct.</li> </ul>

**Table 12-5** VBR Management Server status codes (*continued*)

Status Code Range	Short Description	Recommended Action
4000 - 4999	CORBA Exceptions	<ul style="list-style-type: none"> <li>■ Verify that the CORBA service is running.</li> <li>■ Verify that Symantec Private Branch Exchange is running.</li> <li>■ Verify that Symantec Product Authentication service is running.</li> <li>■ Review the CORBA server logs for more details.</li> </ul>
5000 - 5999	User Exceptions	Review the CORBA server logs for more information
6000 - 6999	System Exceptions	Review the CORBA server logs for more information
7000 - 7999	Alert Manager Exceptions	Review the CORBA server logs for more information
8000 - 8999	Third Party Exceptions	No specific recommendations
9000 - 9999	Reserved for future use	No specific recommendations

The following is a complete list of the VBR Agent status codes listed in numerical order:

---

**Note:** Agent status codes are displayed with an 'A' prefix.

---

### VBR status code: A1

Message: Cannot resolve version

Explanation: The agent and management server software installed are not compatible.

Recommended action: Verify that you have installed the same version of software for the agent and the management server.

### VBR status code: A2

Message: Invalid agent home directory

Explanation: The agent's home directory is invalid or not present.

Recommended action: Verify that the file path specified for the agent is present, by doing the following:

- In the VBR console, choose **Settings > Global Settings > Agent Configuration**.
- Choose a configured agent and then select a configured data collector.
- Verify the home directory path to the actual installation path of the agent, as it appears in the operating system of that agent.

### **VBR status code: A3**

Message: Could not load configuration

Explanation: The agent configuration file is missing or invalid.

Recommended Action: - In Solaris the default path is "". - In the default path is .  
- Open agent.conf and review the entries for invalid information.

- Verify that agent.conf exists.  
Solaris - /opt/VRTScsava/conf/agent.conf  
Windows - <install path>\Veritas Backup Reporter\agent\conf\agent.conf
- Open agent.conf and review the entries for invalid information.

### **VBR status code: A4**

Message: Could not save configuration

Explanation: The agent was unable to save its configuration file after authentication of the agent with the management server.

Recommended Action: If authentication is successful then the agent.conf file must be manually updated by doing the following:

- Open agent.conf.
- Add or edit the entry 'serverName =' with the correct hostname of the server that the agent is installed on.
- Restart the agent.

### **VBR status code: A5**

Message: Fatal Authentication Exception

Explanation: The agent is not able to authenticate with the management server.

Recommended Action:

- Verify that the arguments provided to 'agentauth.exe' are correct.
- Verify that the Symantec Authentication service is running

- Review the 'Resolving agent authentication failures manually on Solaris and Windows' section in this guide.  
See "[Resolving agent authentication failures manually on Solaris and Windows](#)" on page 110.

### **VBR status code: A6**

Message: Fatal Scheduler Error

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A7**

Message: Network error

Explanation: The IP address or host name of the agent could not be determined.

Recommended Action:

- Verify that the agent is running.
- Verify that the data collector is configured with the correct location.
- Check name resolution and the hosts file on the management server.

### **VBR status code: A8**

Message: Agent not authenticated with the server

Explanation: The VBR agent could not authenticate with the management server

Recommended Action: Review 'Resolving agent authentication failures manually on Solaris and Windows' in this guide.

See "[Resolving agent authentication failures manually on Solaris and Windows](#)" on page 110.

### **VBR status code: A9**

Message: Invalid Arguments passed on the command line

Explanation: Invalid arguments were passed on the command line while starting the agent from the command prompt.

Recommended Action: Review ‘Stopping and starting the Veritas Backup Reporter Agent on Solaris and Windows’ in the this guide.

See “[Stopping and starting the Veritas Backup Reporter Agent](#) ” on page 115.

### **VBR status code: A10**

Message: The EventQueueElement already exists

Explanation: The data collection event to be performed already exists in the data collection event queue.

Recommended Action: Do not click on ‘Force Poll’ until all of the running data collection events complete.

### **VBR status code: A11**

Message: Fatal invalid configuration

Explanation: The VBR agent is unable to start.

Recommended Action:

- Verify that the agent is not already running.
- Verify that the agent home directory is present.
- Verify that the agent is authenticated with the management server - Check file and logon permissions.

### **VBR status code: A200**

Message: Invalid date range

Explanation: The date range, i.e. either start time or end time, is invalid (null) for Job or Image data collection.

Recommended Action: This is an internal error from the agent and should not occur under normal usage. The date range used by the agent is dependent on the data collection interval, but this could be magnified by incorrect OS date and time settings. Collect all agent logs and error information and then contact Symantec support.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A201**

Message: Invalid communication method

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A202**

Message: Data collection event was improperly initialized

Explanation: Data collection event is not initialized properly

Recommended Action: Check to see that all of the VBR software (agents, management server, view builder) have been upgraded to the same version level.

### **VBR status code: A203**

Message: Failed to transmit data

Explanation: Error while transmitting data from the agent to the management server.

Recommended Action: Do the following steps: 1. 2. 3.

- In the VBR console choose from **Settings > Global Settings > Agent Configuration > Show All Agents Status**.
- Click on the appropriate agent and choose 'Show Agent Data Transmission Problems'.
- Click on 'Force Load'.

### **VBR status code: A204**

Message: The data collection event is already in the queue

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A205**

Message: Cannot get session

Explanation: Cannot get a CORBA session with the CORBA server.

Recommended Action:

- Verify that Veritas Backup Reporter Corba Server service is running.
- Verify that Symantec Private Branch Exchange service is running.

### **VBR status code: A206**

Message: Invalid connection parameters

Explanation: An invalid connection parameter was used while an agent was connecting to management server.

Recommended Action: Verify that the server name is valid in agent.conf.

### **VBR status code: A207**

Message: Cannot contact server

Explanation: The agent cannot communicate with the VBR CORBA server.

Recommended Action:

- Verify the VBR CORBA server is running.
- Verify that `agent.conf` has valid configuration parameters.
- Verify agent authentication.
- Verify the network path between the agent and the VBR management server is working
- Verify that the ports used by VBR are not blocked by a firewall

### **VBR status code: A208**

Message: Cannot update meta data

Explanation: The agent cannot update its configuration.

Recommended Action:

- This is usually a VBR server-side exception. Check the VBR management server's logs.
- Verify file permissions of the VBR directories and files.

### **VBR status code: A209**

Message: Cannot send heartbeat

Explanation: This error should not occur through normal use of VBR.

**Recommended Action:** Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A210**

**Message:** Cannot get data from server

**Explanation:** The agent is not able to get VBR server version information from the VBR management server.

**Recommended Action:** Verify that the VBR management server processes are running and that the correct version is present in the version file.

### **VBR status code: A211**

**Message:** The requested action is not supported

**Explanation:** This error should not occur through normal use of VBR.

**Recommended Action:** Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A212**

**Message:** Improper use of method

**Explanation:** This is an internal message.

**Recommended Action:** Upgrade to the latest maintenance release. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A213**

**Message:** Invalid data collector instance The agent is expecting to gather data for a non-existent data collector.

**Explanation:**

**Recommended Action:**

- Verify that agent.conf has valid data collector entries.
- Stop the VBR agent. Remove problematic data collector entries from agent.conf.
- Start the agent.
- Check the agent log for further messages.

## VBR status code: A214

Message: Invalid data collection event

Explanation: The agentdatacollectionutility.exe command line utility provides the ability to run an immediate poll of any of the seven data collection types within a VBR data collector. The agent tried to collect data using invalid options.

Recommended Action: Upgrade to the latest maintenance release. If manually running commands verify that the correct options are being used.

## VBR status code: A215

Message: Log Configuration Error

Explanation: Database transaction logs are not in the format expected during an upgrade.

Recommended Action:

- Verify that any release dependencies have first been installed.
- Close any open VBR consoles before upgrading.
- Upgrade the management console before upgrading the agents or ViewBuilder.
- Ensure that you have administrative rights
- For Symantec Backup Exec: - Verify that all operating system patches have been applied
- Install the redistributable package for Microsoft Visual C++ 200

## VBR status code: A216

Message: Cannot send alert

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

## VBR status code: A217

Message: Data rejected by server

Explanation: The data received by VBR could not be loaded.

Recommended Action:

- Examine the VBR Corba Server logs for more details - Windows default path: c:\program files\symantec\veritas backup reporter\server\corbaserver\logs - Solaris: /var/VRTSccsvs/log/ - I -
- Increase the maxheap setting.
- Disable automatic reboot if the maxheap setting is configured.

### **VBR status code: A218**

Message: Could not initiate data collection event

Explanation: The agent is not getting any data returned from a query

Recommended Action:

- Verify the path to the binary location for NetBackup.
- Check the Agent logs, /opt/VRTSccsva/logs, to see what is reported as a problem when trying to collect information from this data collector. (Specifically, check agent-core-0.log.)
- Check to see how the problematic data collector was configured. Look in the /opt/VRTSccsva/conf/agent.conf config file.
- For UNIX, confirm that the homeDirectory value is set to the UNIX path. The homeDirectory refers to the location of Net Backup binaries on the Agent.
- For Windows, check C:\Program Files\Symantec\Veritas Backup Reporter\Agent\Logs and C:\Program Files\Symantec\Veritas Backup Reporter\Agent\conf.

### **VBR status code: A219**

Message: The data collector has thrown an error.

Explanation: A data collector has experienced a Java error. The message can also be related to memory (e.g. Java heap space)

Recommended Action: Check which data collector has the error condition and correct or recreate the data collector.

### **VBR status code: A220**

Message: Invalid null data

Explanation: The backup product sent invalid or null data to the agent.

Recommended Action:

In the NetBackup master server:

- Check images using bpimagelist commnd for "no entity found"
- Upgrade the master server to the latest maintenance release

### **VBR status code: A221**

Message: Invalid state transition

Explanation: VBR data collection event is in invalid state.

Recommended Action: Restart the VBR agent

### **VBR status code: A222**

Message: Internal communication error

Explanation: The agent has determined that it has no space to create a file in the spooler directory.

Recommended Action:

- Verify that the file path specified for the agent is present.
- Verify that the file path specified for the spooler directory is present and on same computer as the agent.
- Stop the agent service.
- Edit the MaxMemoryUsage value in agent.conf. By default the value is set to 500 - Note: value must be set lower than the amount of available disk space on the server hosting the agent.
- Start the agent service.

### **VBR status code: A223**

Message: Invalid parameter

Explanation: A data collector configuration parameter is not valid while updating the configuration.

Recommended Action: Review the data collector configuration for correctness. Check VBR logs for more details.

### **VBR status code: A224**

Message: Communication Queue does not exist

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A225**

Message: Communication Queue does not exist

Explanation: This error should not occur through normal use of VBR.

Recommended Action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A226**

Message: Data collector does not exist

Explanation: The data collector for the specified instance identifier does not exist

Recommended action: Verify that the data collector configuration is present with said instance number in the agent.conf file.

### **VBR status code: A227**

Message: Event already exists

Explanation: The data collection event already exists.

Recommended action: Wait for the data collection event to finish. No further action should be needed.

### **VBR status code: A228**

Message: Invalid event schedule

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A229**

Message: Event does not exist

Explanation: An attempt was made to remove an event that does not exist.

Recommended action: Review the agent logs for more details.

### **VBR status code: A230**

Message: Data collector already exists

Explanation: The data collector has already been instantiated. This status can occur if a new data collector is configured that is identical to an existing one or if agent.conf has more than one entry with the same instance ID.

Recommended action: Verify that the data collector configuration is correct. Verify that agent.conf does not have a duplicate instance ID.

### **VBR status code: A231**

Message: <no message is displayed>

Explanation: The requested CORBA object does not exist.

Recommended action: This is an internal status code. Verify that the VBR Corba Server service is running. Check the VBR management server log core-0.log for more details.

### **VBR status code: A232**

Message: <no message is displayed>

Explanation: The CORBA session times out.

Recommended action: This is an internal status code. Verify that the VBR Corba Server service is running. Check the VBR management server log core-0.log for more details.

### **VBR status code: A2000**

Message: Parameter passed is NULL

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A2001**

Message: Data stream is NULL

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

## **VBR status code: A2002**

Message: Data collector configuration is NULL

Explanation: The data collector configuration is invalid.

Recommended action: Correct the data collector configuration. Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

## **VBR status code: A2003**

Message: Data collector configuration is invalid

Explanation: The home directory in the data collector configuration was not specified or is invalid while configuring a TSM data collector.

Recommended action: Review the data collector configuration and correct the home directory. This can also be reviewed in agent.conf.

## **VBR status code: A2004**

Message: Collection method is NULL

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

## **VBR status code: A2005**

Message: Invalid value for collection method

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

## **VBR status code: A2006**

Message: Collection request is not supported.

Explanation: The data collection for the configured event and configured product is not supported.

Recommended action: Verify that the data collector was correctly created. Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2007**

Message: Data collector configuration is invalid

Explanation: The home directory in the data collector configuration was not specified or is invalid while configuring a Networker data collector.

Recommended action: Review the data collector configuration and correct the home directory. This can also be reviewed in agent.conf.

### **VBR status code: A2008**

Message: Home directory of the product does not exist

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2009**

Message: The master server is NULL

Explanation: The product host specified while configuring a CommVault data collector is invalid.

Recommended action: Correct the data collector configuration.

### **VBR status code: A2011**

Message: IOException happened when executing external process

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2012**

Message: Command array for external process is NULL or empty

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2013**

Message: External process interrupted

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2014**

Message: External process terminated because of not returning data in a timely manner

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2015**

Message: External process exited abnormally

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2020**

Message: Data source file not found

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

<http://www.symantec.com/business/support/index.jsp>

### **VBR status code: A2021**

Message: IOException happened when using data source file

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A2022**

Message: Invalid data source

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A2030**

Message: Unexpected problem encountered when parsing command output

Explanation: An unexpected problem was encountered.

Recommended action: Review the agent logs for more information.

### **VBR status code: A2031**

Message: Incorrect named value count

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A2032**

Message: File not found

Explanation: The Networker messages file could not be located using the provided information.

Recommended action:

Verify that the location of the messages file in the Legato Networker installation and compare it to the data collector configuration. Default paths for the messages file:

Windows: c:\program files\nsr\logs\messages

Solaris: /usr/sbin/nsr/logs/messages

### **VBR status code: A2033**

Message: File name invalid

Explanation: The Networker messages file couldn't be located using the provided information.

Recommended action:

Verify that the location of the messages file in the Legato Networker installation and compare it to the data collector configuration. Default paths for the messages file:

Windows: c:\program files\nsr\logs\messages

Solaris: /usr/sbin/nsr/logs/messages

### **VBR status code: A3000**

Message: Netbackup host name is NULL

Explanation: The NetBackup host name that was configured is invalid.

Recommended action: Verify the NetBackup product host name used in agent.conf.

### **VBR status code: A3001**

Message: Failed to initialize NBU job data collector for master server

Explanation: The job data collection could not be initialized because the NetBackup product host name was not recognized.

Recommended action:

In Global Settings, Agent Configuration, open the configured agent and check that the product host is the hostname of the NetBackup server from which data is to be collected.

### **VBR status code: A3002**

Message: Failed to get the slot count information from vmchange

Explanation: An error was experienced trying to execute the vmchange command.

Recommended action:

- Verify that the agent has access to the vmchange command if the agent is not installed on the NetBackup master server.
- Verify that the vmchange command being executed is of the same version as the NetBackup master server.  
Windows default location: <install path>\volmgr\bin\vmchange.exe  
Unix default location: /usr/opensv/volmgr/bin/vmchange
- Verify that vmchange has not been replaced with some other file.  
Verify that in the operating system's search path a vmchange file does not get executed before reaching NetBackup's vmchange.  
Check the data collector configuration in agent.conf.

### **VBR status code: A3003**

Message: Media data collection failed.

Explanation: Tape library information is not available for the media.

Recommended action: Check the data collector configuration in agent.conf.

### **VBR status code: A3004**

Message: Failed to get the volume database host information for the agent product host

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A3005**

Message: Failed to get the master server hostname for the agent product host

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A3006**

Message: Failed to fully qualify host name: Please contact System Administrator

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A3007**

Message: Failed to initialize NetBackup agent: Local NetBackup version does not match with Remote NetBackup version

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A3008**

Message: Failed to initialize NetBackup agent: Could not determine the product version

Explanation: Unable to determine the version of the remote NBU product host.

Recommended action:

- Verify that NBU product host name is valid in agent.conf.
- Verify that the NetBackup product server is accessible from the agent.

---

**Note:** The agent is trying to run the command "bpcnlntcmd -get\_remote\_host\_version <product host name>"

---

### **VBR status code: A3009**

Message: Failed to initialize NetBackup data collector

Explanation: Unable to determine the version of the remote NBU product host.

Recommended action: Check the values provided in data collector configuration or in agent.conf, such as Server name, collection method, and Home Directory.

### **VBR status code: A4000**

Message: BE host name is NULL

Explanation: BE server host name is invalid in data collector configuration.

Recommended action: Verify that correct host name is provided while configuring the data collector for BE.

### **VBR status code: A4001**

Message: Failed to initialize BE agent

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4002**

Message: Failed to connect to BE master server

Explanation: The agent was unable to connect to BE master server.

Recommended action: Verify that the BE server is up and running. Ensure that BE Server is accessible from the agent host.

### **VBR status code: A4003**

Message: Failed to connect to BE master server using BEMSDK

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4004**

Message: Failed to initialize BE Job data Collector

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4005**

Message: Invalid BE Job data Collector

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4006**

Message: BE Job data parsing error

Explanation: An error occurred during data collection.

Recommended action: Review the data collector logs for more detail.

### **VBR status code: A4007**

Message: Parsing error in BE Job data from BEMSDK

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4008**

Message: BE Policy data parsing error

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4009**

Message: Parsing error in BE Policy data from BEMSDK

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4010**

Message: Failure determining the BE version

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A4011**

Message: Error while Policy data collection

Explanation: An error occurred collecting policy data.

Recommended action: Review the data collector logs (module-XXX-backupexec-<BE Server Name>X.log) for specific details.

### **VBR status code: A4012**

Message: Error while Job data collection

Explanation: An error occurred collecting job data.

Recommended action: Review the data collector logs (module-XXX-backupexec-<BE Server Name>-X.log) for specific details.

### **VBR status code: A4013**

Message: Error while Tape Drive collection

Explanation: An error occurred collecting tape drive data.

Recommended action: Review the data collector logs (module-XXX-backupexec-<BE Server Name>-X.log) for specific details.

### **VBR status code: A4014**

Message: Error while Media data collection

Explanation: An error occurred collecting media data.

Recommended action: Review the data collector logs (module-XXX-backupexec-<BE Server Name>-X.log) for specific details.

### **VBR status code: A4500**

Message: Invalid user name specified

Explanation: Invalid user name specified while configuring CommVault data collector.

Recommended action: Verify the username provided while configuring the CommVault data collector.

### **VBR status code: A4501**

Message: Invalid password specified

Explanation: Invalid password specified while configuring CommVault data collector.

Recommended action: Verify the password provided while configuring the CommVault data collector.

### **VBR status code: A4502**

Message: Invalid port specified

Explanation: Invalid port number specified while configuring CommVault data collector.

Recommended action: Verify the port number provided while configuring the CommVault data collector.

### **VBR status code: 4503**

Message: Could not determine the product version

Explanation: The CommVault version could not be determined.

Recommended action: Verify that a supported version of CommVault is installed. Verify the agent installation. Check the CommVault product host name used.

### **VBR status code: A4504**

Message: Could not connect to the CV database

Explanation: Could not connect to the CommVault database.

Recommended action: Verify that CommVault database is up and running.

