

# Veritas Backup Reporter Installation Guide



# Veritas Backup Reporter Installation 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 6.0

PN: : (HRO7210)SKU 11132088

## Legal Notice

Copyright © 2006 Symantec Corporation.

All rights reserved.

Federal acquisitions: Commercial Software - Government Users Subject to Standard License Terms and Conditions.

Actionable Infrastructure™, Active Extensions™, ActiveAdmin™, Anti-Freeze™, Application Saver™, Backup Exec™, Bare Metal Restore™, BindView™, Bloodhound™, Bootguard™, Brightmail™, bv-Admin™, bv-Control™, CarrierScan™, CleanSweep™, ColorScale™, CommandCentral™, Confidence Online™, CrashGuard™, Day-End Sync™, dbAnywhere™, DeepSight™, Defender™, Digital Immune System™, DiskDoubler™, DiskLock™, Drive Image™, Enterprise Security Manager™, Enterprise Vault™, FlashSnap™, FlowChaser™, Ghost Walker™, Ghost™, GoBack™, Healthy PC™, i3™, iCommand™, I-Gear™, InDepth™, Information Integrity™, Intellicrypt™, Intruder Alert™, LiveUpdate™, LiveState™, Mail-Gear™, ManHunt™, ManTrap™, MicroMeasure™, Mobile Update™, NetBackup™, NetProwler™, NetRecon™, Norton™, Norton 360™, Norton AntiSpam™, Norton AntiVirus™, Norton Commander™, Norton Editor™, Norton Guides™, Norton Internet Security™, Norton Mobile Essentials™, Norton Password Security™, Norton SystemWorks™, Norton Utilities™, Norton WinDoctor™, OmniGuard™, OpForce™, PartitionMagic™, pcAnywhere™, PowerQuest™, PowerVPN™, Procomm™, Procomm Plus™, PureDisk™, QuickLog™, Raptor™, Recourse Technologies™, RELICORE™, Replication Exec™, SafetySweep™, SANPoint™, SANPoint Control™, SecureExchange™, SecureLink™, ServerMagic™, SESA™, SiteStor™, SmartSector™, SmarTune™, Speed Disk™, SpeedSend™, Storage Exec™, StorageCentral™, Sygate™, Symantec™, Symantec AntiVirus Research Center (SARC)™, Symantec AntiVirus™, Symantec DeployCenter™ Library, Symantec Enterprise Security Architecture™, Symantec Inform™, Symantec Insight™, Symantec Intruder Alert™, Symantec Logo, Symantec Mail-Gear™, Symantec Mobile Essentials™, Symantec ON Command Discovery™, Symantec ON iCommand™, Symantec ON iPatch™, TalkWorks™, TruStor™, UnErase™, UpScale™, V2i™, V2i Builder™, V2i Protector™, V2i Observer™, VelociRaptor™, Veritas™, Veritas Data Center Foundation™, Veritas Server Foundation™, Veritas Storage Foundation™, Vision360™, Virtually Anywhere™, WebDefender™, WinFax™, WipeDisk™, WipeFile™, Work Virtually Anywhere™

Windows is a trademark of Microsoft Corporation. Additional company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged.

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" and "commercial computer software documentation" as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino,  
CA 95014 USA  
<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 feature and function, installation, and configuration. The Technical Support group also authors 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
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

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

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

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

## Contacting Technical Support

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

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

Select your region or language under Global Support.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate 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/ent/enterprise.html](http://www.symantec.com/techsupp/ent/enterprise.html)

Select your region or language under Global Support, and then select the Licensing and Registration page.

## Customer service

Customer service information is available at the following URL:

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

Select your country or language under Global Support.

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 insurance and maintenance contracts
- Information about the Symantec Value License Program

- 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: [contractsadmin@symantec.com](mailto:contractsadmin@symantec.com)
- Europe, Middle-East, and Africa: [semea@symantec.com](mailto:semea@symantec.com)
- North America and Latin America: [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

## 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 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.

# Symantec Software License Agreement

## Veritas Backup Reporter 6.0

PLEASE READ THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AGREEMENT BETWEEN YOU AND SYMANTEC CORPORATION (“LICENSOR”). LICENSOR AGREES TO LICENSE THE LICENSED SOFTWARE AND RELATED DOCUMENTATION TO YOU (PERSONALLY AND/OR ON BEHALF OF YOUR EMPLOYER) ONLY IF YOU ACCEPT ALL THE TERMS CONTAINED IN THIS AGREEMENT. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE “ACCEPT” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING OR USING THE LICENSED SOFTWARE YOU INDICATE YOUR ACCEPTANCE OF THE TERMS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE “DO NOT ACCEPT”, “DECLINE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE LICENSED SOFTWARE AND WITHIN THIRTY (30) DAYS OF YOUR PURCHASE OF THE LICENSED SOFTWARE YOU MAY RETURN THE LICENSED SOFTWARE, ALONG WITH ALL ACCOMPANYING DOCUMENTATION, PACKAGING MATERIALS AND PROOF OF PURCHASE, TO THE LICENSOR RESELLER OR DEALER FROM WHOM YOU OBTAINED IT (OR TO LICENSOR IF THE LICENSED SOFTWARE WAS ORDERED DIRECTLY FROM LICENSOR), FOR A FULL REFUND.

Should You have any questions regarding this Agreement, or wish to contact Licensor, You may write to Symantec Corporation, Attention: : Legal Department, 20330 Stevens Creek Blvd, CC1, 1st Floor Cupertino, CA 95014.

### 1. License Grant:

Subject to Your compliance with the terms and conditions of this Agreement and Your payment of the applicable license fees, Licensor grants You a non-exclusive, non-transferable license to use a single copy of the executable code version of the computer software including any Licensor modifications, corrections or updates supplied to You now or under a Maintenance/Support program (“Licensed Software”) and all associated user manuals, release notes, installation notes, and other materials delivered with the Licensed Software in hard copy or electronic formats (“Documentation”). You may use the Licensed Software and Documentation solely in support of Your internal business operations for the number of Managed Backup Devices or other license or usage limitations (“Use Levels”) as indicated in the applicable Licensor license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or following this Agreement, for the country in which the Licensed

Software was furnished to You (“Territory”) and as may be further defined in the user documentation accompanying the Licensed Software. The Licensed Software may contain third party software programs as further specified in the Documentation for the Licensed Software. Any such third party software is provided under and subject to the terms and conditions of the license agreement applicable to such software, as indicated in the Documentation for the Licensed Software. Licensed Software may not be used in excess of the applicable Use Levels unless You purchase the additional requisite number of licenses for such use. You may make a single copy of the Licensed Software and Documentation for archival purposes, provided You reproduce all copyright and other proprietary notices contained in the original copy of the Licensed Software and Documentation. The Licensed Software and Documentation is licensed, not sold, to You for use pursuant to the terms of this Agreement. You own the media on which the Licensed Software and/or Documentation is recorded, but Licensor and/or its suppliers retain all right, title and interest in the Licensed Software and Documentation itself, to all patents, copyrights, trade secrets, trademarks and all other intellectual property rights embodied in the Licensed Software and Documentation and in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software or Documentation. Your rights to use the Licensed Software and Documentation shall be limited to those expressly granted in this Section 1. All rights not expressly granted to You are retained by Licensor and/or its suppliers.

### 2. Restricted Use:

You agree not to cause or permit the use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software or Documentation, except as expressly provided in this Agreement. You may not: (i) create any derivative works based on the Licensed Software or Documentation; (ii) reverse engineer, disassemble, or decompile the Licensed Software (except that You may decompile for the purposes of interoperability only to the extent permitted by and subject to strict compliance with applicable law); (iii) use the Licensed Software or Documentation in connection with a service bureau or like activity whereby You, without purchasing a license from Licensor, operate or use the Licensed Software or Documentation for the benefit of a third party who has not purchased a copy of the Licensed Software; or (iv) permit the use of the Licensed Software or Documentation by any third party without the prior written consent of Licensor . In addition, You shall not release the results of any benchmark testing of the Licensed Software to any third party without the prior written consent of Licensor.