### **VBR status code: A4505**

Message: Could not find the database driver

Explanation: Could not find the CommVault database driver

Recommended action: Verify that CommVault version is supported.

### **VBR status code: A4506**

Message: Could not get data from the result set

Explanation: Could not get data from the result set

Recommended action: Review the data collector logs (module-XXX-commvault-<CommVault Server Name>-X.log) for specific details.

### **VBR status code: A4507**

Message: Invalid data returned by the commvault db query

Explanation: Invalid data returned by the commvault db query

Recommended action: Review the data collector logs (module-XXX-commvault-<CommVault Server Name>-X.log) for specific details.

### **VBR status code: A4508**

Message: Problem with the properties file

Explanation: Properties file containing CommVault sql queries is invalid.

Recommended action: Review the data collector logs (module-XXX-commvault-<CommVault Server Name>-X.log) for specific details.

### **VBR status code: A5001**

Message: Could not instantiate report manager stub

Explanation: Initialization failure of PureDisk data collector. Secure port may not be available/open to connect.

Recommended action: Verify secure port 1044

### **VBR status code: A5002**

Message: Could not add header to report manager stub

Explanation: Internal connectivity issues between internal objects.

Recommended action: Increase cache size, verify that the server is not overburdened by CPU or memory usage.

### **VBR status code: A5003**

Message: Error in retrieving policy data

Explanation: There was an error in retrieving the policy data.

Recommended action: Typically this exception occurs after creating the PureDisk data collector. Restarting the data collector works in most of the cases. If it doesn't work then delete and recreate data collector.

### **VBR status code: A5004**

Message: Error in retrieving completed job data

Explanation: There was an error in retrieving the completed job data.

Recommended action: Typically this exception occurs after creating the PureDisk data collector. Restarting the data collector works in most of the cases. If it doesn't work then delete and recreate data collector.

### **VBR status code: A5005**

Message: Could not connect to the PD database

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5006**

Message: Could not find the database driver

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5007**

Message: Could not get data from the result set

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5008**

Message: Error in executing the query

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5009**

Message: Problem with the properties file

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5010**

Message: Data iterator is already destroyed.

Explanation: Occurs if the PureDisk data collector tries to process an expired job/policy data iterator.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5011**

Message: Invalid configuration for PureDisk.

Explanation: An invalid configuration was provided while creating a PureDisk data collector

Recommended action: Check the specified PureDisk SPA host is valid and running.

### **VBR status code: A5012**

Message: Report Manager is not responding for given request.

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A5013**

Message: Failed to load queries from file.

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A6000**

Message: Resource type invalid

Explanation: CLI output validation failed.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A6001**

Message: Failed to load resource

Explanation: Unable to load an event data class, e.g. "NetworkerMedia" class for the event "Media".

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A6010**

Message: IOException encountered when parsing message log file

Explanation: The message file location is incorrect or the message file is missing.

Recommended action: Verify that the message file is in its location. Take corrective action if it is not there or the location is invalid.

### **VBR status code: A6020**

Message: The command passed to 'nsradmin' is not supported

Explanation: This error will occur when trying to run a command that is unsupported or invalid.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A6030**

Message: Error while date parsing, possibly unsupported locale

Explanation: The date returned in the CLI output is different than the default date format. This may be due to a different locale than the local of the server.

Recommended action: The date format should be in the default locale format. Verify that the locale is supported by VBR. Verify that the date format of the Operating System has not been customized.

### **VBR status code: A8000**

Message: TSM Product Host Name is NULL

Explanation: The TSM server name is not specified in the data collector configuration.

Recommended action: Verify that the TSM data collector configuration is correct and that the TSM server name is present.

### **VBR status code: A8001**

Message: Failed to connect to TSM Server

Explanation: Failed to connect to the TSM server.

Recommended action: Verify that the TSM server is running.

### **VBR status code: A8002**

Message: Failed to initialize TSM data collector

Explanation: Failed to initialize the TSM data collector.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8003**

Message: Error while executing TSM query

Explanation: An error occurred while executing the TSM query.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8004**

Message: TSM Header-Check error

Explanation: The header of the output from a TSM command line query does not match the expected header.

Recommended action: Verify that data is being collected from a supported version of TSM. Verify that the TSM data collector is correctly configured. Review data collector logs for more details, with the log level set to ALL.

### **VBR status code: A8005**

Message: Error while Policy data collection

Explanation: An error occurred while collecting TSM policy data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8006**

Message: Error while Job data collection

Explanation: An error occurred while collecting TSM job data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8007**

Message: Error while Skipped File data collection

Explanation: An error occurred while collecting TSM skipped files data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8008**

Message: Error while Error / Log data collection

Explanation: An error occurred while collecting TSM errors and logs data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8009**

Message: Error while Tape Drive / Library data collection

Explanation: An error occurred while collecting TSM tape drive and library data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A8010**

Message: Error while Media data collection

Explanation: An error occurred while collecting TSM media data.

Recommended action: Review the data collector logs (module-XXX-tsm-<TSM server name>-X.log) for specific details.

### **VBR status code: A9000**

Message: Generic agent host name is NULL

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9001**

Message: Invalid utility location for Generic agent

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9002**

Message: Failed in running utility specified for Generic agent

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9004**

Message: Failed to initialize Generic data Collector

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9005**

Message: Invalid Generic data Collector

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9006**

Message: Generic data parsing error

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9500**

Message: Failed to create API object

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9501**

Message: Failed to collect single host data from CCMM API

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9502**

Message: Failed to collect hosts data from CCMM API

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9503**

Message: Failed to collect filter data from CCMM API

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9504**

Message: Failed to collect sample data from CCMM AP

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9505**

Message: Failed to check for more elements from CCMM API

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A9506**

Message: Failed to get the next element from CCMM API

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10001**

Message: SQL Server driver not loaded

Explanation: SQL Server driver not loaded

Recommended action: Install the SQL Server driver and check the database access from the data collector to the VaultDirectory.

### **VBR status code: A10002**

Message: Error during collection of event data

Explanation: Error during collection of event data

Recommended action: Check the Enterprise Vault data collector logs for more specific details.

### **VBR status code: A10003**

Message: Error during collection of VaultPartition data

Explanation: Error during collection of event data

Recommended action: Check the Enterprise Vault data collector logs for more specific details.

### **VBR status code: A10004**

Message: Error during collection of event data

Explanation: Error during collection of event data

Recommended action: Check Enterprise Vault data collector logs for more specific details.

### **VBR status code: A10005**

Message: Error during collection of event data

Explanation: Producer thread for savesets failed with an exception

Recommended action: Check Enterprise Vault data collector logs for more specific details.

### **VBR status code: A10007**

Message: Invalid data port

Explanation: An invalid port was specified during collection of event data

Recommended action: Check the Enterprise Vault data collector logs for more specific details.

### **VBR status code: A10008**

Message: Producer thread for savesets failed with an exception

Explanation: Invalid database port

Recommended action: Check the database port configured in the data collector configuration.

### **VBR status code: A10009**

Message: Error querying SQL Server database

Explanation: I/O Error saving EV spooler files

Recommended action: Check the systems free space

### **VBR status code: A10010**

Message: I/O Error saving EV spooler files

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10011**

Message: I/O Error reading EV spooler files

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10012**

Message: Error querying SQL Server database

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10013**

Message: I/O Error saving EV spooler files

Explanation: This error should not occur through normal use of VBR.

Recommended action: Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10014**

Message: Producer thread for targets failed with an exception

**Explanation:** This error should not occur through normal use of VBR.

**Recommended action:** Review the VBR documentation for correct installation and usage. Save all error information and contact Symantec Support if the issue persists.

### **VBR status code: A10015**

**Message:** I/O Error reading EV spooler files

**Explanation:** An error occurred while querying SQL database

**Recommended action:** Check the database access from agent host to Vault Store Database.

### **VBR status code: A10016**

**Message:** Producer thread to vault capacity failed with an exception

**Explanation:** An error I/O error occurred while saving EV spooler files

**Recommended action:** Check the file system space.

## Gathering troubleshooting data with the support script

If you are running Veritas Backup Reporter on Solaris or Windows, you can use the `supportscript` to gather troubleshooting information. The script collects server and agent logs, collects information about any data collection problems, captures the current agent configuration, and compresses the results into a tar or zip file.

### **To gather troubleshooting data with the support script**

- 1 From a console or Windows Command Prompt, change to one of the following directories:

---

**Note:** The following are all default directory locations on Windows and Solaris machines.

---

#### ■ Solaris

`/opt/VRTSccsvb`

`/opt/VRTSccsvs`

#### ■ Windows

`C:\Program Files\Symantec\Veritas Backup Reporter\Server\util`

```
C:\Program Files\Symantec\Veritas Backup Reporter\Agent\bin
```

- 2 Type the following command and press **Enter**:

```
support
```

- 3 Transfer the resulting `.tar` or `.zip` file to the Veritas Support FTP server when prompted.

## About contacting the Veritas Backup Reporter support team

You can contact Veritas Backup Reporter support team on the Web, by email, or by telephone.

### About using the Symantec support Web site

For technical assistance with any Symantec product, go to the following Web site:

<http://www.symantec.com/enterprise/support/index.jsp>

From there you can do the following:

- Contact the Symantec Support staff and post questions
- Get the latest software patches, upgrades, and utilities
- View updated hardware and software compatibility lists
- View frequently asked questions (FAQ) pages for the products you are using
- Search the knowledge base for answers to technical support questions
- Receive automatic notice of product updates
- Find out about training in the Symantec products
- Read current white papers related to the Symantec products

### About subscribing to the Symantec email notification service

Subscribe to the Symantec email notification service to receive alerts for newly published documentation, software, beta programs, and other services.

Select a product and click Email Notifications. Your customer profile ensures that you receive the latest technical information pertaining to your specific interests.

## About accessing Symantec telephone support

Telephone support is available with a valid support contract. To contact Symantec for technical support, dial the appropriate phone number listed on the Support Guide included in the product box. Have your product license information ready for quick navigation to the proper support group.

## About support for software updates

Licensed customers can use the following URL to obtain help with technical questions: <http://www.symantec.com/enterprise/support/index.jsp>.

To obtain software updates, send your requests to <http://fileconnect.symantec.com> or via the License Portal at <https://licensing.symantec.com>.

## About obtaining license information

To obtain license information, contact Veritas in one of the following ways:

- U.S. and Canada telephone: 1-800-634-4747, option 3
- Worldwide fax: +1-650-527-0952
- URL: [http://www.symantec.com/enterprise/support/assistance\\_information.jsp](http://www.symantec.com/enterprise/support/assistance_information.jsp)

## About purchasing Symantec products

For help with purchasing Symantec products, visit the Symantec Web site, from there you can contact product experts or view information about the products.

You can contact a Symantec product representative at the following URL:

[http://www.symantec.com/enterprise/contact\\_sales.jsp](http://www.symantec.com/enterprise/contact_sales.jsp)

Customers in the U.S. and Canada can call a Symantec product representative at 1-800-327-2232.

## About commenting on Symantec product documentation

Submit comments about the Symantec product documentation to the following URL: <http://www.symantec.com/enterprise/support/overview.jsp?pid=54202>

Please include the following information with your documentation comments:

- The title and product version of the guide you are commenting on
- The section in the guide (if relevant) you are commenting on
- Your comment

- Your name

# About the Veritas Backup Reporter database

This appendix includes the following topics:

- [About the VBR database schema](#)
- [About querying the VBR database](#)

## About the VBR database schema

The Veritas Backup Reporter (VBR) database is a rich repository of information about your storage network. This section gives an overview of the VBR database, and describes the tables in the VBR namespace.

The VBR Management Server uses Sybase SA (SQL Anywhere) database management system to store backup and archive data collected from various backup products.

The `ccsvc` database uses several database user names in which database objects - tables, views, and stored procedures - are organized.

Each database user provides a namespace for database objects defined by Veritas Backup Reporter:

- Veritas Backup Reporter uses the database to store service usage and expenditure reports, cost metrics, cost formulas, and alerts.

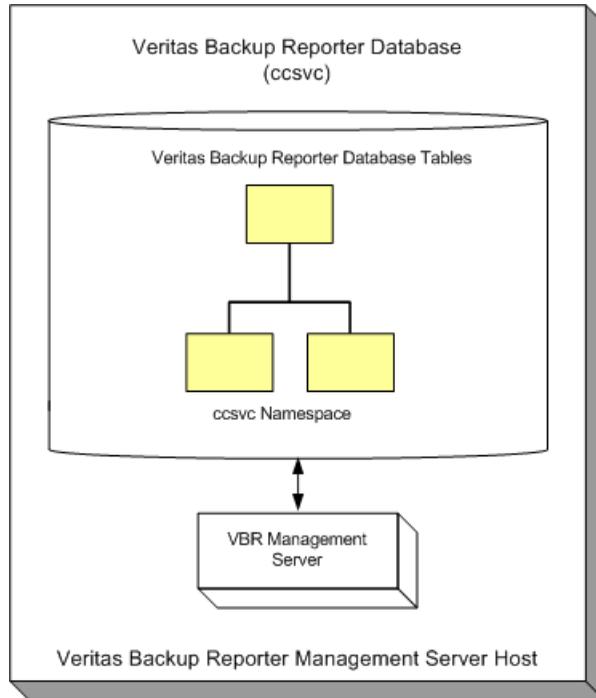
The VBR installation script creates the required namespaces depending on which Symantec products are installed.

## About namespaces for the VBR Management Server

When the VBR Management Server is the only Symantec product installed on a host, the following namespace is created in the database instance:

- `ccsvc` namespace

**Figure A-1** Database namespaces created on the VBR Management Server



## About querying the VBR database

This section provides information on how to query the VBR database.

[Table A-1](#) provides the connection details that you can use to access the VBR database through dbisql, ODBC, or JDBC.

**Table A-1** VBR database connection details

Database Connection Detail	Value
Database Name	ccsvc

**Table A-1** VBR database connection details (*continued*)

Database Connection Detail	Value
Server	<ul style="list-style-type: none"> <li>■ On Solaris:  <code>SYMANTEC_VBRDBMS_hostname</code>                      where <i>hostname</i> is not the fully qualified domain name.</li> <li>■ On Windows:  <code>VBR_hostname</code></li> </ul>
Database port	13799
Default User Name	guest
Default Password	guest

**Note:** `guest` is an account with read-only permissions.

## About accessing the VBR database using dbisql

The Sybase Interactive SQL program, `dbisql`, is the client interface for querying the database. `dbisql` is installed by default in the following directories:

Solaris	<code>/opt/vbrdbms/bin32</code>
Windows	<code>\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer\win32</code>

Before running `dbisql`, remember to set the necessary SA environment variables:

Solaris:	<code>/opt/vbrdbms/bin/sa_config.sh</code>
Bourne, K shells	For example: <code>cd /opt/vbrdbms/bin/sa_config.sh</code>
Solaris:	<code>/opt/vbrdbms/bin/sa_config.sh</code>
C shell	For example: <code>cd /opt/vbrdbms/bin</code> <code>source sa_config.sh</code>

**Windows:**                   **For example:**  
**SQLANY10**                   SQLANY10=C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer\Win32  
**SQLANYSH10**                 SQLANYSH10=C:\Program Files\Symantec\Veritas Backup Reporter\Server\DBServer\Win32

**Examples:**

**Solaris dbisql**           **Following is an example connect string for dbisql on Solaris:**

```
dbisql -c "UID=guest;PWD=guest;  
ENG=SYMANTEC_VBRDBMS_<hostname>;  
DBN=ccsvc;links=tcPIP (port=13799)"
```

**Replace hostname with the host running the database.**

**Windows dbisql**           **Following is an example connect string for dbisql on Windows:**

```
dbisql -c "UID=guest;  
PWD=guest;ENG=VBR_%COMPUTERNAME%;  
DBN=ccsvc; links=tcPIP (port=13799)"
```

## About accessing the database using JDBC

JDBC is another option available for performing VBR database queries.

The syntax is:

```
jdbc:sybase:Tds:<hostname>:port?ServiceName=<databasename>
```

**For example:**

```
jdbc:sybase:Tds:myhost:13799?ServiceName=ccsvc
```

# Command and configuration file reference

This appendix includes the following topics:

- [Command and configuration file locator](#)

## Command and configuration file locator

Veritas Backup Reporter provides commands that you can run from a UNIX shell or a command prompt (Windows), as well as configuration files that are integral to its operation. This section lists the Veritas Backup Reporter commands and configuration files in alphabetical order.

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory during installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable so that you do not need to change the directory to run the Veritas Backup Reporter command or script.

---

**Note:** To view the man pages for the utilities, add `/opt/VRTS/man/` to your host's `MANPATH` environment variable using the following command: `export MANPATH=$MANPATH:/opt/VRTS/man/`

---

[Table B-1](#) maps the Veritas Backup Reporter command and configuration file with its respective Veritas Backup Reporter host and default installation directory:

**Table B-1** Veritas Backup Reporter commands and configuration file locations

File	Default locations
vbr_conf.properties	/opt/VRTScsvs/conf  \Program Files\Symantec\Veritas Backup Reporter\Server\conf
eventposter	/opt/VRTScsvs/bin/goodies  \Program Files\Symantec\Veritas Backup Reporter\Server\util
jobutility	/opt/VRTScsvs/bin/goodies  \Program Files\Symantec\Veritas Backup Reporter\Server\util
runstoredquery	/opt/VRTScsvs/bin/goodies  \Program Files\Symantec\Veritas Backup Reporter\Server\util
support	/opt/VRTScsvs/bin  \Program Files\Symantec\Veritas Backup Reporter\Server\util  /opt/VRTScsva/bin  \Program Files\Symantec\Veritas Backup Reporter\Agent\bin
xml	/opt/VRTScsvs/bin  \Program Files\Symantec\Veritas Backup Reporter\Server\util
agentauth	/opt/VRTScsva/bin  \Program Files\Symantec\Veritas Backup Reporter\Agent\bin
dbbackup	/opt/VRTScsvs/bin  \Program Files\Symantec\Veritas Backup Reporter\Server\util
vbragent	/opt/VRTScsva/bin  \Program Files\Symantec\Veritas Backup Reporter\Agent\bin

**Table B-1** Veritas Backup Reporter commands and configuration file locations  
(continued)

File	Default locations
<a href="#">changedbpassword</a>	/opt/VRTScsvs/bin \\Program Files\\Symantec\\Veritas Backup Reporter\\Server\\util
<a href="#">vbrvb</a>	/opt/VRTScsvb/bin
<a href="#">vbrserver</a>	/opt/VRTScsvs/bin
<a href="#">vbrweb</a>	/opt/VRTScsvs/bin

# vbr\_conf.properties

`vbr_conf.properties` – configuration file for the VBR Management Server.

## DESCRIPTION

`vbr_conf.properties` is a general purpose configuration file for the Veritas Backup Reporter Management Server. For Veritas Backup Reporter installations made highly available against system failure on a clustered network, `vbr_conf.properties` should contain Symantec Product Authentication Service settings that identify the broker host.

## OPTIONS

`authentication.services.broker.host=hostname`

The fully-qualified host name of the Symantec Product Authentication Service broker host or the fully-qualified DNS name for the virtual IP or the cluster name of the Symantec Product Authentication Service broker host.

`authentication.services.broker.port=port`

The port for the Symantec Product Authentication Service broker host that the Veritas Backup Reporter Management Server connects to. By default, Symantec Product Authentication Service listens to port 2821.

`authentication.services.domain.suffix=brokerHostName`

Modifies the Symantec Product Authentication Service broker host name in situations when the Veritas Backup Reporter Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are not fully qualified in Symantec Product Authentication Service.

*brokerHostName* is either the Symantec Product Authentication Service broker host cluster name or the Symantec Product Authentication Service broker fully qualified host name.