### 3. Services:

You may acquire under a separate agreement, education, installation, implementation, configuration, professional or consulting services (“Services”) from Licensor pursuant to the then applicable Licensor Services policies and the in-country list prices in effect at the time the Services are ordered.

### 4. Maintenance/Support:

You may acquire maintenance/technical support services (“Maintenance/Support”) for the Licensed Software provided that You subscribe to Licensor’s Maintenance/Support programs or to an authorized Licensor partner support program. Maintenance/Support shall be based on the in-country list price and then applicable Maintenance/Support policy in effect at the time such Maintenance/Support is ordered. Maintenance/Support fees are due annually in advance and are nonrefundable and non-cancelable.

### 5. Limited Warranties; Disclaimer:

#### 5.1 Licensed Software Performance Warranty; Media Warranty:

Licensor warrants that the Licensed Software, as delivered by Licensor and when used in accordance with the Documentation, shall substantially conform with the Documentation for a period of ninety (90) days from delivery and that the media upon which the Licensed Software is furnished to You shall be free from defects in material and workmanship under normal use for a period of ninety (90) days from delivery.

#### 5.2 Licensed Software Warranty Remedies:

For any Licensed Software that does not operate as warranted in Section 5.1, Licensor shall, at its sole discretion, either repair the Licensed Software, replace the Licensed Software with software of substantially the same functionality, or terminate the license and refund the relevant license fees paid for such non-compliant Licensed Software only when You return the Licensed Software to Licensor or its authorized reseller, from whom You obtained the Licensed Software, with the purchase receipt within the warranty period. The above warranties specifically exclude defects resulting from accident, abuse, unauthorized repair, modifications or enhancements, or misapplication.

#### 5.3 Maintenance/Support Warranty:

Licensor warrants, for a period of thirty (30) days from the date of performance of the Maintenance/Support covered by this warranty that the Maintenance/Support shall be performed in a manner consistent with generally accepted industry standards.

#### 5.4 Maintenance/Support Remedies:

For Maintenance/Support not performed as warranted in Section 5.3, and provided Licensor has received written notice of such non-conformance within thirty

(30) days of performance of the Maintenance/Support, Licensor shall, at its discretion, either correct any nonconforming Maintenance/Support or refund the relevant fees paid for the specific nonconforming Maintenance/Support service.

### 5.5 DISCLAIMERS:

THE WARRANTIES SET FORTH IN SECTIONS 5.1 AND 5.3 ARE YOUR EXCLUSIVE WARRANTIES AND ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, AND LICENSOR EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND WARRANTIES OF STATUTORY NON-INFRINGEMENT. NO THIRD PARTY, INCLUDING AGENTS, DISTRIBUTORS, OR AUTHORIZED LICENSOR RESELLERS IS AUTHORIZED TO MODIFY ANY OF THE ABOVE WARRANTIES OR MAKE ANY ADDITIONAL WARRANTIES ON BEHALF OF LICENSOR. LICENSOR DOES NOT WARRANT THAT THE LICENSED SOFTWARE SHALL MEET YOUR REQUIREMENTS OR THAT USE OF THE LICENSED SOFTWARE SHALL BE UNINTERRUPTED OR ERROR FREE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE LICENSED SOFTWARE OR TO THE MINIMUM PRESCRIBED BY LAW. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY DEPENDING ON THE TERRITORY IN WHICH THE LICENSED SOFTWARE WAS FURNISHED TO YOU. NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT ANY LIABILITY OF LICENSOR WHICH CANNOT BE EXCLUDED OR LIMITED BY ANY LAW OR REGULATION APPLICABLE TO THIS AGREEMENT. FOR WARRANTY ASSISTANCE CONTACT LICENSOR OR THE LICENSOR RESELLER FROM WHOM YOU OBTAINED THE LICENSED SOFTWARE.

### 6. Evaluation License:

Notwithstanding any provision of this Agreement to the contrary, the following terms and conditions shall apply to any Licensed Software acquired by You for purposes of evaluation. Any evaluation license for the Licensed Software shall terminate sixty (60) days from the date of Your initial installation of the Licensed Software. The Licensed Software may be used solely for internal non-production evaluation. You may not use an evaluation copy of the Licensed Software for any purpose, including production use, other than evaluation. The Licensed Software may not be transferred, is licensed to You without fee, and is provided “AS IS” without warranty of any kind. To the maximum extent permitted by applicable law, You agree to release, defend and indemnify and hold Licensor harmless from any claims and/or damages of any kind, by any party or entity, arising out of Your use of the Licensed Software for evaluation. All other terms and conditions of this

Agreement shall otherwise apply to the Licensed Software.

## 7. Termination:

This Agreement is effective until terminated. This Agreement, including without limitation Your right to use and copy the Licensed Software as specified in Section 1, terminates immediately and without notice from Licensor if You fail to comply with any of its provisions. Upon termination You shall immediately discontinue use of and destroy the Licensed Software and all copies or portions thereof, including any master copy, and within ten (10) days certify in writing to Licensor that all copies have been destroyed. Your payment obligations incurred prior to termination shall survive termination of this Agreement.

## 8. Limitation of Liability:

IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE TO YOU OR ANY PERSON FOR ANY COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS OR SERVICES, LOSS OF PROFITS, LOSS OF, OR CORRUPTION OF DATA, LOSS OF PRODUCTION, LOSS OF BUSINESS, LOSS OF REVENUES, LOSS OF CONTRACTS, LOSS OF GOODWILL OR ANTICIPATED SAVINGS OR WASTED MANAGEMENT AND STAFF TIME, OR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, OR ANY AND ALL OTHER SIMILAR DAMAGES OR LOSS EVEN IF LICENSOR, ITS RESELLERS, SUPPLIERS OR ITS AGENTS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT AS LIMITED BY APPLICABLE LAW, REGARDLESS OF THE LEGAL BASIS FOR YOUR CLAIM, LICENSOR'S AND ITS SUPPLIERS' TOTAL LIABILITY UNDER THIS AGREEMENT SHALL BE LIMITED TO DIRECT DAMAGES WHICH SHALL NOT EXCEED THE AMOUNT OF FEES PAID FOR THE LICENSED SOFTWARE GIVING RISE TO THE CLAIM. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

## 9. U.S. Government Rights:

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.

## 10. Compliance With Law:

Each party agrees to comply with all applicable laws, rules, and regulations in connection with its activities under this Agreement. You acknowledge that the Licensed Software, Documentation, related technical data and/or controlled technology may be subject to the export and import control laws of the United States and any country where the product or controlled technology is manufactured or received. By using Licensed Software, Documentation, related technical data and/or controlled technology, You agree that You will not violate any such laws. You agree not to export any Licensed Software, Documentation, related technical data and/or controlled technology to any prohibited country, entity, or person for which an export license or other governmental approval is required. Obtaining necessary licenses and approvals is solely Your obligation. You agree that You will not export or sell any Licensed Software, Documentation, related technical data and/or controlled technology for use in connection with chemical, biological, or nuclear weapons, or missiles capable of delivering such weapons.