`authentication.broker.domain.conf.file=domainBrokerMappingPathname`

Used when the Veritas Backup Reporter Management Server is clustered or when the Symantec Product Authentication Service broker is on a host remote from the Veritas Backup Reporter Management Server host.

Path and filename for the file that maps Veritas Backup Reporter domains to their brokers. By default, *domainBrokerMappingPathname* is:

`/opt/VRTSccsvs/conf/domain_broker.txt`

**exportDirectoryPrefix=*path***

Controls the default export path (Directory Prefix) that Veritas Backup Reporter console users see when they attempt to save scheduled reports. If the specified prefix directory is not present on the host, the Veritas Backup Reporter Management Server creates it.

**corba.external.ip=*port***

Identifies the actual public IP address (the “natted” address) for the Veritas Backup Reporter Management Server, when a firewall is configured to act as a Network Address Translation (NAT) device to route packets to hidden addresses behind the firewall.

**bram.corba.port=*port***

The port that the Veritas Backup Reporter Management Server uses to communicate with the Veritas Alert Manager Object Request Broker (ORB). (The default is 5431.)

**internal.trap.receiver.enabled=TRUE|FALSE , vxtrapd.enabled=TRUE|FALSE**

Controls which trap processor the Veritas Backup Reporter Management Server uses to receive SNMP traps: the Veritas Trap Processor (`vxtrapd`) and a second, internal trap receiver. Only one of the trap processors can be used (TRUE) at a time.

## NOTES

`vbr_conf.properties` resides by default in: `/opt/VRTSccsvs/conf` (Solaris) and `\Program Files\Symantec\Veritas Backup Reporter\Server\conf`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

`vbr_conf.properties` uses the standard Java properties file format. Each option inside the file must begin on a new line.

On Windows systems, you must insert an extra backslash.

For example on Windows:

```
exportDirectoryPrefix=C:\\Shared\\Reports
```

To get a list of private domains known to the Symantec Product Authentication Service, type the following command on a Veritas Backup Reporter Management Server:

```
Solaris      /opt/VRTSat/bin/vssat showallbrokerdomains
```

**Windows**      \Program Files\Veritas\Security\Authentication\bin\vssat  
showallbrokerdomains

## EXAMPLES

**EXAMPLE 1:** The following is an example of a `vbr_conf.properties` entry:

```
authentication.services.broker.host=myhost.example.com
authentication.services.broker.port=2821
authentication.broker.domain.conf.file=/opt/VRTSccsvs/conf
    /domain_broker.txt
authentication.services.domain.suffix=myhost.example.com
```

**EXAMPLE 2:** The following example is a `vbr_conf.properties` entry, when one or more of the Veritas Backup Reporter private domains is not fully qualified in Symantec Product Authentication Service:

```
authentication.services.broker.host=myhost.example.com
authentication.services.broker.port=2821
authentication.services.domain.suffix=myhost.example.com
authentication.broker.domain.conf.file=/opt/VRTSccsvs/conf
    /domain_broker.txt
```

## SEE ALSO

[agentauth](#)

[vbrserver](#)

# eventposter

eventposter - posts alerts to the VBR Console Alerts Summary

## SYNOPSIS

```
eventposter -server -port -usr -passwd -domainName -domainType  
-severity -summary -node [-agent|-ip  
|-alertGroup|-alertKey|-otherInfo1|-otherInfo2|-eventTime|-notify]
```

## DESCRIPTION

eventposter is a Veritas Backup Reporter utility that lets you post alerts to the Veritas Backup Reporter Console Alerts Summary.

## OPTIONS

-server *serverName*

(Required) Name of the Veritas Backup Reporter Management Server host you want to connect to.

-port *number*

(Required) Server port to use for the connection. The default port is 1556.

-usr *userName*

(Required) The valid user name for the server login credentials.

-passwd *password*

(Required) The valid password for the server login credentials.

-domainName *domainName*

(Required) The domainName for the server login credentials.

-domainType *domainType*

(Required) The type of domain against which to authenticate the server login credentials.

Valid domains are: nis, nt, vx, or a user-defined Symantec Product Authentication Service-authenticated domain.

-severity *severityLevel*

(Required) Severity of the event.

*severityLevel* must be an integer, 1-5, that represents the following on the event console:

5 - critical, 4 - error, 3 - warning, 2 or 1 - info

- summary *"string"*  
(Required) Text that appears in the summary field. *string* must be an exact match and enclosed in quotes.
- node *nodeName*  
(Required) Node name on which the events occurred. The Veritas Backup Reporter Management Server attempts to match this alert against Veritas Backup Reporter's business views based on this value.
- agent *agentName*  
Veritas Backup Reporter Agent on which the events occurred.
- ip *IPAddress*  
(Optional) IP address on which the events occurred.  
*IPAddress* must be a valid IP address.
- alertGroup *groupName*  
(Optional) Alert group to which the events belong, that is, failure, partial success.
- alertKey *key*  
(Optional) Alert key to which the events belong, usually used for error code information.
- otherInfo1 *fieldName*  
(Optional) Custom field for extra information.
- otherInfo2 *fieldName*  
(Optional) Custom field for extra information.
- eventTime *time*  
(Optional) Time (in milli-seconds) that the event occurred.  
The valid format is a number.
- notify true | false  
(optional) `true` or `false`; (replaces `sendTrap` parameter in version 3.5) internally sets different alert types. You can configure notification (that is, SNMP traps, email, write to the system log, perform commands through a policy on the server). If set to `true`, the type is set against `Event Poster - Notify`, otherwise, against `Event Poster - No Notify`.

## NOTES

`eventposter` resides by default in `/opt/VRTSccsvs/bin/goodies` (Solaris). The Windows version is named `eventposter.bat` and resides in `\Program Files\Symantec\Veritas Backup Reporter\Server\util`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

## EXAMPLE

The following example demonstrates the posting of an alert that has a severity of three, is in the Failure alert group, and contains the string, "Error Occurred:". It is created against the alert type `Event Poster - Notify` that can be defined through a policy on the Veritas Backup Reporter Management Server to send traps, emails, write to system log, or perform commands:

```
eventposter -server myServer -port 1556 -usr admin -password mypswd  
-domainName myDomain -domainType nt -agent myAgent -node myNode -ip  
127.0.0.1 -alertGroup Failure -severity 3 -otherInfo1 23 -otherInfo2  
31s -Summary "Error Occurred" -notify true
```

## SEE ALSO

[jobutility](#)

# jobutility

`jobutility` – reports on backup job activity in the VBR database

## SYNOPSIS

```
jobutility.sh [--host hostName] --server serverName --port portNumber  
--usr username--passwd password--domain domainName--domaintype  
domainType
```

## DESCRIPTION

`jobutility` is a script that queries the Veritas Backup Reporter database and reports on backup activity.

## OPTIONS

`--host hostName`

Name of the host for which you want backup job information. (Use the host name only, not the host IP address or qualified host name.)

Omit the `--host` option if searching over all backup jobs.

`--server serverName`

Name of the Veritas Backup Reporter Management Server host to which you want to connect.

`--port portNumber`

Port number to use to connect to the specified server. The default is 1556.

`--usr username`

A valid user account with which to connect to the specified server.

`--passwd password`

The password for the specified user name used to connect to the server.

`--domain domainName`

Name of the network domain of which the specified user account is a member.

The default is the private domain name (`cc_users`).

`--domaintype domainType`

The type of network domain specified: NIS, NT, or a private domain. Valid entries are: `nis`, `nt`, or `vx`.

The default is private domain (`vx`).

## NOTES

If you specify `host hostName`, then `jobutility.sh` outputs information about the `hostName`'s first and last backup job. If you specify no `host hostName` option, then `jobutility.sh` outputs information about the first and last job (across all hosts) in the database.

To display a help page listing script options and a brief description for each, specify no options when running `jobutility.sh`.

`jobutility.sh` resides by default in `/opt/VRTSccsvs/bin/goodies` (Solaris). The Windows version is named `jobutility.bat` and resides in `\Program Files\Symantec\Veritas Backup Reporter\Server\util`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

## EXAMPLE

When you use the following command:

```
jobutility --usr Administrator --pass mypasswd --server myHost --port
1556 --domain cc_users@myHost.myCompany.com --domaintype nis
```

The `jobutility` command returns output similar to the following:

```
-----
SubJob Information (Entry for Each SubJob)
-----
Directory/Filesystem Name :
Primary ID                 :
Size                       :
File Count                 :
Management Groups        :
-----
Attempt Information (Entry for Each Attempt)
-----
Attempt Sequence          :
Secondary ID              :
Throughput                :
Size                     :
File Count                :
Status                    :
Status Code               :
```

```
Start Time          :  
Finish Time        :
```

-----  
Finished Job Information  
-----

```
Primary Id         :  
Secondary Id      :  
Client Name       :  
Client ProductID  :  
Master Server Name :  
Media Server Name :  
Product Name      :  
Product Version   :  
Agent Host        :  
Job Type          :  
Level             :  
Throughput        :  
Total Size        :  
Try Count         :  
File Count        :  
Status            :  
Status Code       :  
Start Time        :  
Finish Time       :  
Expiration Time   :  
Policy Domain name :  
Policy Name       :  
Policy Keyword    :  
Schedule Name     :
```

## SEE ALSO

[eventposter](#)

[runstoredquery](#)

# runstoredquery

`runstoredquery` - runs queries created with the VBR Saved Query Tool

## SYNOPSIS

```
runstoredquery.sh -qid  
queryID [-filetype {htm} | {csv [-noheader]}}
```

## DESCRIPTION

`runstoredquery.sh` is a Veritas Backup Reporter script you can use to run custom SQL queries of Veritas Backup Reporter's database of logged events, backup jobs, media usage, and change requests. The custom query is first created with the Saved Query Tool in the Veritas Backup Reporter console. `runstoredquery.sh` outputs the data to the Solaris console, or as HTML or comma-delimited format (CSV) files. As with most shell scripts, you can schedule `runstoredquery.sh` and email its output.

For more information, see the Solaris documentation for the `cron` and `mail/mailx` commands.

## OPTIONS

`-qid queryID`

Specifies the query ID for the custom query you want to run.

*queryID* must be a valid identifier for the custom query created with the Saved Query Tool.

`-filetype htm | csv`

Specifies the type of output `runstoredquery.sh` generates. `htm` causes `runstoredquery.sh` to output the query in HTML format. `csv` causes `runstoredquery.sh` to output the query in comma-delimited format.

`-noheader`

Applies to `-filetype csv` only. Causes `runstoredquery.sh` to create the comma-delimited file without a heading line. (`-noheader` can be useful for customers who want to import the script output into an external billing application without having to manually remove the header line.)

## NOTES

If you run `runstoredquery.sh` without the `-filetype` option, `runstoredquery.sh` outputs to the Solaris console.

You specify the output file and path with the Saved Query Tool in the Veritas Backup Reporter console.

`runstoredquery.sh` resides by default in `/opt/VRTSccsvs/bin/goodies` (Solaris). The Windows version is named `runstoredquery.bat` and resides in `\Program Files\Symantec\Veritas Backup Reporter\Server\util`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

## EXAMPLES

### EXAMPLE 1:

The following example displays to a Solaris console the results from query ID 7:

```
sh runstoredquery.sh -qid 7
```

### EXAMPLE 2:

This example causes `runstoredquery.sh` to output query ID 7 in HTML format:

```
sh runstoredquery.sh -qid 7 -filetype htm
```

The output path and filename is defined when the query is created.

### EXAMPLE 3:

This command outputs query ID 7 in comma-delimited (CSV) format:

```
sh runstoredquery.sh -qid 7 -filetype csv
```

## SEE ALSO

[jobutility](#)

# support

`support` – collects VBR data for troubleshooting

## SYNOPSIS

```
support [ options]
```

## DESCRIPTION

`support` is a script used for collecting Veritas Backup Reporter data used by Veritas Technical Support in troubleshooting. You can also use `support` for running EMC Legato Networker Command-Line Interfaces (CLIs). `support` produces a compressed file with the following types of information: log files, Veritas Backup Reporter Management Server and Veritas Backup Reporter Agent configuration files, and Veritas NetBackup Command-Line Interface (CLI) summaries.

## OPTIONS

- `-s [true|false]`  
Include Veritas Backup Reporter Management Server information.
- `-a [true|false]`  
Include agent information.
- `-c [true|false]`  
Include View Builder information.
- `-f filename`  
Compresses output (zip format) to *filename*.
- `-d directoryName`  
Overrides the default directory where `support` writes its compressed output file and its log.  
If the specified directory does not exist, `support` terminates.
- `-noconsole`  
Do not log to console.  
The created zip file has the machine's hostname in the name:  
`support-hostName`
- `-h`  
Displays help information for `support`.

## NOTES

`support` resides on the Veritas Backup Reporter Management Server, Veritas Backup Reporter Agent, and View Builder host in the following locations by default:

**Veritas Backup Reporter Management Server:** `/opt/VRTSccsvs/bin`

`\Program Files\Symantec\Veritas Backup Reporter\Server\util`

**Veritas Backup Reporter Agent:**

`/opt/VRTSccsva/bin`

`\Program Files\Symantec\Veritas Backup Reporter\Agent\bin`

**View Builder:**

`/opt/VRTSccsvb/bin`

`\Program Files\Symantec\Veritas Backup Reporter\ViewBuilder\bin`

The Windows version is named: `support.exe`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

Unless changed with the `-f` and `-d` options, `support` compresses its output to the following default path and filename:

Solaris            `/var/tmp/support-hostname.zip`

Windows          `\DOCUME~1\ADMINI~1\LOCALS~1\username\Temp\support-hostname.zip`

## EXAMPLE

The following examples show output similar to what you see when you run `support`. The first three lines are for the three major components of Veritas Backup Reporter. After that, if the Veritas Backup Reporter Agent is installed, a menu appears with all your configured Veritas NetBackup Agent modules, and you can select the modules you are troubleshooting.

### EXAMPLE 1:

The following input and output is representative of an interactive session where the user specified `support` to collect information for all three Veritas Backup Reporter components and specified one configured Veritas NetBackup Agent Module:

```
C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util>support.exe
Do you want to include server information (yes/y/no/n) [yes]?y
Do you want to collect data from the DB (must be running)
(yes/y/no/n) [yes]?y
Do you want to include Agent information (yes/y/no/n) [yes]?y
Do you want to include Agent Module information (yes/y/no/n) [yes]?y
Please select the Module(s) for which you wish to collect
debugging information:

    0) VERITAS BackupExec on server1.domainname.com
    1) VERITAS BackupExec on server2.domainname.com
    2) VERITAS BackupExec on server3.domainname.com
    3) VERITAS NetBackup on server4.domainname.com
    4) Select All
    5) Commit Selection
?:2
Please select the Module(s) for which you wish to collect
debugging information:

    0) VERITAS BackupExec on server1.domainname.com
    1) VERITAS BackupExec on server2.domainname.com
    2) VERITAS BackupExec on server3.domainname.com [SELECTED]
    3) VERITAS NetBackup on server4.domainname.com
    4) Select All
    5) Commit Selection
?:5
Do you want to include view builder information (yes/y/no/n) [yes]?y
Gathering server logs...
    Added 19 log files from the server
Gathering server configuration...
    Added Web-App configuration file from the server
Gathering Agent listing...
Gathering CCSvc DB data..
Connecting to DB on localhost:2994 ...
ran 23 queries from properties file.
ran 0 queries from disk.
Disconnecting from DB localhost ...
Gathering CCSvc DB data complete.
Gathering Agent logs...
Agent log directory is:
C:\Program Files\Symantec\Veritas Backup Reporter\Agent\logs
    Added 14 log files from Agent directory
```

```
Gathering Agent configuration...
    Added 1 Agent configuration files.
Gathering Agent listing...
Collecting VERITAS BackupExec Agent Module data for server3.domainname.com..
.
Gathering view builder logs...
Gathering Agent listing...
Gathering install/uninstall logs...
Gathering Agent version...
Picking up log file.

The Veritas Backup Reporter support data has been collected and placed in:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\support-host.zip
Please send it to your Symantec contact.
```

Collector Successful

```
C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util>
```

#### EXAMPLE 2:

**The following input and output is representative of an interactive session where the user specified `support` to collect information for all three Veritas Backup Reporter components and specified no configured Veritas NetBackup Agent Module:**

```
Do you want to include server information (yes/y/no/n) [yes]?
Do you want to include Agent information (yes/y/no/n) [yes]?
Do you want to include Agent Module information (yes/y/no/n) [yes]?
No Agent Modules were found...
Do you want to include view builder information (yes/y/no/n) [yes]?
Gathering server logs...
    Added 26 log files from the server
Gathering server configuration...
    Added configuration files from the server
Gathering Agent listing...
Gathering Agent logs...
Agent log directory is :C:\Test Directory\Veritas Products\
Veritas Backup Reporter\Service\Agent\logs
    Added 4 log files from Agent directory
Gathering Agent configuration...
    Added 1 Agent configuration files.
```

```
Gathering Agent listing...
No valid modules were executed.
Gathering view builder logs...
No Client log file found.
Gathering Agent listing...
Gathering install/uninstall logs...
Gathering Agent version...
Picking up log file.
```

```
The Veritas Backup Reporter support data has been
collected and placed in:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\support-host.zip
Please send it to your Symantec contact.
```

# xml

xml – imports and exports object views to and from VBR

## SYNOPSIS

```
xml {-I | -e} {-f filename [--hosthostname] [--port port] --usr  
username [--pass password] --domaindomainName --domaintype domainType  
[--broker brokerHostname] [--brokerport port] [-v errorLevelNumber  
] [-l logFilename] --type [csv | tsv | xml] --forceMerge}
```

## Description

xml is a script used to import and export object views to and from Veritas Backup Reporter Management Servers.

## Options

- I  
Import XML mode.
- e  
Export XML mode.
- f *filename*  
Name of the XML file to use for import or export.
- host *hostname*  
(Optional) name of the Veritas Backup Reporter Management Server you want to connect to. *Hostname* can be either a hostname, IP address, or a fully qualified domain name. For example: `myHostname`, `0.0.0.0`, or `myhost.example.com`  
  
If no *Hostname* is supplied, the script defaults to the local host.
- port *port*  
(Optional) the port for the Veritas Backup Reporter Management Server you are connecting to. If no *port* is specified, the script uses port 1556.
- usr *username*  
The user account name used for authenticating your connection to the Veritas Backup Reporter Management Server host. Specify a system account valid for the host you are connecting to.

**--pass** *password*

The user account password used for authenticating your connection to the Veritas Backup Reporter Management Server host.

`xml` checks for the stored password in its first attempt to connect to the Veritas Backup Reporter Management Server. If the password is not present, then re-run `xml` and supply the password for the specified account.

**--domain** *domainName*

The name of the domain to which the user belongs (default, `cc_users`) and that the Symantec Product Authentication Service uses to authenticate users.

**--domaintype** *domainType*

The type of the domain to which the specified user belongs. Valid domain types are: `nis`, `nt`, or `vx` (default).

**--broker** *brokerHostname*

(Optional) the name of the Symantec Product Authentication Service broker host. The default is the Veritas Backup Reporter Management Server host.

**-brokerport** *port*

(Optional) the port for the Symantec Product Authentication Service broker host you are connecting to. If no *portNumber* is specified, the script uses port 2821.

**---select** *options*

(Optional) object selection options that can be the following: view (`view=name`), object name (`objname=name`), object type (`objname=name`), object ID (`objid=name`).

**-v** *errorLevelNumber*

(Optional) turns logging on (default) and off and controls the type of errors that the script outputs.

*ErrorLevelNumber* is a number 0-8, whose meaning is described below:

0—(Off)

1—Severe

2—Warning

3—Info

4—Config

5—Fine

6—Finer

7—Finest

## 8—All error messages

### -l *logFilename*

(Optional) a log file that the XML script creates to capture script error messages. By default, logging is on and outputs to the console or command prompt. *logFilename* can be any valid file name. The script writes the log file to the current directory.