## 11. General:

You agree to pay all fees under this Agreement net thirty (30) days from date of invoice. You agree to pay any tax assessed on the Licensed Software, other than taxes based on Licensor's net income or corporate franchise tax. This Agreement shall be governed by and construed in accordance with the laws of the State of California, exclusive of any provisions of the United Nations Convention on Contracts for Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. Any suits concerning this Agreement shall be brought in the federal courts for the Northern District of California or the state courts in Santa Clara County, California, or if the matter is brought by Licensor, in a court of competent jurisdiction in Your domicile. This Agreement is personal and may not be assigned or assumed (including by operation of law) without Licensor's prior written consent. A change of control shall constitute an assignment. During the period this Agreement remains in effect, and for three years thereafter, Licensor has the right to verify Your compliance with this Agreement on Your premises during Your normal business hours and in a manner that minimizes disruption to Your business. Licensor may use an independent auditor for this purpose with Your prior approval which You will not unreasonably withhold. By virtue of this Agreement, You may be exposed to certain information concerning Licensor's software products and other information not generally known to the public (including the Licensed Software and the Documentation), all of which are the confidential and proprietary information of Licensor ("Confidential Information"). You may use Confidential Information solely as necessary in order to facilitate Your use of the Licensed Software under this Agreement. You agree that during and after the term of this Agreement You will not disclose any Confidential Information without

Licensor's prior written consent to any third party and will take all necessary precautions, using in any event not less than a reasonable degree of care, to protect and keep confidential the Confidential Information. If any provision of this Agreement is held to be unenforceable, it shall be enforced to the maximum extent permissible, and the remaining provisions shall remain in full force. A waiver of any breach or default under this Agreement shall not constitute a waiver of any other subsequent breach or default. Unless You have entered into a separate, written and signed agreement with Licensor for the supply of the Licensed Software, this Agreement is the complete and exclusive statement of the agreement between us which supersedes any proposal, prior agreement, oral or written, purchase order or similar terms issued by You, or any other communications between us in relation to the subject matter of this Agreement. Any modifications to this Agreement shall be made in writing and must be duly signed by authorized representatives of both parties or they shall be void and of no effect.

## 12. Additional Uses and Restrictions:

### 12.1 Managed Backup Device:

"Device" is defined as a single computer, storage drive or other device (i) on which licensee can install and use the software, (ii) from which licensee accesses and uses the software installed on a network, or (iii) a physical connection point that links together two separate devices. A "Managed Backup Device" is defined as a Device that is managed, monitored and/or protected by the software but that may not actually be running the software itself.

### 12.2 Installation on Servers:

The Licensed Software shall be licensed for the maximum number of Managed Backup Devices managed by the Licensed Software. In the event that the Licensed Software includes components to be installed on a server computer, You may install such portions of the Licensed Software on any number of server computers so long as such installed Licensed Software is only used for the authorized maximum number of Managed Backup Devices as may be specified in the License Module.

### 12.3 Third Party Access Licenses:

In order to use any components of the Licensed Software designated as third party access license modules or options in support of licensed Managed Backup Devices (for example, IBM Tivoli Storage Manger Option, Legato Networker Option and Commvault Option etc.), You must acquire a license for each such third party modules or options at additional charges for use with VERITAS Backup Reporter



# Contents

## Technical Support

Chapter 1	Planning your Veritas Backup Reporter installation	
	About the resources required in the installation process .....	17
	About choosing Veritas Backup Reporter hosts .....	18
	About choosing a VBR Management Server host .....	18
	About choosing a VBR Agent host .....	19
	About choosing a VBR Java View Builder host .....	19
	About choosing a VBR console host .....	19
	About typical VBR Agent deployment scenarios .....	20
	Scenario 1: VBR Agent installed on the VBR Management Server host .....	20
	Scenario 2: VBR Agent installed on a remote backup application host .....	21
	Scenario 3: VBR Agents installed on remote backup application hosts .....	22
Chapter 2	Veritas Backup Reporter host and firewall requirements	
	Veritas Backup Reporter operating system requirements .....	23
	Veritas Backup Reporter system resource requirements .....	24
	Solaris system resource requirements .....	25
	Windows system resource requirements .....	25
	Veritas Backup Reporter firewall requirements .....	26
	Changing the VRTSweb HTTP port .....	28
	Veritas Backup Reporter NAT firewall considerations .....	29
	Veritas Backup Reporter setup requirements .....	30
	Veritas Backup Reporter Web Browser requirements .....	30
Chapter 3	Installing, uninstalling, and upgrading Veritas Backup Reporter	
	About installation prerequisites .....	33
	Installing Veritas Backup Reporter on the Symantec Product Authentication Service host .....	34

Installing Veritas Backup Reporter on Solaris .....	35
Finding installation/uninstallation log directory data on	
Solaris .....	39
Modifying Veritas Backup Reporter on Solaris .....	39
Uninstalling Veritas Backup Reporter on Solaris .....	40
Installing Veritas Backup Reporter on Windows .....	41
Finding installation/uninstallation log directory data on	
Windows .....	44
Resolving Agent authentication failures manually on Solaris or	
Windows .....	44
Modifying Veritas Backup Reporter on Windows .....	46
Performing a sanity check after installing Veritas Backup Reporter	
on UNIX or Windows .....	47
Uninstalling Veritas Backup Reporter on Windows .....	47
About upgrading to Veritas Backup Reporter 6.0 .....	48
Identifying version of .jar files .....	48
Upgrading Veritas Backup Reporter 4.1, or 4.2 to 6.0 .....	49
Installing the Veritas Backup Reporter demo on Windows .....	51

## Chapter 4 Starting and stopping Veritas Backup Reporter Service

Stopping and starting the VBR Server .....	53
Stopping and starting the VBR Agent .....	56

## Chapter 5 Configuring Veritas Backup Reporter Service

Configuring VBR Management Server data retention settings .....	59
Configuring VBR Agent modules .....	60
About the Veritas NetBackup module .....	61
About the Veritas Backup Exec module .....	62
About the EMC Legato Networker module .....	63
About the IBM Tivoli Storage Manager module .....	63
About the CommVault Galaxy & Backup Agent module .....	64
Configuring the SMTP Mail server .....	64
Disabling error log collection on VBR Agents .....	65
About creating and importing object views in XML .....	66

## Chapter 6 Backing up and restoring Veritas Backup Reporter data

Backing up the VBR database .....	67
Restoring the VBR database .....	68

## Appendix A Veritas Backup Reporter install packages

About Veritas Backup Reporter install packages .....	73
Veritas Backup Reporter UNIX component packages .....	74

## Index



# Planning your Veritas Backup Reporter installation

This chapter includes the following topics:

- [About the resources required in the installation process](#)
- [About choosing Veritas Backup Reporter hosts](#)
- [About typical VBR Agent deployment scenarios](#)

## About the resources required in the installation process

There are several planning steps you need to take before installing Veritas Backup Reporter. There are some typical configurations and deployment scenarios that ensure proper product functionality.

You need the following documents and resources to plan and successfully complete your installation.

- *Veritas Backup Reporter 6.0 Hardware and Software Compatibility List*  
The VBR 6.0 HSCL.pdf is shipped with the product CD and is updated regularly at:  
<http://support.veritas.com/docs/285754>.
- *Veritas Backup Reporter Release Notes*
- A license key (possibly multiple keys for different features)
- Administrator accounts and passwords for all target hosts

- A checklist of the Veritas Backup Reporter features you plan to use
- Additional backup application licenses, depending on how you choose to deploy the VBR Agent

You must also decide how you want to configure your Veritas Backup Reporter environment to best capture and report on data from supported applications, especially Veritas NetBackup and Veritas Backup Exec. Your configuration decisions depend on how you choose to deploy the VBR Agent.

See [“About typical VBR Agent deployment scenarios”](#) on page 20.

## About choosing Veritas Backup Reporter hosts

In addition to the standard system requirements for Veritas Backup Reporter, there are other factors you should consider when choosing hosts.

The following topics provide additional information for choosing hosts:

- [About choosing a VBR Management Server host](#)
- [About choosing a VBR Agent host](#)
- [About choosing a VBR Java View Builder host](#)
- [About choosing a VBR console host](#)

### About choosing a VBR Management Server host

The VBR Management Server is a Web application that acts as the central point of the product. VBR Agents modules collect data from various backup products and send it to the Management Server. The Management Server then merges the backup data received from all backup products and stores it in the Sybase ASA database server.