### --type *option*

A file type that you use to import or export views. If you do not specify a file type, views are imported or exported as xml by default.

*option* is a file type, such as csv (comma-separated value), tsv (tab-separated value), or xml

### --forcemerge

A command which you can use to merge the specified objects forcefully, when you are sure that they represent the same backup clients that were discovered by the same source

## Notes

xml resides by default in: /opt/VRTSccsva/bin (Solaris only). Its Windows counterpart (xml.bat) resides by default in: \Program Files\Symantec\Veritas Backup Reporter\Server\util

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's PATH environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

## Examples

### EXAMPLE 1:

In the following example, xml selects the `tape_drive` object in the `backup_view` to export to a file in /var named `export.xml`. Logging is turned on and outputs to the operating system console or command prompt for all error levels is as follows:

```
xml.bat -e -f /var/export.xml --host myhost1.example.com
--usr admin --pass
password --domain cc_users@myhost1.example.com --domaintype vx
--select
view=backup_view;objname=tape_drive --l backup_view_export.log
-v 8
```

**EXAMPLE 2:**

In the following example, `xml` imports an object view (`export.xml`) to a Veritas Backup Reporter Management Server host (`myhost2`). Logging is turned off as follows:

```
xml --host myhost2.example.com --usr admin
    --pass password --domain
cc_users@myhost2.example.com --domaintype vx -I -f /var/export.xml
    -v 0
```

## See also

[vbrvb](#)

[vbrserver](#)

# agentauth

`agentauth` – authenticates the Veritas Backup Reporter Agent with the Symantec Product Authentication Service.

## SYNOPSIS

```
agentauth { [password] -server serverHostName [-port port] [{  
-brokerhost brokerHostName [-brokerport port] [-domainnamesuffix  
brokerHostName] }] | h
```

## Description

`agentauth` authenticates the Veritas Backup Reporter Agent with the Symantec Product Authentication Service (AT).

## Options

### *password*

(Optional) password associated with the account used by AT to authenticate the Veritas Backup Reporter Agent. Required only when this internal account (`ccsvc_Agent`) is changed.

### `-server serverHostName`

(Required) name of the Veritas Backup Reporter Management Server against which you are authenticating the Veritas Backup Reporter Agent.

`serverHostName` should be the fully qualified host name, or in clustered situations, the cluster name. If no `serverHostName` is supplied, `agentauth` defaults to the local host.

### `-port port`

(Optional) port number on the Veritas Backup Reporter Management Server used to connect with the Veritas Backup Reporter Agent. (The default port is 1556.)

### `-brokerhost brokerHostname`

The fully qualified host name of the AT broker host or the fully qualified DNS name for the virtual IP or the cluster name of the AT broker host.

`-brokerhost` requires `-server`

Use `-brokerhost` when the Veritas Backup Reporter Agent resides on a host other than the Veritas Backup Reporter Management Server host. Use

`-brokerhost` with `-domainnamesuffix` when the Veritas Backup Reporter

Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are not fully qualified in AT.

**-brokerport** *port*

(Optional) the port for the AT broker host that the Veritas Backup Reporter Management Server connects to. By default, AT listens to port 2821.

**-domainnamesuffix** *brokerHostName*

Modifies the AT broker host name in situations when the Veritas Backup Reporter Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are not fully qualified in AT.

**-domainnamesuffix** requires **-brokerhost** and **-server**

*brokerHostName* is either the AT broker host cluster name or the AT broker fully qualified host name.

**-h**

Displays command-line help information for `agentauth`.

## Notes

`agentauth` resides by default in: `/opt/VRTSccsva/bin` (Solaris only). Its Windows counterpart (`agentauth.exe`) resides by default in:

`\Program Files\Symantec\Veritas Backup Reporter\Agent\bin`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

If the Veritas Backup Reporter Agent cannot connect to the Veritas Backup Reporter Management Server, a message such as the following appears in the Veritas Backup Reporter Agent log:

```
Authentication failed
The user or password are not valid in the given domain.
Domain="ccsvc_services@myServer", User="ccsvc_Agent"
```

By default, the Veritas Backup Reporter Agent logs are located:

**Solaris**            `/opt/VRTSccsva/logs`

**Windows**        `\Program Files\Symantec\Veritas Backup Reporter\Agent\logs`

The agent should have been authenticated during installation, but could have failed for a number of reasons, including not starting the Veritas Backup Reporter Management Server when the Veritas Backup Reporter Agent was installed.

`agentauth` can fail for a number of reasons. Below are two of the most common issues:

The AT libraries are not in the PATH. In this case, reboot the Veritas Backup Reporter Agent machine or specify the absolute path to the libraries:

**Solaris**            Update `LD_LIBRARY_PATH` to include `/opt/VRTSat/lib`

**Windows**            `\Program Files\Veritas\Security\Authentication\bin` PATH changes do not take affect over Windows Terminal Services unless you log out and log back in.

Make sure the server is running, and can be reached on port 1556.

To get a list of private domains known to the Symantec Product Authentication Service (AT), type the following command on a Veritas Backup Reporter Management Server:

**Solaris**            `/opt/VRTSat/bin/vssat showallbrokerdomains`

**Windows**            `\Program Files\Veritas\Security\Authentication\bin\vssat showallbrokerdomains`

## Examples

The following examples assume that AT is installed on the same machine as the Veritas Backup Reporter Management Server.

### EXAMPLE 1:

The following command authenticates the Veritas Backup Reporter Agent with the Symantec Product Authentication Service (AT). Both the Veritas Backup Reporter Agent and the Veritas Backup Reporter Management Server reside on the same host, `Veritas Backup Reporter.example.com`:

```
agentauth mypasswd -server Veritas Backup Reporter.example.com
```

### EXAMPLE 2:

The following command authenticates the Veritas Backup Reporter Agent with AT, when the Veritas Backup Reporter Agent is installed on a different host than the Veritas Backup Reporter Management Server (`Veritas Backup Reporter.example.com`):

```
agentauth mypasswd -server Veritas Backup Reporter.example.com -brokerhost  
Veritas Backup Reporter.example.com
```

**EXAMPLE 4:**

The following command authenticates the Veritas Backup Reporter Agent with AT, when the Veritas Backup Reporter private domain (`cc_users`) is not fully qualified in AT:

```
agentauth mypasswd -server Veritas Backup Reporter.example.com -brokerhost  
Veritas Backup Reporter.example.com -domainNameSuffix Veritas Backup Report
```

## See also

[vbr\\_conf.properties](#)

[vbragent](#)

# dbbackup

`dbbackup` – backup up the VBR database on Solaris systems

## SYNOPSIS

```
dbbackup {backupDir | -restore [restoreDir]} [-o [logfile]]
```

## Description

`dbbackup` is a script used for backing up the Veritas Backup Reporter database.

## Options

### *backupDir*

(Required) *backupDir* is the directory where the Veritas Backup Reporter database is backed up to, or restored from. *backupDir* should be an absolute path.

### restore *restoreDir*

(Optional) *restoreDir* is the directory where the Veritas Backup Reporter database is restored. If not included, `dbbackup` restores the database to the default data directory (`/var/Veritas/ccs_data`). *restoreDir* should be an absolute path.

### -o *logfile*

Record backup and restore actions to a log file. If *logfile* is unspecified, output is written to the current directory.

## Notes

`dbbackup` resides by default at the following locations:

On Solaris: `/opt/VRTSccsvs/bin`

On Windows: `\Program Files\Symantec\Veritas Backup Reporter\Server\util`

On Windows, you perform backups with the `DbBackup.bat` batch file.

The backup script creates the following files in the backup directory: `ccsvc.db` and `ccsvc.log`

Data spaces are started when the main database (`ccsvc.db`) is started; therefore, starting and stopping the data space file is not required.

Both the Solaris and the Windows scripts automatically stop and restart the database.

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

## Examples

**EXAMPLE 1:** The following command backs up the Veritas Backup Reporter database to the `my_db_backups` directory:

```
/opt/VRTScsashd/bin/dbbackup /my_db_backups
```

**EXAMPLE 2:** The following command restores a previously backed up Veritas Backup Reporter database to the `/var/Veritas/ccs_data` directory. Logging is turned on to write restore-related messages to a log. Because a log directory is not specified, the log is written to the current directory (`/opt/VRTScsashd/bin`):

```
/opt/VRTScsashd/bin/dbbackup/my_db_backups -restore  
/data/cc_database -o
```

## See also

[vbrserver](#)

# vbrserver

`vbrserver` - performs start up and shut down on Solaris systems for the VBR Management Server and its dependencies

## SYNOPSIS

```
vbrserver { stop | start | status } [serverProcess]
```

## Description

`vbrserver` is the startup and shutdown script (Solaris only) for the Veritas Backup Reporter Management Server and one or all of its dependencies: Veritas Backup Reporter Alert Manager, Veritas Backup Reporter database, Symantec Product Authentication Service (AT), Veritas Backup Reporter Trap Processor, Symantec Private Branch Exchange, and the Veritas Backup Reporter Active Practices.

On Windows, use the Windows Services applet.

## Options

`stop` [*serverProcess*]

Terminates the Server and its dependencies.

If *serverProcess* is omitted, `vbrserver` terminates the Veritas Backup Reporter Management Server and Active Practices only. `stop force` terminates the Veritas Backup Reporter Management Server and all its dependencies (including dependencies shared with other Veritas products).

(Optional) *serverProcess* can be one of the following values: `vxccsvs` (Veritas Backup Reporter Management Server), `vas` (Symantec Product Authentication Service), `vxdbms_d` (Server DBMS only), `bram` (Alert Manager), `vxtrapd` (Trap Processor), `pm` (Active Practices), `vxpbx` (Symantec Private Branch Exchange), and `force` (use with `stop` only).

`start` [*serverProcess*]

Starts the server and its dependencies.

If *serverProcess* (see earlier definition) is omitted, starts the Veritas Backup Reporter Management Server and all its dependencies. Otherwise, starts only the specified server process.

`status` [*serverProcess*]

Identifies whether the Veritas Backup Reporter Management Server and its dependencies are running without starting or stopping a server process.

If *serverProcess* (see earlier definition) is omitted, displays status for all the Veritas Backup Reporter Management Server and all its dependencies. Otherwise, shows status for only specified server process.

## Notes

`vbrserver` can start and stop the Veritas Backup Reporter Management Server and one or all of its dependencies (shared or otherwise), while its companion script, `vbrweb` only starts and stops the server. The Veritas Backup Reporter Management Server is a Symantec Web Server application. `vbrserver` and `vbrweb` only terminates the Web server if no other Symantec Web server applications are running on the host.

You can specify only one *serverProcess* argument at a time. For example, to stop two Veritas Backup Reporter Management Server dependencies, you must issue two separate commands. For example, the command stops the Alert Manager, and the second command stops the Symantec Product Authentication Service:  
`vbrserver stop bramvbrserver stop vas`

`vbrserver` resides by default in: `/opt/VRTSccsvs/bin` (Solaris only).

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

On Windows, the Veritas Backup Reporter Management Server is installed as a service that starts automatically.

## Examples

### EXAMPLE 1:

The following command stops Veritas Backup Reporter Management Server and all its dependencies (including dependencies shared with other Veritas products):

```
vbrserver stop force
```

### EXAMPLE 2:

The following command stops the Veritas Backup Reporter Management Server and Active Practices only. The remaining Veritas Backup Reporter Management Server dependencies (see earlier list) are not stopped:

```
vbrserver stop
```

### EXAMPLE 3:

The following command stops the Trap Processor only:

```
vbrserver stop vxtrapd
```

**EXAMPLE 4:**

The following command starts the Veritas Backup Reporter Management Server and all its dependencies (see earlier list):

```
vbrserver start
```

**EXAMPLE 5:**

The following command starts the Veritas Database Management System only:

```
vbrserver start vxdbms_d
```

**EXAMPLE 6:**

The following command indicates if the Veritas Backup Reporter Management Server and any of its dependencies are running:

```
vbrserver status
```

## See also

[vbr\\_conf.properties](#)

[xml](#)

[vbragent](#)

[vbrvb](#)

[vbrweb](#)

# vbragent

`vbragent` – performs start up and shut on Solaris systems for the VBR Agent

## SYNOPSIS

```
vbragent { start | stop | status | version }
```

## Description

`vbragent` is the (Solaris only) startup and shutdown script for the Veritas Backup Reporter Agent.

## Options

`start`

Starts the Veritas Backup Reporter Agent.

`stop`

Terminates the Veritas Backup Reporter Agent.

`restart`

Stops and then starts the Veritas Backup Reporter Agent.

`status`

Identifies whether the Veritas Backup Reporter Agent is running.

`version`

Displays `vbragent` version and copyright information.

## Notes

`vbragent` resides by default in: `/opt/VRTSccsva/bin` (Solaris only).

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

An agent's configuration is stored in the Veritas Backup Reporter database and the agent caches the most recent version of its configuration locally in `Agent.conf`. The agent periodically compares `Agent.conf` with the one stored in the database, uses whichever is most recent, and modifies the earlier version to keep it up to date. If the last modified time for `Agent.conf` is later than the timestamp for the configuration stored on the server, the agent uses the local configuration and

updates the configuration stored on the server. Otherwise, the agent uses the configuration stored on the server host and overwrites the locally cached configuration.

Logging for the core agent and individual agent explorers is administered in the same fashion but written to different log files. The core agent writes to `ccsvcAgent-core-#.log`. Individual agent explorers write to `ccsvcAgent-<ExplorerName>-<InstanceNumber>-<ProductHost>-#.log`. **Standard error output (stderr) is redirected to `ccsvcAgent-err-#.log`.**

`InstanceNumber` is the instance identifier that is to the module when it is configured. `ProductHost` is the host that the agent module is using to collect data with all periods (‘.’) replaced by underscores (‘\_’).

When the log file reaches a certain maximum file size, it is rolled over (purged). The pound sign (#) in the log file name indicates the number of times that the log file has rolled over. The lower the rollover number, the more recent the log file.

On Windows, `vbragent` is installed as a service that starts automatically.

By default, the Veritas Backup Reporter Agent logs are located as follows:

Solaris	<code>/opt/VRTSccsva/logs</code>
Windows	<code>\Program Files\Symantec\Veritas Backup Reporter\Agent\logs</code>

## See also

[agentauth](#)

[vbrvb](#)

# vbrvb

`vbrvb` – runs the Veritas Backup Reporter View Builder (Java) GUI.

## SYNOPSIS

```
vbrvb [version]
```

## Description

`vbrvb` runs the Veritas Backup Reporter View Builder GUI—a Java application in which an administrator creates, modifies, and manages access to object views that users see in the Veritas Backup Reporter Console. Veritas Backup Reporter also ships with a Flash-based View Builder.

For more information, see “Managing Veritas Backup Reporter Views.”

## Options

`version`

Displays `vbrvb` version and copyright information.

## Notes

`vbrvb` resides by default in: `/opt/VRTSccsva/bin` (Solaris only).

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host’s `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

On Windows, you access the View Builder from either the Veritas Backup Reporter Console or directly from the Windows Start menu.

## See also

[vbragent](#)

[vbrserver](#)

# changedbpassword

`changedbpassword` – changes the VBR database password

## SYNOPSIS

```
changedbpassword [--setGuestPassword=<guest  
password>] [--setDBAPassword=<DBA  
password>] [--setServerPassword=<server password>] | [--restoreDefault]  
| [-h|-?|--help]
```

## Description

Sybase SA (SQL Anywhere) database management system is used to store the Veritas Backup Reporter data. You require a user name and a password to access the database. The following database user accounts are shipped with Veritas Backup Reporter:

<code>guest</code>	A read-only account with 'guest' as a password. The guest account is not used by the Veritas Backup Reporter Management Server. It can currently be changed by using the tools provided for accessing the database.
<code>ccsvc</code>	An account used by the Veritas Backup Reporter Management Server to access the database. This account can access all database tables of Veritas Backup Reporter.
<code>dba</code>	The database administrator account. The dba account is required by the database queries that are used to update the database schema or upgrade to a new product version.

The `guest` account can have its password changed already with no impact to the rest of the product. For consistency, the provided tool can update the `guest` password in addition to changing the `ccsvc` and `dba` user passwords. When the tool changes the `ccsvc` or `dba` password, it updates a configuration file on the file system so that the server can still access the database. The password is encrypted before it is stored in the configuration file. However, since the server needs to retrieve the password it cannot be stored with a one-way hash. Thus, someone could obtain the password. When the tool is run, the system administrator is advised to check the permissions on the configuration file to ensure that only an administrator can read the file. The server uses the `vbr_conf.properties` configuration file to read in configuration values. This configuration file is used to store the encrypted passwords.

## Options

- `--setGuestPassword` : Change the database guest password.
- `--setDBAPassword` : Change the database DBA password.
- `--setServerPassword` : Change the password used by the server to log into the database.
- `--restoreDefault` : Reset all the passwords to default passwords.
- `--h|-?|--help` : Show this usage statement and exit.

## Notes

If you did not specify any user account in options, all passwords change to the values that you specify.

For example, you can change the password of the user account that is specified in the option. The default operation is to change all passwords. The password is prompted for. To specify the password on the command line, use an equals and specify the password. `ccsvc-changedbpassword --setGuestPassword=tseug --setDBAPassword` This sets the guest password to “tseug” and prompts for a DBA password.

## Examples

You can change database account passwords by entering the following command in the command-line:

```
changedbpassword.exe --setGuestPassword=testpassword  
--setDBAPassword
```

The `changedbpasswordutility` sets the guest password to ‘testpassword’ and prompts you to enter a new DBA (database administrator) password.

After running the `changedbpassword` utility, set the permissions of the `vbr_conf.properties` file so that only a system administrator can read the file.

# vbrweb

`vbrweb` – startup and shutdown script for the Veritas Backup Reporter Management Server

## SYNOPSIS

```
vbrweb start | stop | restart | status | version
```

## Description

`vbrweb` is the (Solaris-only) startup and shutdown script for the Veritas Backup Reporter Management Server.

## Options

**start**

Starts the Veritas Backup Reporter Management Server.

**stop**

Terminates the Veritas Backup Reporter Management Server.

**restart**

Stops and then starts the Veritas Backup Reporter Management Server.

**status**

Identifies whether the Veritas Backup Reporter Management Server is running.

`status` does *not* report on any processes on which the server is dependent.

**version**

Displays `vbrweb` version.

## Notes

`vbrweb` can start and stop the Veritas Backup Reporter Management Server only, while its companion script, `vbrserver` can start and stop the server and one or all of its dependencies (shared or otherwise). The Veritas Backup Reporter Management Server is a Symantec Web Server application. `vbrserver` and `vbrweb` only terminate the Web server if no other Symantec Web server applications are running on the host.

`vbrweb` resides by default in: `/opt/VRTSccsvs/bin` (Solaris only).

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to avoid changing the directory in order to run the Veritas Backup Reporter command or script.

On Windows, the Veritas Backup Reporter Management Server is installed as a service that starts automatically.

## See also

[xml](#)

[vbrserver](#)

[vbragent](#)

[vbrvb](#)



# XML interface reference

This appendix includes the following topics:

- [About the XML API](#)
- [About the XML DTD](#)
- [About the DTD elements](#)
- [Examples of XML files](#)

## About the XML API

You can create views in the Veritas Backup Reporter (Veritas Backup Reporter) by creating and importing XML files that describe the views.

By using the Veritas Backup Reporter XML API, you can import IT asset data and their relationships that you maintain through in-house or third-party systems (for example, Peregrine AssetCenter). The XML import capability enables you to import arbitrary groupings of hosts and file systems, for example, groupings defined around business units.