Use the following criteria to identify the kind of system that you need for hosting the VBR Management Server and Web Engine:

- The host should meet the system requirements described in detail in the *Veritas Backup Reporter Release Notes*.
- The host should have sufficient storage space to accommodate the historical data. We recommend that you install the database on mirrored or RAID-protected storage.
- The host must have network access to hosts that are running backup applications such as Veritas NetBackup, Veritas Backup Exec, or EMC Legato Networker.

For more information about the VBR Management Server and its architecture, see the *Veritas Backup Reporter Administrator's Guide*.

## About choosing a VBR Agent host

The VBR Agent collects high-level data from various backup applications. Veritas Backup Reporter monitors these applications locally or remotely.

Use the following general criteria to identify the kind of system you need to host the VBR Agent:

- The system should meet the system requirements described in detail in the *Veritas Backup Reporter Release Notes*.
- If the Agent is not installed on the same host as the VBR Management Server, the Agent host must be able connect to the VBR Management Server host through the 1556 and 2821 ports. The VBR Management Server host must be able to connect to the 7806 port of the Agent host.

In addition to the criteria above, your choice of a VBR Agent host depends on specific criteria related to your network environment, the backup applications that you want to monitor, and the operating systems of the backup application hosts.

For more information about the VBR Agent and its architecture, see the *Veritas Backup Reporter Administrator's Guide*.

## About choosing a VBR Java View Builder host

An administrator can create, modify, and manage access to the object views (logical group of IT assets) using Java View Builder. The views are available in the VBR console.

The kind of system you need to host the Java View Builder should meet the system requirements described in detail in the *Veritas Backup Reporter Release Notes*.

For more information about the Java View Builder and its architecture, see the *Veritas Backup Reporter Administrator's Guide*.

## About choosing a VBR console host

The VBR console is a graphical user interface that displays reports and other information for users of Veritas Backup Reporter through a standard Web browser. For the Veritas Backup Reporter users, the console is a central point to manage cost analysis and chargeback for services, displaying and managing reports.

One of the following Web browsers is required to run the console:

- Internet Explorer 6.x or later
- Mozilla Firefox 1.0 or later
- Netscape Navigator 7.x or later

Your browser must support either JScript 5.5 (provided with Microsoft Internet Explorer 6 or later) or JavaScript 1.2 (provided with Netscape Navigator 7.x). Additionally, for Internet Explorer, Secure Sockets Layer (SSL) 3.0 ActiveX scripting must be enabled.

If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the Veritas Backup Reporter Web Engines, to which you will connect. In Netscape 7.2, pop-up blocking is enabled by default.

---

**Note:** For Internet Explorer 6.0 on Windows 2003 (Server and Advanced Server), set the default Intranet zone security level to medium or lower.

---

## About typical VBR Agent deployment scenarios

Following are the typical deployment scenarios for the VBR Agent:

- [Scenario 1: VBR Agent installed on the VBR Management Server host](#)
- [Scenario 2: VBR Agent installed on a remote backup application host](#)
- [Scenario 3: VBR Agents installed on remote backup application hosts](#)

The scenario you choose depends on a number of factors, including the following:

- The type of backup application you want to monitor
- The operating system of the host running the backup application
- Your organization's policies with respect to adding software on dedicated backup application hosts
- Backup host system performance criteria

### Scenario 1: VBR Agent installed on the VBR Management Server host

You can install the VBR Agent on the VBR Management Server host. You can then configure the Agent to collect data from backup application master and media servers.

In this deployment scenario, Veritas Backup Reporter can monitor the following:

- Veritas NetBackup
- Veritas Backup Exec

- IBM Tivoli Storage Manager
- CommVault Galaxy Backup & Recovery
- EMC Legato Networker

This deployment scenario is recommended if the operating systems of the NetBackup or Tivoli Storage Manager hosts are not supported by the VBR Agent.

Advantages of installing the VBR Agent on the VBR Management Server host

- 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 could have been involved in upgrading the Agent.

Disadvantages of installing the VBR Agent on the VBR Management Server host

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

For more information about enabling, modifying, and disabling VBR Agent module configurations, see the *Veritas Backup Reporter Administrator's Guide*.

## Scenario 2: VBR Agent installed on a remote backup application host

You can install the VBR Agent on a remote system in your network that hosts a backup application. You can configure the Agent to collect data from the backup application on its own host as well as applications on other hosts within the network.

In this deployment scenario, Veritas Backup Reporter can monitor the following:

- Symantec NetBackup
- IBM Tivoli Storage Manager

This is the highly recommended deployment scenario, because it has a very low impact on the backup environment by adding only one Agent. The operating system of the backup application host must be supported by the VBR Agent.

Advantages of installing the VBR Agent on a remote backup application host

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

Disadvantages of installing the VBR Agent on a remote backup application host

- The VBR Agent may use significant system resources with possible impact to the backup application host's performance

For more information about enabling, modifying, and disabling VBR Agent module configurations, see the *Veritas Backup Reporter Administrator's Guide*.

## Scenario 3: VBR Agents installed on remote backup application hosts

You can install the VBR Agent on all remote backup hosts in your network, provided the hosts run an operating system that the Agent supports. You can then configure each Agent to collect data from the backup host on which it is installed.

In this deployment scenario, Veritas Backup Reporter can monitor the following:

- Veritas NetBackup
- Veritas Backup Exec
- IBM Tivoli Storage Manager
- EMC Legato NetWorker

For most environments, Symantec does not recommend this deployment strategy. However, for Legato NetWorker environment, it is the only supported deployment option.

Advantages of installing the VBR Agents on remote backup application hosts

- It distributes the data collection task across all backup hosts, minimizing the load on any one host.

Disadvantages of installing the VBR Agents on remote backup application hosts

- The maintenance is high while upgrading the VBR Agent.

For more information about enabling, modifying, and disabling VBR Agent module configurations, see the *Veritas Backup Reporter Administrator's Guide*.

# Veritas Backup Reporter host and firewall requirements

This chapter includes the following topics:

- [Veritas Backup Reporter operating system requirements](#)
- [Veritas Backup Reporter system resource requirements](#)
- [Veritas Backup Reporter firewall requirements](#)
- [Veritas Backup Reporter setup requirements](#)
- [Veritas Backup Reporter Web Browser requirements](#)

## Veritas Backup Reporter operating system requirements

[Table 2-1](#) provides operating system requirements for Veritas Backup Reporter hosts:

**Table 2-1** Veritas Backup Reporter Operating System Requirements

Component	Operating systems supported
VBR Management Server	<ul style="list-style-type: none"> <li>■ Solaris 8/9</li> <li>■ Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)</li> <li>■ Windows Server 2003 (Standard Edition, Enterprise Edition [32-bit only], Datacenter Edition [32-bit only], Web Edition)</li> </ul>
VBR Agent	<ul style="list-style-type: none"> <li>■ Solaris 7/8/9/10</li> <li>■ Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)</li> <li>■ Windows Server 2003 (Standard Edition, Enterprise Edition [32-bit only], Datacenter Edition [32-bit only], Web Edition)</li> </ul>
VBR console	Any platform with network access to the VBR Management Server host and a supported Web browser. The minimum required resolution for the Console is 1024 x 768.
VBR Java View Builder	<ul style="list-style-type: none"> <li>■ Solaris 8/9/10</li> <li>■ Windows 2000 SP4 or later (Server, Advanced Server, Datacenter Server)</li> <li>■ Windows Server 2003 (Standard Edition, Enterprise Edition [32-bit only], Datacenter Edition [32-bit only], Web Edition)</li> </ul>

For more information about the operating system updates required to run Veritas Backup Reporter, refer to the *Veritas Enterprise Reporter Release Notes*.

## Veritas Backup Reporter system resource requirements

You can determine the memory and disk space requirements for depending on your operating system.

The tables provide memory and disk space specifications for components.

- [Solaris system resource requirements](#)
- [Windows system resource requirements](#)

The amounts of memory and disk space are in addition to the resources already consumed by other software on the host.