The following examples illustrate the practical use of Veritas Backup Reporter's XML import functionality.

**Example 1:** You can use a spreadsheet to define Host A as the marketing host and Host B as the sales host. Using the XML import function in Veritas Backup Reporter, you can import the data in the spreadsheet, create a view using the imported data, and chargeback the services based on business units.

**Example 2:** You can build a view of a chart of accounts showing server ownership by company department for chargeback purposes. With large enterprises, the chart of accounts can easily exceed a thousand. Entering this data into Veritas Backup Reporter is cumbersome and error prone. By using the XML import functionality, you can import this data from your local system. While importing

the data into Veritas Backup Reporter, you can continue with the maintenance of the data in the local system.

Importing data using the XML API is the best example of Veritas Backup Reporter's open architecture that enables integration with other systems.

## About the XML DTD

The XML DTD is constructed as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT application (objects?,view*,user*,mergeitems*)>1
  <!ATTLIST application version CDATA #REQUIRED>
<!ELEMENT objects (object+)>
<!ELEMENT view (node*,aliaslevels?)>
  <!ATTLIST view identifier CDATA #REQUIRED>
  <!ATTLIST view action (add|delete|update|declare) "declare">
  <!ATTLIST view id ID #IMPLIED>
<!ELEMENT object (attribute*)>
  <!ATTLIST object id ID #IMPLIED>
  <!ATTLIST object name CDATA #IMPLIED>
  <!ATTLIST object action (add|delete|update|declare) "declare">
  <!ATTLIST object type CDATA #IMPLIED>
  <!ATTLIST object master IDREF #IMPLIED>
  <!ATTLIST object dbid CDATA #IMPLIED><!ELEMENT node (object?,node*)>
  <!ATTLIST node id ID #IMPLIED>
  <!ATTLIST node action (add|delete|declare) "declare">
  <!ATTLIST node object IDREF #IMPLIED>
  <!ATTLIST node parents IDREFS #IMPLIED>
<!ELEMENT aliaslevels (level*)>
  <!ATTLIST aliaslevels action (add|update|delete|declare) "declare">
<!ELEMENT level EMPTY>
  <!ATTLIST level number CDATA #REQUIRED>
  <!ATTLIST level label CDATA #REQUIRED>
<!ELEMENT user EMPTY>
  <!ATTLIST user action (add|delete) "add">
  <!ATTLIST user login CDATA #REQUIRED>
  <!ATTLIST user domainName CDATA #REQUIRED>
  <!ATTLIST user domainType CDATA #REQUIRED>
  <!ATTLIST user firstName CDATA #IMPLIED>
  <!ATTLIST user lastName CDATA #IMPLIED>
  <!ATTLIST user email CDATA #IMPLIED>
  <!ATTLIST user accessLevel (admin|adminReadOnly|user|default) "default">
```

```
<!ATTLIST user department CDATA #IMPLIED>
<!ATTLIST user costCenter CDATA #IMPLIED>
<!ATTLIST user workNumber CDATA #IMPLIED>
<!ATTLIST user mobileNumber CDATA #IMPLIED>
<!ATTLIST user pagerNumber CDATA #IMPLIED>
<!ELEMENT mergeitems (mergeitem+)>
<!ELEMENT mergeitem EMPTY>
<!ATTLIST mergeitem toobject IDREF #IMPLIED>
<!ATTLIST mergeitem fromobject IDREF #IMPLIED>
<!ELEMENT attribute (name,value*)>
<!ATTLIST attribute name CDATA #IMPLIED>
<!ATTLIST attribute value CDATA #IMPLIED>
<!ELEMENT value (#PCDATA)>
```

## About the DTD elements

The elements of the XML DTD are as follows:

- [About the <application> element](#)
- [About <objects> and <object> elements](#)
- [About <attribute> elements](#)
- [About the <view> element](#)
- [About <node> elements](#)
- [About <user> elements](#)
- [About <mergeitems> and <mergeitem> elements](#)

### About the <application> element

The <application> element is the root level tag that encloses rest of the XML definitions. This tag contains <objects> tag and zero or more other tags, namely <view>, <users>, and <mergeitems> in this order.

### About <objects> and <object> elements

The <objects> tag holds the definition of the objects to be acted on, and so contains a number of <object> tags. Each object tag represents a single asset in the Veritas Backup Reporter configuration.

Each object has the following properties that define it in the XML file:

<code>id</code>	The ID of the object. This is not the actual object ID but a unique value that identifies the object in the working XML.
<code>name</code>	The actual name of the object.
<code>action</code>	The action to be taken for the object.
<code>add</code>	Add the object.
<code>delete</code>	Delete the object.
<code>update</code>	Update the properties of the object.
<code>declare</code>	No action. You may need this object in XML at a later stage. In some cases, another object already present in the Veritas Backup Reporter configuration may be required to take action using this object (for example, setting it as a master object for a newly defined object). To be able to do that, the object must first be “declared” in the XML.
<code>type</code>	The type of the object. Currently, an object can be one of four types:
<code>Generic_Object</code>	A generic object such as a hierarchical node in the View tree.
<code>Host</code>	A host object.
<code>File_System</code>	A file system object.
<code>Application</code>	An application object.
<code>master</code>	The ID of the master object. An object with this ID should have been in the XML.
<code>dbid</code>	The database ID of the object. This is an optional field and is written when the data is exported. It is very useful in cases where you want to update or declare objects. Because the <code>dbid</code> is actually an ID in the database, lookups are much faster. So, it is recommended to use the <code>dbid</code> to speed up the overall XML processing whenever possible. This ID is entirely database dependant and is created when the object is created. One cannot specify an object to have a specific <code>dbid</code> .

## About <attribute> elements

Each object has a set of attributes that defines it in the Veritas Backup Reporter configuration. These attributes are defined in the <attribute> tag. Each attribute tag can contain a <name> tag and multiple <value> tags. The <name> tag defines the name of the attribute and a <value> tag defines a value for it. There are several ways by which the attribute tags can be defined, such as in the following example:

```
<attribute>
  <name>attrname</name>
  <value>attrvalue 1</value>
</attribute>
```

Or, more simply:

```
<attribute name="attrname" value="attrvalue"/>
```

## About the <view> element

The <view> tag defines a view in the Veritas Backup Reporter configuration. A view is a hierarchical association of objects. So, this tag contains multiple nested <node> tags that define the nodes of the tree. The tree tag contains the following properties:

identifier	The name of the view.
action	The action to be taken for the tree.
add	Create a new view.
delete	Delete an existing view.
update	Update the view.
declare	No action. This defines an already existing tree in the XML.
id	Deprecated and no longer used.

## About <node> elements

A node can be viewed as a container that holds a single object. The same object can be contained in more than one node in the tree, but a node can contain only one object. The properties of nodes are as follows:

id	The unique identifier of the node in XML.
----	---

<code>object</code>	The ID of the object that the node contains. This is the ID given to that object in the working XML file and not the actual ID. There can be multiple parents for a node. In such a case, the parent node IDs should be separated by spaces in the XML.
<code>parent</code>	The node ID of this node's parent node. The current node is added as a child to the specified parent node. This is the ID given to the parent node in the working XML file and not the actual ID.
<code>action</code>	The action to be taken for the node.
<code>add</code>	Add the node to the tree.
<code>delete</code>	Delete the node.
<code>declare</code>	No action. You may need this node in XML at a later stage. In some cases, another node already present in the Veritas Backup Reporter configuration may be required to take action using this node (for example, adding a child node). To use the node in XML as a parent for some other node, the node must first be "declared" in the XML.

## About <aliaslevel> elements

In Veritas Backup Reporter, you can set aliases or labels for levels in views. Using the <aliaslevel> element, you can specify names for view levels. A view contains number levels. By default, the levels are labeled Level 1, Level 2, and Level 3, which is not intuitive. To name the levels as per your requirements, you can use the <aliaslevel> element.

<code>action</code>	The action to be taken for the aliaslevel.
<code>add</code>	Add the level number and level label.
<code>update</code>	Update the level number and level label.
<code>delete</code>	Delete the level number and level label.
<code>declare</code>	Default action.
<code>level number</code>	Enter the level number, for example, 1 or 2.
<code>level label</code>	Enter the label for the level.

## About <user> elements

The <user> tag holds the information about the user to be added to or deleted from the system. The attributes of the <user> tag are explained below. The first

**four attributes** (`action`, `login`, `domainName`, and `domainType`) are mandatory. The remainder are optional.

<code>action</code>	Action to be taken for the user. .
<code>add</code>	Add the user. Specified user gets added in the Veritas Backup Reporter database as well as to the Veritas Security Services.
<code>delete</code>	Delete the user. Specified user gets deleted from the Veritas Backup Reporter database as well as from the Veritas Security Services.
<code>login</code>	Login name of the user.
<code>domainName</code>	Domain name for the user.
<code>domainType</code>	Domain type for the user
<code>firstName</code>	First name of the user.
<code>lastName</code>	Last name of the user.
<code>email</code>	Email address of the user.
<code>accessLevel</code>	Access level assigned to the user. .
<code>admin</code>	Administrator user. An administrator user has all privileges.
<code>adminReadOnly</code>	Administrator user with read-only access. This user can view most of the UI that an administrator can view. The <code>adminReadOnly</code> user cannot access Global Settings.
<code>user</code>	User who does not have administrator or administrator read-only privileges.
<code>default</code>	System default <code>accesslevel</code> . The default is set to <code>user</code> .
<code>department</code>	Department of the user.
<code>costCenter</code>	Optional text field that can be used to store information, such as cost center of the user.
<code>workNumber</code>	Work phone number of the user.
<code>mobileNumber</code>	Mobile phone number of the user.
<code>pagerNumber</code>	Pager number of the user.

## About <mergeitems> and <mergeitem> elements

The <mergeitems> tag holds a number of <mergeitem> tags. Each <mergeitem> tag represents a pair of objects to be merged. The source object is merged into the destination object and the source object is deleted. Merging through the XML file allows a merge of multiple pairs at the same time.

You can merge objects in cases where the same object (such as a host or file system) is discovered by different discovery mechanisms and has different values for the same property, or has different properties of the object are discovered by different discovery mechanisms, or both. Merge these objects so that one object can be referenced as a single entity in the system.

---

**Note:** Once objects are merged, the operation cannot be reversed. Be extremely careful merging objects, because incorrect usage can result in data corruption. Do not merge objects while agents are collecting data, since agents may not be able to report some data.

---

The <mergeitems> tag includes these properties:

toobject	Destination object ID. This is the ID of the object in which the source object is merged.
fromobject	Source object ID. This is the ID of the object that is merged into the destination object. After the merge, this source object is deleted.

## Examples of XML files

You can create several types of XML files, including the following:

- Add several host and file system objects and use them to create a tree.  
See “[Example 1: Adding objects and a tree](#)” on page 567.
- Update the properties of two host objects.  
See “[Example 2: Updating two hosts](#)” on page 570.
- Delete a single host object.  
See “[Example 3: Deleting a host](#)” on page 570.
- Merge two objects into a single object.  
See “[Example 4: Merging objects](#)” on page 571.

Examples also ship with Veritas Backup Reporter in the following location (by default):

Solaris	/opt/VRTSccsvs/xml-examples
Windows	\Program Files\Symantec\Veritas Backup Reporter\Server\xml-examples

## Example 1: Adding objects and a tree

Example 1, when imported into Veritas Backup Reporter, creates a simple view with two top-level branches, each of which contains two host objects (“alpha” and “bravo,” “charlie,” and “delta”). The host “alpha” contains two file system objects.

```
<?xml version="1.0"?>
<!DOCTYPE application [
<!ELEMENT application (objects?,view*,user*,mergeitems*)>
  <!ATTLIST application version CDATA #REQUIRED>
<!ELEMENT objects (object+)>
<!ELEMENT view (node*)>
  <!ATTLIST view identifier CDATA #REQUIRED>
  <!ATTLIST view action (add|delete|update|declare) "declare">
  <!ATTLIST view id ID #IMPLIED>
<!ELEMENT object (attribute*)>
  <!ATTLIST object id ID #IMPLIED>
  <!ATTLIST object name CDATA #IMPLIED>
  <!ATTLIST object action (add|delete|update|declare) "declare">
  <!ATTLIST object type CDATA #IMPLIED>
  <!ATTLIST object master IDREF #IMPLIED>
  <!ATTLIST object dbid CDATA #IMPLIED>
<!ELEMENT node (object?,node*)>
  <!ATTLIST node id ID #IMPLIED>
  <!ATTLIST node action (add|delete|declare) "declare">
  <!ATTLIST node object IDREF #IMPLIED>
<!ELEMENT user EMPTY>
  <!ATTLIST node parents IDREFS #IMPLIED>
  <!ATTLIST user action (add|delete) "add">
  <!ATTLIST user login CDATA #REQUIRED>
  <!ATTLIST user domainName CDATA #REQUIRED>
  <!ATTLIST user domainType CDATA #REQUIRED>
  <!ATTLIST user firstName CDATA #IMPLIED>
  <!ATTLIST user lastName CDATA #IMPLIED>
  <!ATTLIST user email CDATA #IMPLIED>
  <!ATTLIST user accessLevel (admin|adminReadOnly|user|default) "default">
  <!ATTLIST user department CDATA #IMPLIED>
  <!ATTLIST user costCenter CDATA #IMPLIED>
```

```
<!ATTLIST user workNumber CDATA #IMPLIED>
<!ATTLIST user mobileNumber CDATA #IMPLIED>
<!ATTLIST user pagerNumber CDATA #IMPLIED>
<!ELEMENT mergeitems (mergeitem+)>
<!ELEMENT mergeitem EMPTY>
  <!ATTLIST mergeitem toobject IDREF #IMPLIED>
  <!ATTLIST mergeitem fromobject IDREF #IMPLIED>
<!ELEMENT attribute (name,value*)>
  <!ATTLIST attribute name CDATA #IMPLIED>
  <!ATTLIST attribute value CDATA #IMPLIED>
<!ELEMENT name (#PCDATA)>
<!ELEMENT value (#PCDATA)>
]>
<application version="2.0">
<objects>
<object id="o1" action="add" type="Host">
<attribute name="Hostname" value="alpha.veritas.com" />
<attribute name="IP Address" value="10.10.10.1" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version" value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o2" action="add" type="Host">
<attribute name="Hostname" value="bravo.veritas.com" />
<attribute name="IP Address" value="10.10.10.2" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version" value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o3" action="add" type="Host">
<attribute name="Hostname" value="charlie.veritas.com" />
<attribute name="IP Address" value="10.10.10.3" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version" value="unknown" />
<attribute name="Discovered Master Server" value="false" />
```

```
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o4" action="add" type="Host">
<attribute name="Hostname" value="delta.veritas.com" />
<attribute name="IP Address" value="10.10.10.4" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version" value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="fs1" action="add" type="File_System" master="o1">
<attribute name="name" value="/" />
<attribute name="Discovered" value="false" />
<attribute name="Backed Up" value="true" />
</object>
<object id="fs2" action="add" type="File_System" master="o1">
<attribute name="name" value="/export" />
<attribute name="Discovered" value="false" />
<attribute name="Backed Up" value="true" />
</object>
<object id="cat1" action="add" type="Generic_Object">
<attribute name="name" value="Cat1" />
</object>
<object id="cat2" action="add" type="Generic_Object">
<attribute name="name" value="Cat2" />
</object>
</objects>
<view identifier="TestA1" action="add">
<node id="n1" action="add" object="cat1" />
<node id="n2" action="add" object="cat2" />
<node id="n3" action="add" object="o1" parents="n1" />
<node id="n10" action="add" object="fs1" parents="n3" />
<node id="n11" action="add" object="fs2" parents="n3" />
<node id="n4" action="add" object="o2" parents="n1" />
<node id="n5" action="add" object="o3" parents="n2" />
<node id="n6" action="add" object="o4" parents="n2" />
```

```
</view>  
</application>
```

## Example 2: Updating two hosts

Example 2, when imported into Veritas Backup Reporter, updates the properties of the two host objects (“Master Server 3” and “Host 3\_8”) defined in the XML file.

(The DTD header has been snipped.)

```
<application version="2.0">  
<objects>  
<object id="o2" action="update" type="Host">  
<attribute name="Hostname" value="Master Server 3" />  
<attribute name="IP Address" value="unknown" />  
<attribute name="Operating System" value="unknown" />  
<attribute name="Operating System Version" value="unknown" />  
<attribute name="Discovered Master Server" value="true" />  
<attribute name="Discovered Media Server" value="true" />  
<attribute name="Discovered Backup Client" value="false" />  
<attribute name="Discovered Online Storage Client" value="false" />  
<attribute name="Discovered Agent Server" value="false" />  
</object>  
<object id="o3" action="update" type="Host">  
<attribute name="Hostname" value="Host 3_8" />  
<attribute name="IP Address" value=" " />  
<attribute name="Operating System" value="Solaris" />  
<attribute name="Operating System Version" value="2.6" />  
<attribute name="Discovered Master Server" value="false" />  
<attribute name="Discovered Media Server" value="false" />  
<attribute name="Discovered Backup Client" value="true" />  
<attribute name="Discovered Online Storage Client" value="true" />  
<attribute name="Discovered Agent Server" value="false" />  
</object>  
</objects>  
</application>
```

## Example 3: Deleting a host

Example 3, when imported into Veritas Backup Reporter, deletes the host object “Host 8\_0” from the data store.

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o1" action="delete" type="Host">
<attribute name="Hostname" value="Host 8_0" />
</object>
</objects>
</application>
```

## Example 4: Merging objects

Example 4, when imported into Veritas Backup Reporter, merges object “o2” into the object “o1.” Objects “o1” and “o2” represent the same host. One has a host name of “hostA.veritas.com” and the other has the host name as “hostXYZ.somedomain.veritas.com.” While merging object “o2” into object “o1,” you can specify “hostXYZ.somedomain.veritas.com” as an alias for object “o1.” After merging object “o2,” it is deleted and only object “o1” remains.

In Example 4, a host object has the hostname “hostA.veritas.com” which also goes by the name “hostXYZ.somedomain.veritas.com.” The XML export of this object looks like the following:

(The DTD header has been snipped.)

```
<object id="o1" action="declare" type="Host" dbid="50">
<attribute>
  <name>Hostname</name>
  <value>hostA.veritas.com</value>
  <value>hostXYZ.somedomain.veritas.com</value>
</attribute>
<attribute>
  <name>IP Address</name>
  <value>UNKNOWN</value>
</attribute>
<attribute>
  <name>Operating System</name>
  <value>Windows</value>
</attribute>
<attribute>
  <name>Operating System Version</name>
  <value>Windows 2000</value>
</attribute>
<attribute>
  <name>Discovered Master Server</name>
  <value>>false</value>
</attribute>
```

```
<attribute>
  <name>Discovered Media Server</name>
  <value>>false</value>
</attribute>
<attribute>
  <name>Discovered Backup Client</name>
  <value>>false</value>
</attribute>
<attribute>
  <name>Discovered Online Storage Client</name>
  <value>>true</value>
</attribute>
<attribute>
  <name>Discovered Agent Server</name>
  <value>>false</value>
</attribute>
</object>
```

This example has another host object whose host name is “hostA” and whose XML export is as follows:

```
<object id="o2" action="declare" type="Host" dbid="70">
<attribute>
  <name>Hostname</name>
  <value>hostA</value>
</attribute>
<attribute>
  <name>IP Address</name>
  <value>10.10.10.1</value>
</attribute>
<attribute>
  <name>Operating System</name>
  <value>UNKNOWN</value>
</attribute>
<attribute>
  <name>Operating System Version</name>
  <value>UNKNOWN</value>
</attribute>
<attribute>
  <name>Discovered Master Server</name>
  <value>>false</value>
</attribute>
<attribute>
  <name>Discovered Media Server</name>
```

```
<value>>false</value>
</attribute>
<attribute>
  <name>Discovered Backup Client</name>
  <value>>true</value>
</attribute>
<attribute>
  <name>Discovered Online Storage Client</name>
  <value>>false</value>
</attribute>
<attribute>
  <name>Discovered Agent Server</name>
  <value>>false</value>
</attribute>
</object>
```

If you are certain that these two host objects are the same host, you can merge them. But, before you merge the underlying objects, you must update the surviving object with data that ensures that no future objects with the name “hostA” is created. To do this, update the first host record as such. The host name attribute is now a union of the two objects, and the IP address is set to the actual discovered IP address.

```
<objects>
<object id="01" action="update" type="Host" dbid="50">
<attribute>
  <name>Hostname</name>
  <value>hostA.veritas.com</value>
  <value>hostXYZ.somedomain.veritas.com</value>
  <value>hostA</value>
</attribute>
<attribute>
  <name>IP Address</name>
  <value>10.10.10.1</value>
</attribute>
<attribute>
  <name>Operating System</name>
  <value>Windows</value>
</attribute>
<attribute>
  <name>Operating System Version</name>
  <value>Windows 2000</value>
</attribute>
<attribute>
```

```
<name>Discovered Master Server</name>
<value>>false</value>
</attribute>
<attribute>
  <name>Discovered Media Server</name>
  <value>>false</value>
</attribute>
<attribute>
  <name>Discovered Backup Client</name>
  <value>>true</value>
</attribute>
<attribute>
  <name>Discovered Online Storage Client</name>
  <value>>true</value>
</attribute>
<attribute>
  <name>Discovered Agent Server</name>
  <value>>false</value>
</attribute>
</object>
</objects>
```

Now, whenever a particular Veritas Backup Reporter Agent refers to a host as “hostA,” the Veritas Backup Reporter Management Server identifies the object since one of its host names matches this object. After this object update, you can merge the two hosts with the following syntax:

```
<mergeitems>
<mergeitem toobject = "o1" fromobject = "o2"/>
</mergeitems>
```

Merging of two hosts moves all data from the hostA object to the newly updated object and deletes the hostA object.

# Using the Veritas Backup Reporter Knowledge Base

This appendix includes the following topics:

- [About the Veritas Backup Reporter Knowledge Base](#)
- [Browsing Knowledge Base entries](#)
- [Creating Knowledge Base entries](#)
- [Modifying Knowledge Base entries](#)
- [Deleting Knowledge Base entries](#)

## About the Veritas Backup Reporter Knowledge Base

The Veritas Backup Reporter Knowledge Base is a database of reference information for error codes and commands. It is a good way for users to store and retrieve installation specific information about system events, individual resources, processes, and procedures.

When viewing other parts of the database, such as the backup job history, an administrator can click an error code for a failed job to view the Knowledge Base entry for that error code.

In addition to viewing the Knowledge Base entries that ship with Veritas Backup Reporter, you can create and modify your own entries.

## Browsing Knowledge Base entries

You can browse all the entries in the Knowledge Base the VBR console.

#### **To browse entries in the Knowledge Base**

- 1** Click **Reports > Explorers > Knowledge Base**.
- 2** In the table of Knowledge Base categories, click the category whose entries you want to view.
- 3** In the table of Knowledge Base entries, click the entry you want to view.

## **Creating Knowledge Base entries**

You can add your own entries to the Knowledge Base. This may be helpful for making notes about the administration or operation of Veritas Backup Reporter available for others or for your own future reference.

#### **To create a new entry in the Knowledge Base**

- 1** Click **Reports > Explorers > Knowledge Base**.
- 2** In the table of Knowledge Base categories, in the Tools box in the task pane, click **Add Knowledge Base Entry**.

- 3 In the Add Knowledge Base Entry dialog box, type or select the following information:

Title	The title of the entry. It should be descriptive, yet short enough to display in a table.
Category	The Knowledge Base category. If the category you specify does not exist, Veritas Backup Reporter creates a new category with that name. To add a new entry to an existing category, you must type the category name exactly as it appears in the Knowledge Base table.
Error Code (optional)	A code associated with the event or condition you are describing. Use this field if your organization has a list of error codes for identifying various types of events or conditions.
Email (optional)	An email address to be notified whenever this entry is updated.
Group (optional)	A group to be notified whenever this entry is updated.
Description	The text of the entry. It can describe a problem and its recommended solution, list configuration details about a resource in the network, or provide any other information of value to users at your installation.

Knowledge Base descriptions can contain standard HTML coding.

- 4 Click **Add** to add the new entry to the Knowledge Base.

## Modifying Knowledge Base entries

To ensure that your Knowledge Base entries contain current information, you can edit them.

To modify an entry in the Knowledge Base

- 1 Click **Monitors > Knowledge Base**.
- 2 In the table of Knowledge Base categories, select the category for the entry you want to modify.
- 3 In the table of Knowledge Base entries, on the line for the entry you want to modify, click the Modify icon.

- 4 In the Add Knowledge Base Entry dialog box, edit the dialog field values.  
See [“Creating Knowledge Base entries ”](#) on page 576.
- 5 Click **Modify** to save your changes to the Knowledge Base entry.

## Deleting Knowledge Base entries

You can delete entries in the Knowledge Base when they are no longer useful.

### To delete an entry in the Knowledge Base

- 1 Click **Monitors > Knowledge Base**.
- 2 In the table of Knowledge Base categories, select the category for the entry you want to modify.
- 3 In the table of Knowledge Base entries, on the line for the entry you want to delete, click the icon in the Delete column.
- 4 Click **OK** to confirm deletion.

# Attributes of NetBackup data

This appendix includes the following topics:

- [About backup data attributes](#)

## About backup data attributes

This section lists all attributes pertaining to data that Veritas Backup reporter collects from NetBackup. You can select these attributes while generating custom reports.

[Creating custom reports](#)

**Table E-1** Backup data attributes

Data Attributes	Sample Data	Explanation
<b>Backup Job Attributes</b>		
Agent Server	host.symantec.com	The name of the server where a Backup Reporter data collection agent is installed
Backup Job Comment	Host could not be reached	Filled in by the user in the Job Reconciliation page to indicate why a job failed so others can see.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Job File Count Deduplication Factor	321	The deduplication file factor for each PureDisk backup job. Meaning that for every 321 files that were backed up only 1 file was actually stored. (321 to 1 file deduplication rate)
Backup Job File Count Deduplication Savings	456	The number of files not needing to be backed up for every backup job in PureDisk because they were already stored with deduplication. Meaning that if 500 files were targeted for backup, only 44 were stored since the savings was 456.
Backup Job Is Ignored	Yes/No	Within Backup Reporter there is the ability to mark a job as ignored (yes/no). If it is ignored it does not count towards things like success rate or time since last successful backup. This marking of a job as ignored is done in the "Reports > Explorers" section.
Backup Job Protected File Count	400 files	The number of files processed in a PureDisk backup. Note that this is not the number actually stored since it is prior to deduplication.
Backup Job Protected Size	200GB	The size in bytes of a PureDisk backup job prior to deduplication.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Job Size Deduplication Factor	567	The deduplication size factor for each PureDisk backup job. Meaning that for every 567KB that were backed up only 1KB was actually stored.
Backup Job Size Deduplication Savings	345	The number of KB's not needing to be backed up for every backup job in PureDisk because they were already stored with deduplication. Meaning that if 346KB were backed up, the savings of 345KB means only 1 KB was needed to be stored.
Backup Job Sub Type	Catalog, File System, MS Exchange, NDMP, Sybase	Each directory under a job and it's type of backup.
Backup Job Transport Type	LAN, SAN	The transport used to move the backup from backup client to media server
Job Attempt Count	4	The number of times a backup job had to be attempted before being successful or reaching the maximum allowable number of retries
Job Client	backup-client.symantec.com	The name of a host being backed up as seen by a backup job
Job Directory	C:\, /var, ALL_LOCAL_DRIVES	The file system directory being backed up as seen by a backup job

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Job Duration	300 seconds	The amount of time in seconds for a backup to start and finish as seen by a backup job
Job End Time	Tues 3/23/2008 03:34:43	The date and time that a backup ended
Job Error Code	0,1,2,3...	The exit code, status code or error code for a particular job
Job Expiration Time	Aug 01, 2008 22:03:48	The time at which this job (really the image that is generated by the job) is going to expire.
Job File Count	300	The number of files a backed up during a backup job
Job Group ID	6114	The group ID that can be specified by the product to group them in a certain way. Note:The secondary ID and the Group ID are basically intended for the same purpose, that is to group the jobs in some way that is useful in reporting.
Job Level	Full, Differential Incremental, User Backup	The Schedule Type for the backup job, Full, Incremental, Cumulative, User etc.
Job Primary ID	5,234,234	A unique number for each backup job in a backup domain that identifies a backup job

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Job Secondary ID	5,234,235	When a unique job number is not enough to distinguish a job, a secondary ID may be used. For NBU, this field is the job Process ID
Job Size	2048	The amount in KB that a backup job transferred from client to media server for backing up
Job Start Time	Tues 3/23/2008 02:34:43	The date and time that a backup started
Job Success Rate (Complete and partial)	98	A percent number that is calculated based on the number of jobs that were successful (NetBackup status 0) and partially successful (NetBackup status 1) divided by the total number of jobs ran in that period of time. Example: 98 successful jobs / 100 total jobs (2 failures) = 98%
Job Success Rate (Complete only)	99	A percent number that is calculated based on the number of jobs that were successful (NetBackup status 0) divided by the total number of jobs ran in that period of time. Example: 98 successful jobs / 100 total

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Job Throughput (Kbytes/sec)	3,234	The speed of a backup job in Kbytes/sec. This is the speed of the overall job which takes in to account transfer time from client to media server and media server to disk or tape storage. It is not just the speed of a tape drive.
Job Type	Backup, Restore, duplication, archive, label, erase	The type of operation done by the backup product
Level Type	Full, Differential Incremental, User Backup	The Schedule Type for the backup job grouped into just two options. Full vs. Other
Master Server	nbu-master.example.com	The name of the master server that executed the backup job
Media Server	nbu-media.example.com	The name of the media server that performed the backup job
Policy	Oracle Backup Policy, User Backup Policy, File System Backup Policy	The name of the backup policy as seen by a backup job
Policy Description	Oracle Backup Policy, User Backup Policy, File System Backup Policy	The name of the backup policy as seen by a backup job
Policy Description	'This policy is for doing Oracle backups'	The user-defined description of a policy as seen by a backup job
Policy Domain Name	NetBackup Policy Domain, PureDisk Policy Domain	The backup product that a backup policy executed a job from

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Policy Type	Standard (UNIX), Windows-NT, Oracle, Exchange	The type of policy as seen by a backup job
Product	NetBackup, PureDisk, TSM	The backup product that performs backup, from which VBR collects data
Schedule	(user-defined), ex: Weekly-Fulls, Daily-Incrementals	The name of a schedule which resides within a policy as seen by a backup job
Status	Success, Partial, Failure	A word description for each job that coorelates status codes to their english meaning. All failures are mapped to the word 'Failure'
Storage Unit Name	(user-defined), ex: tld0-hcart-0	The name of a storage unit which is chosen by a policy to receive and store backups. Storage Units are usually groupings of tape drives within a library or multiple disk locations that are grouped together in pools. This is the storage unit name that was used by a backup job and therefore may or may not exist in present time.
Storage Unit Type	Disk, Media Manager (tape)	The type of storage unit used and seen by a backup job
Job Scheduled Time		
Window Closing Time		
Job Execution Type		

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Original Job ID		
<b>Backup Image Attributes</b>		
Backup Image Compression State	Yes/No	A yes/no property of if a backup image stored in the catalog was compressed or not.
Backup Image Copy Expiration Time	Mon 4/23/2008 4:32:34	The date/time that a backup image copy is set to expire
Backup Image Copy Is Currently Expired	Yes/No	A yes/no property of if a backup image is expired or not. If it is expired it can no longer be restored and that space may be rewritten to by the backup application. If it is not expired it is available for restore.
Backup Image Copy Is Primary	Yes/No	A yes/no property of if a backup image is the primary copy. If the image is a 2nd or greater copy this value would be 'no'.
Backup Image Copy Media Server	backup-server.symantec.com	The name of the backup server that performed the copy of a backup to a second location.
Backup Image Copy Multiplexed State	True/False	A true/false property as to if the backup image copy was written using multiplexing or not (multiple clients/jobs streamed to one image)

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Image Copy Storage Unit Type	Media Manager (tape), Disk	The type of storage unit that the backup image was copied to. This could be disk, tape etc.
Backup Image Copy Unexpired Fragment Count	30	The number of fragments that make up a complete unexpired backup. A single backup can have 1 or a multiple of fragments which are blocks of data seperated by tape marks on tape or seperated in to separate files on the file system if written to disk.
Backup Image Copy Unique ID	backupclient_23423	A unique ID or key for every backup stored in the catalog. This key or ID can be used to look up an image in the catalog for restore or other activity
Backup Image Encryption State	Yes/No	A yes/no property of if a backup image was encrypted between the backup client and backup media server. This value does NOT represent if tape drive or other encryption was used or not.
Backup Image Expiration Time	Mon 4/23/2008 4:32:34	The date and time that a backup image will expire. When a backup image expires it is no longer available for restore and the space that the backup occupied can be reused for additional backups (overwritten)

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Image File Count	432	The actual number of files that are stored within a backup image.
Backup Image Fragment Expiration Time	Mon 4/23/2008 4:32:34	The date/time that the backup image fragment is set to expire
Backup Image Fragment Is Currently Expired	Yes/No	A yes/no property of if the backup image fragment is expired or not. Even if a backup fragment is expired, that space can not be reused until the whole backup image is expired (disk) or the whole backup tape media is expired (tape)
Backup Image Fragment Is TIR	TIR Info on Disk, TIR Rsv Synthetic Info on Disk	The true image restore status for a backup image fragment. True image restores allow a restore to take place at the directory level without overwriting files that weren't backed up but are still in the directory. For this to be possible a 'true image restore' backup image must exist.
Backup Image Fragment Size	2048	The size of the backup image fragment. By default NetBackup uses 1TB fragments (ie no fragments) but this can be configured to different values
Backup Image Fragment Unique ID	backupimagefragment_124	A unique ID associated with every backup image fragment

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Image Is Currently Expired	Yes/No	A yes/no property as to if the backup image is expired or not
Backup Image TIR Status	TIR Info on Disk, TIR Rsv Synthetic Info on Disk	The true image restore status for a backup image. True image restores allow a restore to take place at the directory level without overwriting files that weren't backed up but are still in the directory. For this to be possible a "true image restore" backup image must exist.
Backup Image Type	Regular, Catalog	The type of backup image. Catalog being a NBU catalog image for disaster recovery
Backup Image Unexpired Copy Count	1, 2, 3 etc.	The number of copies that exist for a primary backup image. These are copies that are unexpired and can be used for a restore.
Backup Image Unique ID	backupclient_23423	A unique ID or key for every backup stored in the catalog. This key or ID can be used to look up an image in the catalog for restore or other activity
Backup Image Write End Time	Mon 4/23/2008 4:32:34	The date and time that the backup image was finished writing.
Backup Image Write Start Time	Mon 4/23/2008 4:32:34	The date and time that the backup image began to be written.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Data Classification Master Server	master-server.symantec.com	The name of the server that classified the backup image in some sort of ranking (gold, silver, bronze etc)
Data Classification Name	Gold, Silver, Bronze, Non-DataClassification-Name	The name of the classification of data
Data Classification Rank	1,2,3,etc	The number ranking that corresponds with the name of data classification. A 1 would mean the data is more important than a 2 for example.
<b>Backup Attempt Attributes</b>		
Attempt Duration	3500	The number in seconds that a backup was attempted
Attempt Duration	3500	The number in seconds that a backup was attempted
Attempt End Time	Mon 4/23/2008 4:32:34	The date and time that a backup attempt ended (each attempt is unique)
Attempt Error Code	0, 1, 2, 3 etc.	The error code that the backup attempt finished with
Attempt File Count	0, 1, 2, 3 etc.	The number of files the backup attempted to process
Attempt Size	2048	The number in KB for the amount an attempted backup tried to process
Attempt Start Time	Mon 4/23/2008 4:32:34	The start time that a backup attempt began

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Attempt Status	Success, Partial, Failure	A named status that maps to the error code numbers in the backup application (for example a status 0 in NetBackup is a success, a status 1 is partial and all other numbers are failures)
Attempt Success Rate	98%	The average success rate across all attempts in all backups. Example would be the average of 2 backups were each was attempted 3 times. The success rate would be the success rate average of the 3 attempts within each backup job. (Note that this is different than the success rate across all jobs which does not take in to account attempts)
Attempt Throughput	2048Kbytes/sec	The speed of a backup attempt in Kbytes/sec. This is different than the overall KB/sec for a job which would take in to account all attempts.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Attempt Partial Success Rate	98%	The average success rate across all attempts in all backups but also including partial successes (status 1 in NetBackup). Example would be the average of 2 backups were each was attempted 3 times. The success rate would be the success rate average of the 3 attempts within each backup job. (Note that this is different than the success rate across all jobs which does not take in to account attempts)
Backup Attempt Sequence	1, 2, 3	The attempt number in a sequence. 1 would represent the first attempt, 2 would represent the second attempt etc.
Backup Skipped File Time	Mon 4/23/2008 4:32:34	The date and time that a particular file was skipped over during a backup
Skipped File Code	1	The status code for why that file was skipped (usually a status 1)
Skipped File Reason	File is open by another process	The reason a file was skipped. (Usually because file was in use)
Skipped File Name	C:\Windows\an_open_file.dll	The actual file name that was skipped over during a backup.