---

**Warning:** Veritas Backup Reporter requires an NTFS-formatted installation directory. Installations attempted on drives formatted with FAT32 will fail.

---

## Solaris system resource requirements

[Table 2-2](#) provides system resource requirements for Solaris hosts.

**Table 2-2** System resources for Solaris hosts

Component	Memory required	Memory recommended	Disk space required
VBR Management Server	512 MB	1 GB	900 MB
VBR Agent	256 MB	512 MB	300 MB
VBR Java View Builder	256 MB	512 MB	300 MB

[Table 2-3](#) provides CPU recommendations for Solaris hosts.

**Table 2-3** CPU recommendations for Solaris hosts

Minimum CPU Required Times Speed	Recommended CPU Times Speed
2 x 1 GHz	4 x 1 GHz

## Windows system resource requirements

[Table 2-4](#) provides system resource requirements for Windows hosts.

**Table 2-4** System resources for Windows hosts

Component	Memory required	Memory recommended	Disk space required
VBR Management Server	512 MB	1 GB	900 MB
VBR Agent	256 MB	512 MB	200 MB
VBR Java View Builder	256 MB	512 MB	200 MB

[Table 2-5](#) provides CPU recommendations for Windows hosts.

**Table 2-5** CPU recommendations for Windows hosts

Minimum CPU Required Times Speed	Recommended CPU Times Speed
2 x 2.5 GHz	4 x 2.5 GHz

## Veritas Backup Reporter firewall requirements

For the VBR 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 2-6** lists the default ports Veritas Backup Reporter uses to transfer information. The illustration that immediately follows this table also shows these default port assignments.

**Table 2-6** Default ports in a Veritas Backup Reporter installation

Port	Protocol	Initiator > Recipient	Purpose	Impact if blocked
25	SMTP over TCP/IP	VBR Management Server > email server	Email reports	Users will not receive scheduled email reports if the Management Server cannot reach the email server it has been configured to use.
1885	TCP/IP	VBR Management Server > VBR Management Server	Trap sharing	None. Not used across firewall.
2821	TCP/IP	Agent, Java View Builder, CLI tools > VBR Management Server	Authentication with VBR Management Server	Users will not be able to authenticate with Symantec Private Branch Exchange and VBR Management Server; users denied access.
2994	TCP/IP	VBR Management Server > Database	Store settings	None. Not used across firewall.
2994	TCP/IP	Alert Manager > Database	Store collector data, alerts, policy settings	None. Not used across firewall.
5431	IIOP over TCP/IP	Alert Manager > VBR Management Server	Alert monitoring	None. Not used across firewall.

**Table 2-6** Default ports in a Veritas Backup Reporter installation (*continued*)

Port	Protocol	Initiator > Recipient	Purpose	Impact if blocked
1556	CORBA over SSLIOP	Agent, Java View Builder, CLI tools > VBR Management Server	All communications with VBR Management Server (through PBX)	VBR Management Server will appear to not respond to Agent, Java View Builder, and so on.
7806	CORBA over TCP/IP	VBR Management Server and CLI tools > Agent	Status and data requests for frequent updates of the Agent	Agent status page will not work, CLI tools for querying Agent will not work remotely.
8181	HTTP over TCP/IP	Web Browser > VBR Management Server	Run Veritas Enterprise Reporter Console	Users will not be able to access the console.
8443	HTTPS over TCP/IP	Web Browser > VBR Management Server	Run Veritas Enterprise Reporter Console	Users will not be able to access the console.



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

### 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 have 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 has 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 have chosen.

## Veritas Backup Reporter NAT firewall considerations

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 “natted” address) of the VBR Management Server and the Veritas Alert Manager.

**To configure the VBR Management Server behind a NAT**

- 1 On the VBR Management Server, do one of the following:
  - Solaris - Open a UNIX console, and then log in as root.
  - Windows - Open a Windows command prompt, and then log in as an administrator or user in the Administrators group.
- 2 Stop the VBR Management Server.
  - Solaris - /opt/VRTSccsvs/bin/vxccsvc stop
  - Windows - Using the Windows Service Control Manager (SCM), stop the VBR Management Server.
- 3 Using a text editor, open the vbr\_conf.properties present in the following default location:
  - Solaris - /opt/VRTSccsvs/conf
  - Windows - \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 Type the actual public IP address (the “natted” address) for the VBR 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 VBR Management Server.
  - Solaris - /opt/VRTSccsvs/bin/vxccsvc start
  - Windows - Using the Windows SCM, restart the VBR Management Server.

## Veritas Backup Reporter setup requirements

To enable users to select a domain at logon, VBR Management Server hosts running Windows must be configured either in DNS or with a fully qualified domain name.

## Veritas Backup Reporter Web Browser requirements

One of the following Web browsers is required to run the Console:

- Internet Explorer 6.x or later
- Mozilla Firefox 1.0 or later
- Netscape Navigator 7.x or later

Your browser must support JScript 5.5 (provided with Microsoft Internet Explorer 6 or later). Additionally, for Internet Explorer, Secure Sockets Layer (SSL) 3.0 ActiveX scripting must be enabled.

If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the Veritas Backup Reporter Web Engines to which you will connect.

---

**Note:** For Internet Explorer 6.0 on Windows 2003 (Server and Advanced Server), set the default Intranet zone security level to MEDIUM or lower.

---



# Installing, uninstalling, and upgrading Veritas Backup Reporter

This chapter includes the following topics:

- [About installation prerequisites](#)
- [Installing Veritas Backup Reporter on Solaris](#)
- [Modifying Veritas Backup Reporter on Solaris](#)
- [Uninstalling Veritas Backup Reporter on Solaris](#)
- [Installing Veritas Backup Reporter on Windows](#)
- [Modifying Veritas Backup Reporter on Windows](#)
- [Performing a sanity check after installing Veritas Backup Reporter on UNIX or Windows](#)
- [Uninstalling Veritas Backup Reporter on Windows](#)
- [About upgrading to Veritas Backup Reporter 6.0](#)
- [Installing the Veritas Backup Reporter demo on Windows](#)

## About installation prerequisites

Veritas Backup Reporter uses Symantec Private Branch Exchange to handle user permissions.

See the *Veritas Backup Reporter Administrator's Guide* for more information on how Veritas Backup Reporter uses Symantec Product Authentication Service.

## Installing Veritas Backup Reporter on the Symantec Product Authentication Service host

When installing Veritas Backup Reporter on a host where Symantec Product Authentication Service is already installed, you need to make sure that the authentication broker is running in the correct mode. If it is running in Root Only mode, you need to change the mode to Root + AB before you install Veritas Backup Reporter.

### To verify the mode for Symantec Private Branch Exchange on Solaris

- 1 Determine if Symantec Product Authentication Service is installed on the host by executing the command

```
grep vrtsat
```

- 2 Change your directory to the installation directory.

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

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

```
# vssregctl -l -q -b "Security\Authentication\Authentication  
Broker" -k "Mode"
```

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

Mode 0: The broker is not configured, no change required to VAS.

Mode 1: The broker is running in AB mode, no change required to VAS.

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

Mode 3: The broker is running in Root + AB mode, no change required to VAS.

### To modify the mode for Symantec Private Branch Exchange on Solaris

- 1 Stop the vxatd process.

```
vxatd stop
```

- 2 Change your directory to the installation directory.

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

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

```
vsatd -o -a -r
```

- 4 Start the vxatd process.

```
vxatd start
```

### To verify the mode for Symantec Private Branch Exchange on Windows

- 1 Determine if Symantec Product Authentication Service is installed on a Windows host by checking the Windows Services applet for the Symantec Private Branch Exchange.
- 2 At the command prompt, enter:

```
vssregctl -l -q -b "Security\Authentication\Authentication Broker"  
-k "Mode"
```

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

Mode 0: The broker is not configured, no change required to VAS.

Mode 1: The broker is running in AB mode, no change required to VAS.

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

Mode 3: The broker is running in Root + AB mode, no change required to VAS.