**Backup Policy Attributes**

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Policy Domain Master Server	nbu-master.example.com	The host name of the backup application host that contains the backup policy. In the case of NetBackup this is the master server.
Backup Policy Name	Oracle Backup Policy, User Backup Policy, File System Backup Policy	The name of a backup policy that exists in the backup application. Note that this is similar and can be the same as the 'Backup Job Attribute: Policy' which shows what policy the backup job was executed from. It is different though since this Policy Name simply means that this Policy exists not that anything was executed from it yet.
Backup Policy Type	Standard (UNIX), Windows-NT, Oracle, Exchange	The type of backup policy that exists in the backup application. Note that this is different than the 'Backup Job Attribute: Policy Type'
Data Classification Name		
Policy Storage Unit / Lifecycle policy		
Policy Volume Pool		
Job Priority		
Active		
Effective Date		
Backup Network Drives		

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
True Image Recovery		
Compression		
Encryption		
Allow Multiple Data Streams		
Block Level Incremental		
Perform Snapshot		
Individual File Restore From Raw		
Virtual Machine Proxy		
Multiple copies		
Override policy storage selection		
Override policy volume pool		
Override media owner		
Multiplexing		
Fail all		
Synthetic		
Disk Only		
<b>File System Attributes</b>		
Business Classification	'Business Critical'	User defined field. Can be one of 'Mission Critical', 'Business Critical' or 'Business Support'

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
File System: OID	asset123 etc.	A user defined field for an object ID of the file system. Typically used as a pairing with an asset management database
Filesystem Name	C:\Documents and Settings\All Users\	The file system directory being backed up.
Filesystem Type	NTFS, UFS, ZFS, EXT3	A user-defined field (this is not collected automatically) of what type of file system was backed up.
<b>Host Attributes</b>		
Host Architecture	SPARC, x86	User defined field (this is not automatically collected) for filling in architecture type such as x86, x86-64, SPARC, POWER, PA-RISC, IA64 etc
Host: Misc Info	Pete's server	A user defined field for inserting any extra information regarding a host
Host: OID	asset123, etc.	A user defined field for inserting an object ID from an asset management database
Hostname	hostname.example.com	The name of the host object that contains file systems.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
O.S. Version	2003, 10	The version of the operating system. Usually grouped with Operating System name since this will have values like '10' (i.e. Solaris 10), or '2003' (i.e. Windows 2003)
Operating System	Windows, Solaris	The operating system name of the host
<b>Backup Media Attributes</b>		
Agent Server	vbr-agent.example.com	The name of the Veritas Backup Reporter agent that collected the media information.
Backup Media Allocation Time	Mon 3/4/2008 3:34:34	The date/time that a piece of media was first allocated or had it's first backup written to it. Once the media expires it will have a new allocation date/time when it is reused
Backup Media Available Free Capacity	500,000 KB	How much is left on tape in KB. Value here per sample is either the free capacity if the media is active, or 0 otherwise.
Backup Media Available Total Capacity	19,000,000KB	Total capacity of the tape in KB. Value here per sample is either the total capacity if the media is active, or 0 otherwise.
Backup Media Barcode	JFP000L2	The full barcode as ready by the physical robot. This can be longer than the 6 characters used by a NetBackup Media.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Media Expiration Time	Mon 3/4/2008 3:34:34	The date/time that a backup media is set to expire
Backup Media Free Capacity	500,000 KB	How much is left on tape in KB. This number may be estimated using an algorithm.
Backup Media Is Active	Yes/No	A yes/no property of a particular tape indicating whether the tape has been sampled in the last two collections.
Backup Media Is Available	Yes/No	A yes/no property of a particular tape indicating whether it can still be written to.
Backup Media Is Current	Yes/No	A yes/no property of if the backup media exists in the current configuration (and not historical)
Backup Media Is Data Expired	Yes/No	A yes/no property of if the backup media has expired data on it or not
Backup Media Is Full	Yes/No	A yes/no property of if the backup media is marked as full (no more backups can be written to it)

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Media Is Imported	Yes/No	A yes/no property of if the backup media was imported. Imported media simply means that this particular backup domain did not originally write the data to the media. This could be due to disaster recovery where the catalog could not be moved from an existing domain so the tapes were read individually to determine what data was on them. It also is commonly used to import Backup Exec media to NetBackup.
Backup Media Is Physically Expired	Yes/No	A yes/no property of if the physical media is expired or not. Once all the backup images (data) has been expired on a tape that entire cartridge is marked as Physically Expired=Yes and it can be overwritten or used by future backups.
Backup Media Is Total Capacity Estimated	Yes/No	Since capacity of a tape is often estimated using an algorithm. This specifies whether it was actually calculated, or provided exactly by the DP product.
Backup Media Last Read Time	Mon 3/4/2008 3:34:34	A date/time that the backup media was last used to be read (restored)

**Table E-1** Backup data attributes (continued)

Data Attributes	Sample Data	Explanation
Backup Media Last Write Time	Mon 3/4/2008 3:34:34	A date/time that the backup media was last used to be written to (duplicates, backups)
Backup Media Library Slot Number	1, 2, 3 etc.	The physical slot number that a given piece of media resides in
Backup Media Multiple Retention Levels Allowed	Yes/No	A yes/no property of if a given piece of tape media will allow for multiple expiration dates. Multiple expiration dates means that the whole tape can not be reused until the last backup has expired on the media.
Backup Media Multiplexing Allowed	Yes/No	A yes/no property of if multiplexing is allowed on a piece of tape media. Multiplexing means that multiple clients were backed up to one image so that particular image could have more than one client inside it.
Backup Media Percent Available Free Capacity	0-100%	Calculated value representing (available free capacity /available total capacity ) in percentage
Backup Media Percent Free Capacity	0-100%	Calculated value representing (free capacity total capacity ) in percentage

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Media Percent Used Capacity	0-100%	Calculated value representing (used capacity / total capacity) in percentage
Backup Media Physical Expiration Time	Mon 3/4/2008 3:34:34	The date/time that a piece of media will physically expire (all images on the media) and be able to be reused
Backup Media Retention Level	63072000.00, 31536000.00, 1209600.00	The retention level of the media in number of seconds. Divide by 86400 to get the retention level in days
Backup Media Snapshot Time	Mon 3/4/2008 3:34:34	The date/time that all the media information was collected from the backup application to VBR. History is kept so a history of the state of all media can be determined.
Backup Media Storage Type	Disk, Tape	The type of storage for a given piece of media (disk or tape)
Backup Media Total Capacity	19,000,000 KB	Total capacity of the tape in KB. This number may be estimated using an algorithm.
Backup Media Type	HCART, DLT, 8MM etc.	The density or type of media. This is used to match what drives the media can go in for a mixed media environment.
Backup Media Unexpired Image Count	1, 2, 3 etc.	The number of images that are unexpired on a given piece of media

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Media Used Capacity	500,000 KB	Amount in KB used up in the tape. This value is provided by the DP product and is NOT estimated.
Backup Media Volume Group Name	User defined but defaults to things like '000_00002_TLD'	A user defined field for grouping volumes. By default NetBackup assigns the robot number and type so that TLD(2) would read '000_00002_TLD'
Backup Media Volume Path	/disk_staging_file_system/, C:\disk_staging\	The path on disk where backup images are stored.
Disk Pool High Water Mark	95%	Specific to NetBackup 6.5 - this is the high water mark that is set for a Flexible Disk pool, OpenStorage disk pool or PureDisk backend storage pools. When this threshold is reached by the file system on the disk pools backups will not be attempted to that disk location since it will be considered 'full'.
Disk Pool Low Water Mark	80%	Specific to NetBackup 6.5 - this is the low water mark that is set for a Flexible Disk pool, OpenStorage disk pool or PureDisk backend storage pools. When this threshold is reached by the file system on the disk pools backups will not be sent to the location as often

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Disk Pool Master Server	nbu-master.example.com	The name of the NetBackup master server that the disk pool belongs to
Disk Pool Name	netappfi::fas3050-1a, DDPool, etc.	The name of the disk pool which defaults to the disk array string or a user defined value
Disk Pool Raw Size	69,990.40	The raw size is the size of the disk volume(s) in a disk pool. Raw size does not mean you can actually write to that amount (that's what usable size is) but just tells you there is more possible disk space that could be allocated from raw to usable.
Disk Pool Server Type	AdvancedDisk, SharedDisk	The type of flexible disk that the pool is
Disk Pool Snapshot Time	Mon 3/4/2008 3:34:34	The date/time that a snapshot was taken to produce the backup image that exists in the disk pool
Disk Pool Status	UP, DOWN	Similar to tape drive status, this tells if the disk pool is UP meaning it is usable and can be used or DOWN meaning it is not usable. When in the DOWN state jobs will not attempt to use the disk pool.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Disk Pool Usable Size	1,208,893.44	The usable size is the size of the formatted file system and tells you how much data can be written to the disk pool
Disk Pool Volume Count	4	The number of disk volumes that make up the disk pool
Media Density	HCART, DLT, 8MM etc.	The type of tape media as defined by the backup application. For NetBackup this is also called the 'density' and specifies what types of drive the tape can go in.
Media Hsize	1024	Optical media header size of a backup image
Media ID	JFP000	The Media ID for a given piece of media, usually a subset of the barcode. For NetBackup this is a 6-digit ID.
Media Image Count	54	The number of backup images on a given piece of tape media or disk pool
Media L Offset	2048	Logical block address of the beginning of the block that a backup image exists
Media Restore Count	0, 1, 2, 3, etc.	The number of times a given piece of backup media has been used for restores.
Media Ssize	1024	Optical media sector size of a backup image.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Partner	A/B	The ID of the opposite side of a optical platter. If on side A of a platter this would show Side B
Product	NetBackup, TSM	The backup product that this piece of media belongs to
Status	Active, Non-active, Suspended, Frozen	The status of a given piece of media. Active meaning it is being used at a given point in time, Frozen meaning errors have occurred on the tape media and it is no longer being used for backups, etc.
Volume Pool ID	1, 2, 3, 4 etc.	The volume pool ID which automatically starts at 1 for the default pool "NetBackup". Things like Scratch Pools or onsite/offsite pools are typically also used and these all have unique volume pool ID's. Many encryption solutions such as Decru and IBM use the volume pool ID to determine what backups to encrypt or not
Volume Pool Name	NetBackup, Scratch, CatalogBackup, MSEO, WORM, etc.	This user defined field is the name of the volume pool that media is placed in to. The default is NetBackup but many others are typically created to segment tapes in to groups

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Volume/EMM Database Server	nbu-master.example.com	The name of the Volume Database (pre-NetBackup 6.) or EMM server (NetBackup 6.0+). This is typically the NBU Master but doesn't have to be in the case where multiple masters are sharing the same EMM server.
<b>Tape Library Attributes</b>		
Tape Library Agent Product	NetBackup, TSM	The backup application that controls the tape drive
Tape Library Agent Server	vbr-agent.example.com	The server host name that the VBR agent is installed on that is used to collect tape drive information.
Tape Library Device Database Server	NBU-device-host.example.com	The device database server that is controlling the particular library. This is the Enterprise Media Manager server (EMM) in NetBackup 6.0+ or the device control host in 5.1 and below.
Tape Library Manufacturer	STK, Quantum, IBM etc.	The manufacturer as determined by the SCSI inquiry string in the backup application.
Tape Library Serial Number	ADIC203100468_LL0	The serial number, unique, to each tape library
Tape Library Slot Count	40, 120, 360	The total number of slots that exist in a tape library

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Tape Library Type	Tape Library DLT, Tape Library 8MM, Tape Library ACS	The type of tape library (TLD, ACS, 8MM, 4MM, TLM, TLH etc)
Tape Library Unique ID	0, 1, 2 etc.	The unique number given to each tape library in the EMM database. This ID is put together with the library type in the NBU GUI to show TLD(0), TLD(1) etc.
<b>Tape Drive Attributes</b>		
Name	IBM.ULTRIUM-TD2.000	The name of a tape drive as given by the backup application, usually default names are based on SCSI inquiry strings that contain the manufacturer name and model number
Number	0, 1, 2, 3 etc.	The number of a tape drive as given by the backup application which is unique for each physical drive (a number could be shared between media servers though)
Shared	true/false	A simple true/false on weather the tape drive is shared across backup servers or not
Tape Drive Device Host	NBU-device-host.example.com	The device host (Media Server) that the tape drive is connected to.

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Tape Drive Is Current	true/ false	A simple true/false on whether the tape drive exists in the current configuration (true) or if it is historical and no longer exists (false)
Tape Drive Serial Number	768ZD03034	The unique serial number for a physical tape drive
Tape Drive Storage Unit Name	dcdell214-dlt-robot-tld-0	The storage unit that the tape drive is assigned to
Tape Drive Type	hcart, hcart2, dlt, 8mm etc.	The type of tape drive as defined by the backup application. For NetBackup this is also called the 'density' and specifies what types of tape can go in the drive.
Tape Drive Unique ID for Library	1, 2, 3, 4, 5, 6 etc.	The tape drive number inside the library
<b>Tape Usage Attributes</b>		
Storage Unit Group Name	Storage Unit Tape Group	The storage unit group that the storage unit that the tape drive belongs to
Tape Drive Assigned	nbu-host.example.com	The host (Media Server) that the tape drive is assigned to for use at time of tape drive information collection
Tape Drive Control	TLD, ACS, DOWN-TLD, DOWN-ACS etc.	The robot type that is controlling the tape drive and it's associated status of up or down at time of tape drive information collection

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Tape Drive Enabled	true / false	A true / false for if the tape drive was enabled at the time of tape drive information collection
Tape Drive In Use	true / false	A true / false for if the tape drive was in use at the time of tape drive information collection
Tape Drive Recorded Media ID	VT0036	The tape that was in the drive at the time of tape drive information collection
Tape Drive Snapshot Time	Apr 05, 2008 22:57:17	The date and time that the tape drive information was collected
<b>Backup Log Attributes</b>		
Backup Log Agent Server	vbr-server.example.com	The host name of the VBR management server where the database and web interface resides
Backup Log Message	backup of client dcdell211 exited with status 71 (none of the files in the file list exist)	The detailed status messages for each job
Backup Log Source Host	nbu-host.example.com	The host server with the backup application that logged the error message
Backup Log Client	nbu-client.example.com	The backup client that was associated with the logged error message
Backup Log Daemon Name	bptm, ndmpagent, nbpem, bpbrm	The process or daemon name that wrote the error message

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Backup Log Job Group ID	5980	The group ID that can be specified by the backup product to group them in a certain way. Note:The secondary ID and the Group ID are basically intended for the same purpose, that is to group the jobs in some way that is useful in reporting.
Log Primary ID	6021	A unique number for each backup job in a backup domain that identifies what backup job caused the error message to be logged
Log Time	Mon 3/4/2008 3:34:34	The date/time that the error message or log was written to
Product	NetBackup, TSM	The backup application name that caused the error message to be created
Severity Code	1, 2, 3, 4 etc.	The severity code of the error message
Type Code	1, 2, 3, 4 etc.	The code representing the type of the log and error message
Version	1, 2, 3, 4 etc.	The version of the log/error message
<b>Agent Monitoring</b>		
Agent Configuration ID	1, 2, 3, 4 etc.	A unique number for each data collection agent under the VBR management server

**Table E-1** Backup data attributes (*continued*)

Data Attributes	Sample Data	Explanation
Agent Host	vbr-agent.example.com	The host name of the VBR data collection agent
Last Heartbeat	May 04, 2008 10:52:28	The date and time of the last heartbeat from the data collection agent to the VBR management server
Management Server	vbr-server.example.com	The host name of the VBR management server where the database and web interface resides
Time Since Agent Last Heartbeat	44	The number of seconds since the last heartbeat from the data collection agent to the VBR management server

# Glossary

<b>Agent</b>	See Veritas Backup Reporter Agent
<b>Alerts</b>	An alert is a warning that the Veritas Backup Reporter (VBR) application generates when a specific condition - usually an alarming situation - occurs in the system. You can notify the concerned officials about the alerts by sending an email or an SNMP trap, which help them take corrective actions. The generated alerts are stored in the VBR database. You can view them using the Alerts section in the VBR console.
<b>Alert Manager</b>	Alert Manager is a component in VBR that comprises an alerting mechanism. It keeps track of the alert conditions specified in the policies and generates alerts appropriately.
<b>Data Collector</b>	Data collector is a part of VBR Agent that collects data from various products.
<b>event</b>	A notification that indicates when an action, such as an alert or a change in state, has occurred for one or more objects on the storage network.
<b>My Reports</b>	In Veritas Backup Reporter, a console area in which to display and run custom reports saved by the user.
<b>Management Server</b>	See Veritas Backup Reporter Management Server
<b>NetBackup Master Server</b>	The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster.
<b>Symantec Product Authentication Service</b>	A component of the Veritas Security Services (VxSS) that is used by the Veritas products to provide user authentication. Symantec Product Authentication Service is a set of processes and runtime libraries that enables users to log on to multiple Veritas products with one logon.
<b>Symantec Private Branch Exchange</b>	A common Veritas component that uses socket passing to reduce the number of ports required to be open across a firewall. Symantec Private Branch Exchange uses a paradigm similar to that of a telephone switchboard in which calls placed to a switchboard are redirected to a known extension. In the PBX exchange, client connections sent to the exchange's port are redirected to an extension associated with the VBR Management Server.
<b>Veritas Backup Reporter console</b>	A graphical user interface that displays reports and other information for users of Veritas Backup Reporter through a standard Web browser. The console provides a central point to manage cost analysis and chargeback for services, managing workflow, displaying and managing reports, and other tasks.

<b>Veritas Backup Reporter database</b>	Sybase SA (SQL Anywhere) database management system containing data related to backup /archive service usage and expenditure, cost metrics and chargeback formulas, and alerts. Veritas Backup Reporter 6.6 uses Sybase SA 10 version. Veritas Backup Reporter database is installed silently when you install Veritas Backup Reporter Management Server.
<b>Veritas Backup Reporter</b>	Veritas™ Backup Reporter (VBR) is a Web-based software application that helps organizations by providing visibility into their data protection environment. By using Veritas Backup Reporter, you can track the effectiveness of data backup and archive operations by generating comprehensive business-level reports.
<b>Veritas Backup Reporter Agent</b>	A Veritas Backup Reporter component that collects information from discoverable applications residing on remote host systems, such as Veritas NetBackup, Veritas Backup Exec, EMC Legato Networker, or Enterprise Vault. Veritas Backup Reporter formats the information collected from these applications and displays it through the Veritas Backup Reporter console.
<b>Veritas Backup Reporter Management Server</b>	Veritas Backup Reporter Management Server, the core of the architecture, is a Web application that normalizes backup / archive data collected from various applications. This normalized data is used for reporting on backup related information.
<b>Veritas Backup Reporter View Builder</b>	The Veritas Backup Reporter Java View Builder is an application in which an administrator creates, modifies, and manages access to the Veritas Backup Reporter views that users see in the console..
<b>Veritas NetBackup</b>	A Veritas product family designed to provide a fast, reliable backup and recovery solution for environments ranging from terabytes to petabytes in size. The term is used to refer to either of two products that interact with Veritas Backup Reporter: Veritas NetBackup DataCenter and Veritas NetBackup Business Server.
<b>Views</b>	Veritas Backup Reporter views are logical groups of IT assets (hosts or file systems) organized in a hierarchical manner. You can create views in Java View Builder and make them available in the Veritas Backup Reporter console. The following view details appear in the Veritas Backup Reporter console.
<b>Volume Manager</b>	A Veritas software product installed on storage clients that enables management of physical disks as logical devices. Volume Manager enhances data storage management by controlling space allocation, performance, data availability, device installation, and system monitoring of private and shared systems.