### To modify the mode for Symantec Private Branch Exchange on Windows

- 1 Using the Windows services applet, stop the Symantec Private Branch Exchange.
- 2 Change your directory to the installation directory.

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

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

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

- 4 Using the Windows Services applet, restart the Symantec Private Branch Exchange.

## Installing Veritas Backup Reporter on Solaris

You can install, modify, and uninstall Veritas Backup Reporter components on Solaris and Windows hosts. You can also upgrade from 4.1, and 4.2 installations to Veritas Backup Reporter 6.0.

Use the Veritas Backup Reporter Install Script, which resides at the top level of the product CD, to install Veritas Backup Reporter on a Solaris host.

The install comprises the following phases:

- Select components to install.
- Configure components in the install queue.
- Install the components.

#### To begin installing 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 6.0 product CD for the components you are installing.
- 3 Type the following command, and then 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 then press **Enter**.

The label [INSTALL] displays 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 then press **Enter**.
- 6 When you are finished adding components to the queue, type the menu number that corresponds to the Finished with selections option, and then press **Enter**.
- 7 Review the list of components in the install queue.
- 8 Type `y`, and then press **Enter** to confirm the selection and continue.
- 9 Type `n`, and then 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 then 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 VBR Management Server, do the following:

- Type a directory path under which to install the VBR Management Server's databases, and then 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 will create 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 ReporterServer
This should be a fully qualified domain name or an IP address
that other machines can use:
(installsystem) 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 then press **Enter**.

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

- 4 If you are installing the VBR Management Server, choose whether to configure the Agent to report to a VBR Management Server host at this time by doing the following:
  - Type **y**, and then press **Enter**.
  - Type the name of the VBR Management Server host, and then press **Enter**. Otherwise, type **n**, and then press **Enter**.

The host on which you are installing the 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.

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

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 then 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 installing 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 Type **y**, and then press **Enter** to start Veritas Backup Reporter processes, or type **n** and press **Enter** if you want to start the processes manually later.

The Install Script displays a summary of the installation, including the location of the installation log files.

## Finding installation/uninstallation log directory data on Solaris

The installation/uninstallation logs for Solaris can be found at the following location on the Server CD:

CD Location	Pathname
6.0 Server CD	<code>/var/tmp/installvbr&lt;number&gt;</code> <code>/var/tmp/uninstallvbr&lt;number&gt;</code>

where <number> is generated at installation or uninstallation time. The generated number is a unique number.

### To find the installation/uninstallation log directory for the VBR Management Server on Solaris

- ◆ Type the following commands to find the latest installation/uninstallation log directory for the VBR Management Server:

```
cd /var/tmp  
ls -ltrd *installvbr*
```

The latest installation/uninstallation directory logs will be at the bottom of the list. There will be multiple log files within that directory. When submitting the installation/uninstallation logs to Symantec technical support, please tar and zip all the files contained in the installation/uninstallation log directory, and send the files to the appropriate Symantec contact.

## 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 6.0 product CD for the components you want to install.

- 3 If you are installing additional Veritas Backup Reporter components, do the following:
  - Type the following command, and then press **Enter**:  

```
./installvbr
```

See “[Installing Veritas Backup Reporter on Solaris](#)” on page 35.
- 4 If you are altering the configuration of installed Veritas Backup Reporter components, do the following:
  - Type the following command, and then press **Enter**:  

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

## Uninstalling Veritas Backup Reporter on Solaris

Use the Uninstall Script, which resides at the top level of 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 then 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 then press **Enter**.  

The label [UNINSTALL] displays 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 then press **Enter**.
- 6 To remove a selected component from the uninstall queue, type the component's number again, and then press **Enter**.
- 7 When you are finished adding components to the queue, type the number that corresponds to the Finished with selections option, and then press **Enter**.
- 8 Review the list of components in the uninstall queue.

- 9 Type **y**, and then press **Enter** to confirm the selection and continue.
- 10 Type **n**, and then press **Enter** to return to the component list and revise your selection.
- 11 If you are uninstalling the VBR Management Server, do the following:
  - Choose the data files you want to back up before uninstalling the VBR Management Server.
  - To add a file type to the backup queue, type its corresponding menu number, and then press **Enter**.  
The label [BACKUP] displays 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 are finished adding files to the backup queue, type the number that corresponds to the Finished with selections option, and then press **Enter**.
  - Review the backup options you selected.
  - Type **y**, and then press **Enter** to confirm the selection and continue.
  - Type **n**, and then 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 Type **y**, and then press **Enter** to start the uninstall process, or type **n**, and press **Enter** to quit the uninstall.

## 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 6.0 product CD.

The install comprises the following phases:

- Select components to install.
- Configure components in the install queue.

- Install the components.

---

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

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

#### To install 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 6.0 product CD in the CD-ROM drive.
- 3 If autorun is enabled, the Veritas Backup Reporter Install Wizard displays, and you can skip to [To install Veritas Backup Reporter on Windows](#).
- 4 On the Start menu, click **Run**.
- 5 Type the following in the Open field, and then press **Enter**:

`<D>:\setup.exe`

where <D> is your CD-ROM drive.

- 6 In the Welcome panel of the Veritas Backup Reporter Install Wizard, click **Next** to continue the installation.
- 7 Read the license agreement, accept the terms of the agreement, and then click **Next**.
- 8 Expand the branches in the component tree to display the products and utilities available for installation.
- 9 For each component you want to install, click the drop-down list in front of the component, and then click **This feature will be installed**.  
The drive icon appears indicating that the component is in the install queue.
- 10 If you want to select a different destination folder for the installation, click **Change** and use the navigation buttons to click the destination folder you want to use.

You cannot install Veritas Backup Reporter components to the top-level directory of a Windows file system.

**11** If you want to select a different destination folder for the Management Server database files, click **Change** and use the navigation buttons to select the destination folder you want to use.

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

The next series of prompts in the Veritas Backup Reporter Install Wizard collects configuration information for the components in the install queue. The steps you need to complete may vary, depending on which components are queued for installation.

#### To configure components in the install queue

**1** If you are installing the VBR Management Server, do the following:

- Type the name of the host running the VBR Management Server in the Host field.

**2** If you are installing the VBR Agent, do the following:

- Type the name of the host running the VBR Management Server in the Host text box.

If the VBR Management Server is running on the same host where you are installing the Agent, use the default value Localhost.

- Optionally, type an alternate port for the Agent- Management Server connection in the Port field (default 1556).

**3** Type 8181, the default port for the Veritas Backup Reporter Web Engine, or the alternate port in the Port text box.

**4** Type address of the SMTP mail server.

**5** Click **Next** when you are finished configuring these options.

The next series of prompts in the Veritas Backup Reporter Install Wizard are primarily confirmation prompts to continue the installation after the Install Wizard performs its pre-installation checks.

#### To complete Veritas Backup Reporter component installation

**1** Review the installation settings.

**2** If they are correct, click **Next** to begin the installation.

The Veritas Backup Reporter Install Wizard installs the Veritas Backup Reporter components.

When you see the Install Wizard closing panel, you are finished installing Veritas Backup Reporter.

- 3 If you want to view a PDF of the *Veritas Backup Reporter Release Notes*, check the check box on the wizard's closing panel before closing the Install Wizard.

By default, the Install Wizard launches the *Veritas Backup Reporter Release Notes* in Adobe Reader.

You should read the *Veritas Backup Reporter Release Notes* to find updates that are not contained in the user documentation.

You can download a free copy of Adobe Reader at:

<http://www.adobe.com>

- 4 Click **Finish** to close the Install Wizard.
- 5 Reboot your system.

## Finding installation/uninstallation log directory data on Windows

You can locate the installation/uninstallation log for the VBR Management Server on Windows at the following location:

```
%ALLUSERSPROFILE%\Application  
Data\Symantec\VeritasBackupReporter\VxCommandCentralInstall.log
```

On most systems, the %ALLUSERSPROFILE% directory will be the following:

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

The Application Data directory is a hidden directory.