# Index

## A

- access levels 163–164
- accessing
  - NetBackup Operations Manager host 127
- adding
  - attributes 293
- advanced filters
  - disk-based data protection reports 354
- Agent
  - overview 26
- agent
  - data collectors
    - copying configurations 197
    - resolving authentication failures manually 72, 110
- agent alerts
  - viewing 185
- Agent deployment 42
- agent.conf file 30
- agentauth 542
- agentdatacollection utility 258
- alert conditions. *See* policy types
- Alert Manager 295, 325
  - disabling 322
- alert policies
  - creating 307
  - managing 313
  - modifying 312
  - viewing 312
- alerts
  - description 295
  - managing 318
  - report-generated 341
  - report-triggered 269
  - viewing 315
- Alias X Axis Name parameter 355
- Alias Y Axis Name parameter 355
- aliases
  - updating 289
- application.properties 152
- archive data 237, 405

- archive report categories 406
  - Archive Storage reports 406
  - Exchange reports 406
- archive reports 405, 410. *See* filter parameters 409
- Archive Storage reports 406
  - Archived Size report 427
  - Storage Details report 430
- Archive Window report 424
- Archived Size report 427
- Archives report category 405
- archiving
  - scheduling 263
- archiving reports
  - setting up 273
- attributes
  - changing 293
  - creating 293
  - displaying 289, 294
  - editing 294
  - user-defined 293
  - viewing 289, 294
- authentication failures
  - resolving manually 72, 110

## B

- backing up
  - Veritas Backup Reporter database 133
- backup
  - jobs
    - displaying 289
  - reports 333
- BackupExec data collector 221
- Breakup Jobs option 210
- business planning 19

## C

- cached reports 347
- canned reports 348
  - Archive Window report 424
  - Archived Size report 427

- canned reports *(continued)*
  - Cont of Items report 423
  - Enterprise Vault 410
  - Mailbox Quota report 425
  - Original Size report 420
  - Original Size Vs Archived Size report 426
  - Storage Details report 430
  - Target Details report 426
- categories
  - object view 286
- cc\_users 55
- ccsvc password 554
- Certificate Authority
  - CA 158
- changing
  - attributes 293–294
- Changing database password
  - Sybase ASA 554
- changing user password 261
- chargeback
  - cost variables 455, 457
  - formulas 458–459
  - modeling 452
  - overview 451
  - reports 460
- cluster support
  - VCS 36
- collecting
  - NetBackup data 198
- collection status
  - completed 177
  - failed 177
- columns
  - reports 356
- comma-separated file
  - saving report 443
- commands
  - adding 576
  - browsing 575
  - database 575
  - deleting 578
  - modifying 577
- communication protocols 46
- CommVault data collector 236
- CommVault Galaxy Backup & Recovery 236
- compliance reporting 18
- configuration files 519
  - vbr\_conf.properties 522
- configuring
  - Enterprise Vault data collector 251
  - NetBackup data collector 198
    - user settings 261
  - configuring NetBackup PureDisk data collector 229
- contact information
  - users 163–165
- copying
  - data collector configurations 197
- CORBA 46
- correlation reports 331
- Cost Formula parameter 355
- Cost Formula wizard 458–459
- Cost Variable wizard 455, 457
- costs
  - formulas
    - defining 458
    - deleting 459
    - modifying 459
    - reports 355
  - overview 451
  - reports
    - generating 460
    - variables 455
  - variables
    - creating 455
    - modifying 457
- Count of Items report 423
- creating
  - alert policies 307
  - attributes 293
  - cost formulas 458
  - cost variables 455
  - custom reports 430, 433
  - email recipients 300
  - recipient groups 306
  - SNMP trap recipients 303
- creating principal user 57
- creating private domain users 164
- Custom Report Wizard
  - columns parameters
    - populating table columns 435
  - data parameters 434
  - data selection parameters 433
  - description 430
  - filter parameters
    - selecting 440
    - using 440
  - filtering parameters 440

- Custom Report Wizard *(continued)*
  - forecast parameters 437
  - time frame parameters 437
  - trending parameters 437
- custom reports 433
  - data 434
  - scope 433
  - table columns 435
  - time frame 437
  - trending 437
- custom SQL queries
  - copying 447
  - creating 445
  - deleting queries 448
  - functionality 444
  - modifying 447
  - running instant database queries 446
  - running saved database queries 446
  - tasks 444
  - viewing saved queries 448
- custom views 292
  - storage 291
  - verifying 292
- customizing
  - Alert Manager setting 321
  - autoclear setting 322
  - autocount setting 322

## D

- daemons
  - vbragent 551
  - vbrserver 548, 556
- data
  - in graphical reports 332
  - parameters 434
- data collector
  - deleting 197
- data collectors
  - copying configurations 197
- data selection parameters 433
- data transmission errors 177
- database queries 444
  - deleting 448
  - modifying 447
  - viewing saved queries 448
- dba password 554
- dbbackup 546
- dbisql
  - querying VBR database 516–517

- deduplication 223, 465
- deduplication reports 333
- default reports 348
- Define Viewable Columns parameter 356
- defining
  - cost formulas 458
  - cost variables 455
- deleting
  - cost formulas 459
  - data collector 197
- deploying
  - Agent 42
- deployment mode
  - multi domain 242
  - single domain 242
  - standalone mode 243
- dialog windows
  - Edit Attribute 294
- disk-based data protection feature
  - job storage type parameter 455
- disk-based data protection reports 333
  - DBDP 336
- Display Unit parameter 355
- distribution lists
  - email 264
- domains
  - user membership 165

## E

- Edit Attribute dialog window 294
- editing
  - attributes 294
- email
  - reports
    - body 265
    - scheduling 263
    - sending reports by 342
    - variable tokens 272
- email distribution lists 264
- email notification formats 303
- email recipients
  - creating 300
- EMC Legato Networker 234
- Enterprise Vault 237, 405, 409
  - Advanced Filters 409
  - Archive Storage reports 410
  - canned reports 410
  - custom reports 430
  - data types 238

Enterprise Vault (*continued*)

- Exchange reports 410
- generating archive reports. *See* generating Enterprise Vault reports
- Report On filter parameters 409
- reports 237, 405. *See* archive reports
- Veritas Backup Reporter integration 237
- versions supported 240

Enterprise Vault data collector 251

- data collection checklist 258
- deployment scenarios 240
- logs 257

Enterprise Vault view object 279

error codes

- database 575
  - adding 576
  - browsing 575
  - deleting 578
  - modifying 577

eventposter 525

Exchange Reports 406

Exchange reports

- Mailbox Quota report 425
- Original Size report 420
- Original Size Vs Archived Size report 426
- Target Details report 426

Exchange Server. *See* Microsoft Exchange Server

explorer reports 399

exporting

- report data 443
- reports 150
- xml 538

exporting SSL certificate 157

**F**

file systems

- displaying 289
- views 292

filter parameters

- showing 441

filtering

- parameters 440
- report data 354

firewalls

- ports 46
- Symantec Private Branch Exchange 23
- Veritas Backup Reporter requirements 46

forcing poll updates 196

forecast

- parameters 354–355, 437
- reports 331, 355

Formula Modeling Tool 452

formulas

- costs
  - defining 458
  - deleting 459
  - modifying 459
  - reporting 355
  - variables 455
- modeling 452

## G

generating archive reports 410

generating reports

- temporary files 152

generating savings report

- savings report 465

guest account 516–518

guest password 554

## H

help search tool 126

hierarchy

- object views 286

host views

- backup 292
- custom 292
- verifying 292

hosts

- accessing products 130
- attributes 289
- backup jobs 289
- displaying reports 290
- file systems 289
- IP addresses 290
- searching for 288
- updating aliases 289

HTTP 46

HTTPS 46

## I

IBM Tivoli Storage Manager 235

importing

- xml 538

- installing
  - Veritas Backup Reporter
    - Solaris 60
    - Windows 65
- Installing Veritas Backup Reporter 59
- installvbr 60
- Interactive SQL 517
- IP addresses 290

**J**

- Java View Builder 278–279
  - logging in 281
  - running 281
- JDBC
  - querying VBR database 518
  - VBR database
    - querying 516
- jobutility 528

**K**

- Knowledge Base
  - adding entries 576
  - browsing entries 575
  - deleting entries 578
  - modifying entries 577
  - overview 575

**L**

- Legato data collector 234
- levels
  - object views
    - appearance 287
    - description 286
    - numbering 287
  - reports 333, 352
- license keys
  - adding 161
  - deleting 162
  - viewing 162
- licensing
  - obtaining information 513
- licensing model 160
- links
  - Symantec products 130
- logging
  - Veritas Backup Reporter Management Server 142

- logging on
  - Veritas Backup Reporter 119
- login 119

## M

- Mailbox Quota report 425
- Mailbox Quota reports
  - By Receive Limit 425
  - By Send Limit 425
  - By Warning Limit report 425
- Manage Folders wizard 346
- Management Information Base. *See* MIB
- max heap size
  - setting 467
- merging objects 168
- MIB 325
- Microsoft Exchange Server. *See* Exchange Server
- Microsoft SQL Server
  - versions supported 240
- modeling
  - chargeback 452
- modifying
  - alert recipients 305
  - cost formulas 459
  - cost variables 457
  - custom reports 351, 442
  - Veritas Backup Reporter
    - Solaris 85
    - Windows 85
- Monitor Dashboard reports 333
- My Reports folder
  - managing 346
- My Reports page
  - creating sections 344
  - deleting sections 345
  - edit sections. *See* renaming sections
  - overview 343
  - tree view 344
  - using 343

## N

- nbpemreq 198
- NetBackup data collector 198
  - data collection checklist 219
  - logs 209
- NetBackup PureDisk
  - Single Instance Storage SIS 465

- new functions 20
- node objects
  - adding to object views 282
  - removing from object views 283–284
- notes 576
- notification
  - variable tokens 272
- numeric data
  - viewing 332

## O

- object views
  - accessing 284–285
  - adding node objects 282
  - categories 286
  - creating 281
  - creating levels 282
  - custom 292
  - file system 292
  - hierarchy 286
  - launching 291
  - levels 286–287
  - managing levels 282
  - removing node objects 283–284
  - searching 283, 288
  - selecting 285
  - structure 286
  - summary 285
  - tables 291
  - using 291
- objects
  - renaming 294
  - viewing in console 285, 291
- operating system requirements
  - Agent 36
  - Java View Builder 36
  - Management Server 36
- Original Size report 420
- Original Size Vs Archived Size report 426

## P

- pages
  - views 285
- pagination settings 315
- parameters
  - Custom Report Wizard 433
  - Report Wizard 352
- PBX 23

- PDOS 223
- personal information
  - updating 261
- pie chart reports 331
- policy types 295
- portal pages
  - updating 347
  - using 343
- ports
  - 1556 46
  - 1885 46
  - 25 46
  - 2821 46
  - 7806 46
  - 8181 46
  - 8443 46
  - accessing products 130
  - changing VRTSweb HTTP port 51
  - firewalls 46
    - Symantec Private Branch Exchange 23
  - prerequisites 35
  - preserving report data 443
  - printing
    - reports 444
  - privileges
    - user accounts 163–164
  - Protected Job Size
    - data protected 465
  - protocols
    - communication 46
  - PureDisk reports
    - table columns 435
  - PureDisk savings reports
    - Protected Job Size variable metric 455

## R

- ranking reports 331
- recipient groups
  - creating 306
- recipients
  - viewing 298
- refreshing
  - reports 347
- removing trust relationship 153
- renaming
  - objects 294
- report category
  - Archives 405
- Report Clean Up Schedule 152

- report formats 331
- Report Grouping parameter 352
- report mode 290
- Report Time Frame Grouping parameter 354
- Report Time Frame parameter 353
- Report Time Frame Trendline parameter 354
- Report Wizard 348, 350
  - exception condition parameters 356
  - parameters
    - Alias X Axis Name 355
    - Alias Y Axis Name 355
    - Cost Formula 355
    - Define Viewable Columns 356
    - Display Unit 355
    - Filter options 354
    - Forecast Parameters 355
    - Report Grouping 352
    - Report Time Frame 353
    - Report Time Frame Grouping 354
    - Report Time Frame Trendline 354
    - Retries Restriction 355
    - Target Performance 355
- reporting on
  - archive reports 405
  - Scheduled Jobs reports 390
- reports
  - archiving
    - scheduling 263
    - setting up. *See* exporting
  - backup 333
  - cached 343, 347
  - cleaning temporary files 152
  - conditions 341, 440
  - creating 352
  - custom 430, 442
    - creating 433
    - saving 442
  - default 348
  - displaying 343
  - displaying for hosts 290
  - email
    - body 265
    - distribution lists 264
    - scheduling 263
    - sending 342
  - export path 150
  - exporting 443
    - scheduling 263
  - file system 292
  - reports (*continued*)
    - filter parameters 441
    - forecast 437
    - formats 331, 333
    - graphical
      - formats 331
      - lower level 333
      - numeric data 332
      - saving 333
    - modifying 351
    - My Reports page 343–345
    - notification
      - alerts 269, 341
      - condition parameters 440
      - email 341
    - overview 329
    - portal pages 343
      - refreshing 343
      - selecting reports 344
    - predefined 348
    - preserving data 443
    - printing 444
    - restore jobs. *See* restore image
    - sample 349
    - saving 442
      - CSV file 443
      - TSV file 443
    - Scheduled Jobs 393
    - scope 350, 352
    - storage units 355
    - subject pages
      - My Reports folder 346
    - tabular 333
    - time frame 350, 353–354
    - ToolTips in 332
    - tree view 344
    - X- and Y-axis labels 355
  - reports custom
    - filtering parameters 440
  - requirements
    - firewalls
      - Veritas Backup Reporter 46
  - restore job reports 333, 448
  - restoring
    - Veritas Backup Reporter database 134
  - Retries Restriction parameter 355
  - runstoredquery 531

- S**
- sample reports 349
  - saving
    - custom reports 442
    - data in reports 442
    - report contents 333
  - schedule time 198
  - Scheduled Jobs 198
  - Scheduled Jobs data 198
  - Scheduled Jobs reports 390, 393
    - All Jobs report 392
  - scheduled jobs reports
    - Job Count Details-Scheduled Vs Actual report 397
    - Job Count Within Backup Window report 396
    - Job Count-Scheduled Vs Actual report 394
  - scheduling
    - reports 263
  - scope
    - reports 433
  - scripts
    - eventposter 525
    - installvbr 60
    - jobutility 528
    - runstoredquery 531
    - support 533
    - vbrserver 548, 556
    - vbrvb 553
    - xml 538
  - searching
    - hosts 288
  - setting
    - default currency 275
  - setting alert filters 314
  - setting up trust relationship 153
  - Simple Network Management Protocol. *See* SNMP
  - Single Instance Storage
    - SIS 223
  - SIS
    - single instance storage 435
  - SMTP 46
  - SNMP 323
  - SNMP trap community name 325
  - SNMP trap port 326
  - SNMP trap recipients
    - creating 303
  - SNMP traps
    - generating 325
  - SNMP versions 324
  - Solaris
    - installing
      - Veritas Backup Reporter 60
    - modifying
      - Veritas Backup Reporter 85
    - Veritas Backup Reporter Agent
      - starting 115
      - stopping 115
    - Veritas Backup Reporter Management Server
      - starting 113
      - stopping 113
  - SQL
    - dbisql 517
    - Interactive SQL 517
  - SSL
    - certificates 155
  - SSL certificate
    - exporting 157
  - SSL certificate
    - cloning 159
    - configuring CA-signed SSL certificate 158
  - starting
    - eventposter 525
    - jobutility 528
    - Management Server service
      - Solaris 113
    - runstoredquery 531
    - vbragent 551
    - vbrserver 548, 556
    - vbrvb 553
    - Veritas Backup Reporter Agent
      - Solaris 115
    - Veritas Backup Reporter Management Server
      - Windows 114
    - Veritas Backup Reporter services 114
  - stopping
    - vbragent 551
    - vbrserver 548, 556
    - Veritas Backup Reporter Agent
      - Solaris 115
    - Veritas Backup Reporter Management Server
      - Solaris 113
      - Windows 114
    - Veritas Backup Reporter services 114
  - storage
    - units in reports 355
  - Storage Details report 430
  - support 533
    - documentation comments 513

support (*continued*)

- e-mail 512–513
- license information 513
- phone 513
- purchasing 513
- web site 512
- supported backup products 19, 333
  - CommVault Galaxy Backup & Recovery 40, 187
  - EMC Legato NetWorker 40, 187
  - IBM Tivoli Storage Manager 40, 187
  - Symantec Backup Exec 40, 187
  - Symantec Enterprise Vault 40, 187
  - Veritas NetBackup 40, 187
  - Veritas NetBackup PureDisk 40, 187
- supported data types 333
- supported operating systems 36
- Symantec
  - products
    - accessing 130
  - Symantec Private Branch Exchange 23
  - Symantec Product Authentication Service 57
    - authenticating agent 542
    - overview 25
  - Symantec products
    - setting up trust relationship 153
- symhelp 126

**T**

- tab-separated file
  - saving report 443
- tables
  - launching object views 291
  - reports 333
  - summary 291
- Target Details report 426
- Target Performance parameter 355
- task pane
  - object levels 287
  - object view categories 286
- TCP/IP 46
- thresholds
  - report 341, 440
- time frame
  - absolute 353
  - grouping 354
  - parameters 353–354
  - relative 353
  - trendline 354
  - units 354

## time frames

- parameters 437
- tokens 272
- ToolTips 332
- tree view
  - Veritas Backup Reporter console 286
- trending parameters 354, 437
- trending reports 354
  - format 331
- troubleshooting
  - support 533
- TSM
  - data collector 235

**U**

- UDP 46
- uninstalling
  - Veritas Backup Reporter
    - Solaris 74
    - Veritas Backup Reporter on Windows 75
- updating
  - personal information 261
  - reports 347
- upgrading
  - Veritas Backup Reporter Agent
    - Solaris 79
  - Veritas Backup Reporter Management Server
    - Solaris 79
  - View Builder
    - Solaris 79
- Upgrading Veritas Backup Reporter 76
- user accounts
  - access levels 163–164
  - adding to user groups 167
  - creating 163
  - deleting 166
  - domains 165
  - editing 166
  - private domains 164
  - viewing 165
- user groups
  - adding user accounts to 167
  - creating 166
  - deleting 168
  - editing 167
- users
  - contact information 163–165

- ## V
- variable tokens 272
  - VBR console
    - Knowledge Base 575
  - VBR database
    - connection details 517
    - connection information 516, 518
    - namespaces 516
    - querying
      - dbisql 516–517
      - JDBC URLs 516, 518
  - vbr\_conf.properties 150, 522
  - vbragent
    - starting 551
    - stopping 551
  - vbrserver
    - starting 548, 556
    - stopping 548, 556
  - vbrvb 553
  - Veritas Backup Reporter
    - firewall requirements 46
    - installing
      - Solaris 60
      - Windows 65
    - logging on 119
    - modifying
      - Solaris 85
      - Windows 85
    - reports 329
    - sanity check after installing 73, 111
    - starting services 114
    - stopping services 114
    - uninstalling
      - Solaris 74
      - Windows 75
  - Veritas Backup Reporter 6.6 functions 20
  - Veritas Backup Reporter Agent
    - agentauth 542
    - authenticating 542
    - Solaris
      - starting 115
      - stopping 115
      - upgrading 79
    - starting (Solaris) 551
    - stopping (Solaris) 551
  - Veritas Backup Reporter architecture
    - database 24
    - Server and Authentication Service 25
    - Veritas Backup Reporter clustering
      - known issues 107
      - limitations 88
    - Veritas Backup Reporter clustering on Solaris 105
      - prerequisites 101
      - removing a node 106
    - Veritas Backup Reporter clustering on Solaris nodes
      - installing Veritas Backup Reporter
        - adding a new node 103
    - Veritas Backup Reporter console 122
      - content pane 125
      - header 123
      - object views 285, 291
      - online Help 126
      - products
        - accessing 130
      - tabs 123
      - task pane 125
      - tree view 286
    - Veritas Backup Reporter database
      - backing up 133
      - restoring 134
    - Veritas Backup Reporter Management Server 22
      - Authentication Service 25
      - logging 142
      - ports 46
      - Solaris
        - starting 113
        - stopping 113
        - upgrading 79
      - starting 548, 556
      - stopping 548, 556
      - Web server port settings 140
      - Windows
        - stopping 114
    - Veritas Backup Reporter reports
      - report types 330
    - Veritas Backup Reporter services 112
    - Veritas Backup Reporter View Builder. See View Builder 30
    - Veritas Backup Reporter views
      - overview 278
    - Veritas Backup Reporter XML
      - DTD 560
      - DTD elements 561
      - example files 566
    - Veritas NetBackup PureDisk
      - PDOS 223

- View Builder
  - Solaris
    - upgrading 79
  - starting 553
  - using 292
- viewing
  - agent alerts 185
  - alert recipients 298
  - email recipients 298
  - objects 285, 291
  - recipient groups 298
  - trap recipients 298
- Viewing agent status
  - data collector status
  - data type status 177
- views
  - customizing 291
- VRTSweb HTTP port
  - changing 51

## W

- Web browser requirements 36
- Web server port
  - Veritas Backup Reporter Management Server 140
- Windows
  - installing
    - Veritas Backup Reporter 65
  - modifying
    - Veritas Backup Reporter 85
  - uninstalling
    - Veritas Backup Reporter 75
  - Veritas Backup Reporter Management Server
    - starting 114
    - stopping 114
- wizards
  - Cost Formula 458–459
  - Cost Variable 455, 457
  - Custom Report Wizard 433
  - Manage Folders 346
  - Report Wizard 352

## X

- XML
  - DTD 560
  - examples for importing 566
  - exporting 538
  - importing 538, 560

xml 538