**To view the hidden Application Data directory from Windows Explorer**

- ◆ Select **Tools > Folder Options > View**, and click the option for displaying hidden files and folders.

The installation log file increases in size with each installation or uninstallation, so the installation/uninstallation logs will contain all the required log information for your system. When submitting the installation/uninstallation logs to Symantec technical support, please zip all the files contained in the installation/uninstallation log directory, and send the files to the appropriate Symantec contact.

## Resolving Agent authentication failures manually on Solaris or Windows

If the VBR Agent authentication fails for some reason on Solaris or Windows, you can use the following procedures for manually resolving Agent authentication failures.

If the VBR Agent is unable to connect to the VBR 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 VBR Management Server host with administrator-level privileges.
- 2 Stop the Agent service using the Windows Services applet (Start menu > 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>
```

- 5 Restart the Agent service.

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 the following:

- The Security Dynamic Link Libraries (DLLs) are not in the PATH.

The workaround for this is to execute 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 VBR Management Server and Authentication Service are running, and can be reached on ports 1556 and 2821 respectively.

---

**Note:** Further documentaion on the agentauth command is available in the *Veritas Backup Reporter Administrator's Guide*.

---

## 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 6.0 product CD.

### 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 6.0 product CD in the CD-ROM drive.

If autorun is enabled, the Install Wizard displays and you can skip to 5.

- 3 On the Start menu, click **Run**.
- 4 In the Open field, type the following, and then press **Enter**:

**D:\setup.exe**

where <D> is your CD-ROM drive.

- 5 In the Welcome panel of the Install Wizard, click **Next** to continue past the welcome panel.
- 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 then click **This feature will be installed** from the context menu.  
The icon next to the component will change from an X to a drive icon, indicating that the component is in the install queue.
  - See [“Installing Veritas Backup Reporter on Windows”](#) on page 41.
- 7 If you are altering the configuration of installed Veritas Backup Reporter components, do the following:
  - See [“Installing Veritas Backup Reporter on Windows”](#) on page 41.
  - Follow the prompts presented in the wizard.
- 8 Reboot your system.

## Performing a sanity check after installing Veritas Backup Reporter on UNIX or Windows

After installing Veritas Backup Reporter on either UNIX or Windows, you should perform a sanity 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 there is a Veritas Backup Reporter Login screen, the VBR Management Server, the Web server, and the Authentication Service are all running.

The first time you login it will take longer than usual 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 modules are set up correctly.

- Go to **Settings > Global Settings > Agent Configuration**.

An agent should be displayed.

If an agent is not displayed, do not click **Create**. Instead, troubleshoot the problem by checking that you have the correct ports configured.

## 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, then use the Veritas Backup Reporter 6.0 product CD (original media) to remove Veritas Backup Reporter. This will leave CommandCentral Storage installed on the host.

See the *CommandCentral Storage Installation Guide*.

**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 Suite**, and then click **Remove**.
- 4 In the Welcome panel of the Uninstall Wizard, click **Next** to continue past the welcome panel.
- 5 Review the list of components to be uninstalled.

- 6 Click **Next** to continue past the list of components panel.
- 7 Uncheck 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 will be saved.
- 9 Click **Next** to begin uninstalling Veritas Backup Reporter components.  
  
When you see the Veritas Backup Reporter Uninstall Wizard closing panel, you are finished uninstalling Veritas Backup Reporter components.
- 10 Click **Finish** to close the Veritas Backup Reporter Uninstall Wizard.

## About upgrading to Veritas Backup Reporter 6.0

Veritas Backup Reporter 6.0 supports upgrades from Veritas Backup Reporter 4.1 or 4.2.

On Solaris, the upgrade from 4.1, 4.2, to 6.0 VBR Management Server is handled automatically by the Install Script. The script also automatically upgrades 4.1 or 4.2 versions of the VBR Agent and Java View Builder.

On Windows, the upgrade of all 4.1 or 4.2 components is handled automatically by the Veritas Backup Reporter Install Wizard.

---

**Note:** Veritas Backup Reporter 6.0 does not support VBR Agents from previous releases. When you upgrade your VBR Management Server to 6.0, you must upgrade your VBR Agents to 6.0.

---

See [“Upgrading Veritas Backup Reporter 4.1, or 4.2 to 6.0”](#) on page 49.

## Identifying version of .jar files

While upgrading to Veritas Backup Reporter 6.0, 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: ccsvs-server-core - module name
- Module-Version: 6.0.16.17 - version of module deployed

## Upgrading Veritas Backup Reporter 4.1, or 4.2 to 6.0

You can upgrade Veritas Backup Reporter 4.1 or 4.2 to 6.0. On both Solaris and Windows, the upgrade of all components is handled automatically by the installation programs.

As an optional, best-practice redundancy measure, you should save your data and files in temporary (non-default) directories before you upgrade from Veritas Backup Reporter 4.1 or 4.2 to 6.0.

### Upgrading Veritas Backup Reporter 4.1 or 4.2 components to 6.0 on Solaris

On Solaris, the 6.0 Install Script detects the presence of 4.1 or 4.2 components and guides you through the upgrade to 6.0.

#### To upgrade Veritas Backup Reporter 4.1 or 4.2 components to 6.0 on Solaris

- 1 Open a UNIX console and log in as `root` on the target host.
- 2 Mount the appropriate Veritas Backup Reporter 6.0 product CD for the components you want to upgrade.
- 3 Type the following command, and then press **Enter**:

```
./installvbr
```

The Veritas Backup Reporter Install Script detects installed 4.1 or 4.2 components and prompts you to confirm your choice to upgrade.

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

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

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

- 5 You can, however, 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 to 4.1 or 4.2.

If the /var/Veritas/ccs\_save directory already exists, just 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 installed 4.1 or 4.2 components that you have selected to upgrade.

After completing the backup and uninstall, the Install Script displays a list of Veritas Backup Reporter 6.0 components available for installation.

The label [UPGRADE] displays next to any 4.1 or 4.2 component you are upgrading to indicate that the component is already in the install queue.

- 6 Type the number that corresponds to the **Finished with selections** option, and then press **Enter**.
- 7 Review the list of components in the upgrade queue.
- 8 Type **y**, and then press **Enter** to confirm the selection and continue.
- 9 Type **n**, and then press **Enter** to return to the component list and revise your selection.
- 10 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 6.0 component installation.

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

- See [“To configure components in the install queue”](#) on page 43.
- See [“To complete Veritas Backup Reporter component installation”](#) on page 43.

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

- 11 Confirm that the upgrade is successful as follows:

Solaris

- VBR Management Server: # pkginfo -l VRTSccsvs | grep VERSION
- Agent: # pkginfo -l VRTSccsva | grep VERSION
- Java View Builder: # pkginfo -l VRTSccsvb | grep VERSION

## Installing the Veritas Backup Reporter demo on Windows

You can install the Veritas Backup Reporter Demo on Windows hosts. The demo populates the Veritas Backup Reporter database with rich sample data containing instances of many types of discovered devices and applications. It thus enables you to view an example of a fully installed Veritas Backup Reporter environment in which you can test product functionality and generate reports.

---

**Note:** You can install the demo after you install the full product. During the Veritas Backup Reporter Demo install, your current Veritas Backup Reporter environment is saved. This enables you to return your install to its pre-demo configuration. If you installed Veritas Backup Reporter to the default location, your pre-demo configuration is saved to: \Program Files\Symantec\Veritas Backup Reporter\DB\Data.

---

### To install the Veritas Backup Reporter Demo on Windows

- 1 Log on to the VBR Management Service host as a user with administrator privileges.
- 2 Insert the appropriate Veritas Backup Reporter 6.0 product CD in the CD-ROM drive.
- 3 Browse the CD and copy the VBRDemo directory and VBRDemo.vbs and VBRProduction.vbs files to the host's hard drive.

This host may or may not be the same host as the CommandCentral Storage Web Engine host.

The VBRDemo.vbs and VBRProduction.vbs files must reside at the same directory level as the VBRDemo directory.

- 4 At the Windows command prompt, change to the directory where you copied the directory and files, and run the Veritas Backup Reporter Demo script, using one of the following methods:

Non-interactive mode At a command prompt, run `cscript ccdemo.vbs`.  
All script messages display within the command window.  
(Recommended)

Interactive (GUI) mode At a command prompt, run `ccdemo.vbs`.  
In this mode, you will have to acknowledge the prompts that display.

The Veritas Backup Reporter Demo is now running.

- 5 If you want to view backup reports that provide data for a specific time frame (for example, last 24 hours or last week), do the following:

- At the Windows command prompt, change to the VBR Management Server utilities directory:

```
cd \Program Files\Symantec\Veritas Backup Reporter\Server\util
```

- Run `SampleDBUpdate.bat`.

You should run this file well enough in advance of a demo so that your reports will contain data for the specified periods on which you want to report.

#### To return your Veritas Backup Reporter installation to its pre-demo state on Windows

- 1 Log on to the VBR Management Server host as a user with administrator privileges.
- 2 Run the script to return your environment to production (pre-demo) mode, using one of the following methods:

Non-interactive mode At a command prompt, run `cscript vbrProduction.vbs`.  
All script messages display within the command window.

Interactive (GUI) mode At a command prompt, run `vbrProduction.vbs`.  
In this mode, you will have to acknowledge the prompts that display.

Your Veritas Backup Reporter installation returns to the state it was in prior to running the Veritas Backup Reporter Demo.

# Starting and stopping Veritas Backup Reporter Service

This chapter includes the following topics:

- [Stopping and starting the VBR Server](#)
- [Stopping and starting the VBR Agent](#)

## Stopping and starting the VBR Server

By default, the VBR Management Server starts whenever you boot your VBR Management Server host. You can, however, manually stop and restart the VBR Management Server.

### To stop and (re)start the VBR Management Server on Solaris

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

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

For example:

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

Veritas Backup Reporter (VBR) 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 VBR Management Server by typing the following command:

```
./vxccsvc stop force
```

The `vxccsvc stop force` command stops the VBR Management Server and its shared components, such as Symantec Product Authentication Service, VBR database, Alert Manager, and Licensing.

- 5 To stop the VBR Management Server but not components that are shared among products, use the `vxccsvc stop` command.

After stopping the VBR 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 VBR Management Server may need upon restart.

This command neither starts nor stops the VBR Agent.

- 6 (Re)start the VBR Management Server from the same directory by typing the following command:

```
./vxccsvc start
```

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

By default, the VBR Management Server starts whenever you boot its host.

The command `vxccsvc` starts the VBR Management Server, its services, and the VBR database and loads data in the database.

**To stop and (re)start the VBR Management Server on Windows**

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

```
Adaptive Server Anywhere (Sybase ASA)
Symantec Private Branch Exchange
Symantec Product Authentication Service
Veritas Alert Manager
Veritas Automation Server
Symantec Web Server
Veritas Common Login Service
Veritas Backup Reporter Management Server
Veritas Backup Reporter Agent
```

After stopping the VBR 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 VBR Management Server may need upon restart.

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

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

- 4 (Re)start the following VERITAS services in the order listed by right-clicking the service, and then clicking **Start**.

```
Veritas Backup Reporter Management Server
Veritas Backup Reporter Common Login Service
Symantec Web Server
VERITAS Automation Server
VERITAS Alert Manager
Symantec Product Authentication Service
Symantec Private Branch Exchange
Adaptive Server Anywhere (Sybase ASA)
```

- 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 Service Control Manager.

## Stopping and starting the VBR Agent

By default, the VBR Agent starts whenever you boot your Agent host.

If you need to stop or start the Agent on Solaris, you can use the startup and shutdown script, `vxccsvcagent`.

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

### To stop and (re)start 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:

```
./vxccsvcagent 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 (Re)start the Agent from the same directory by typing the following command:

```
./vxccsvcagent start
```

**To stop and (re)start the Veritas Backup Reporter Agent on Windows**

- 1** Log on to the Windows 2000 Agent host as an administrator or a user in the Administrators group.
- 2** Using the Windows Service Control Manager (SCM), stop the VBR Agent service.
- 3** Right-click the service, and then 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** (Re)start the VBR Agent service.
- 5** Right-click the service, and then click **Start**.
- 6** Close the Windows Service Control Manager.



# Configuring Veritas Backup Reporter Service

This chapter includes the following topics:

- [Configuring VBR Management Server data retention settings](#)
- [Configuring VBR Agent modules](#)
- [Configuring the SMTP Mail server](#)
- [Disabling error log collection on VBR Agents](#)
- [About creating and importing object views in XML](#)

## Configuring VBR Management Server data retention settings

Before you install and run the VBR Agent on any backup servers, you should configure data retention settings on the VBR Management Server. When the Agent discovers the backup server logs for the first time, it collects a large amount of historical data, which it then passes to the VBR Management Server.

However, the VBR Management Server will immediately clean out all data older than the default period for data retention. In the case of backup log data, the default retention period is short (3 days). To accommodate a larger amount of historical data from the Agent's initial discovery, you must change the default data retention settings before running the Agent.

### To configure data retention settings for the VBR Management Server

- 1 Connect to the VBR Management Server with administrator-level privileges.  
For instructions on how to start the console and connect to the VBR Management Server, see the *Veritas Backup Reporter User's Guide*.
- 2 In the console navigation bar, click **Settings > Global Settings**.
- 3 In the console's Administration page, click **Data Retention**.
- 4 In the Data Retention dialog box, edit the value in the Backup Log Data field and any other fields you want to modify.
- 5 Click **Save**.  
You are finished configuring data retention settings for the VBR Management Server.

## Configuring VBR Agent modules

To configure the discovery modules on an Agent host, use the Veritas Backup Reporter console.

The following sections describe variable values you must define for Agent modules:

- [About the Veritas NetBackup module](#)
- [About the Veritas Backup Exec module](#)
- [About the EMC Legato Networker module](#)
- [About the IBM Tivoli Storage Manager module](#)
- [About the CommVault Galaxy & Backup Agent module](#)

### To configure VBR Agent modules

- 1 Connect to the VBR Management Server with administrator-level privileges.  
For instructions on how to start the console and connect to the VBR Management Server, see the *Veritas Backup Reporter User's Guide*.
- 2 In the console navigation bar, click **Settings > Global Settings**.
- 3 In the console's Administration page, click **Agent Configuration**.  
A table of VBR Agent hosts displays.
- 4 Select the Agent whose discovery modules you want to configure.
- 5 In the Agent Configuration panel, use the options on the Agent Configuration panel to delete (disable) existing discovery modules, add (enable) new ones, or modify a module's variable settings.

## About the Veritas NetBackup module

[Table 5-1](#) describes the required variables for the Veritas NetBackup module.

**Table 5-1** Veritas NetBackup module required variables

Module variable	Description
homeDirectory	The absolute home directory for the Veritas NetBackup installation.
volumeManagerHome	The absolute home directory for the VERITAS Volume Manager installation.
collectionMethod	Specifies the collection method that the module uses. The valid value is: <code>cli</code> . The <code>cli</code> method uses the <code>CLIbpdbjobs</code> to gather job data.
breakUpJobs	Breaks up a job (using data from NBU's catalog) so that the size and backup file count can have finer granularity. Enabling this option greatly increases the load on the 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 NBU.

**Table 5-1** Veritas NetBackup module required variables (*continued*)

Module variable	Description
daysPerImageFetch	<p>Determines the number of calls to bpimagelist. bpimagelist is used to collect image data. Each round of collection data load may trigger multiple calls to bpimagelist. daysPerImageFetch limits the amount of collection data used by bpimagelist. For example, if you are going to load image data from three months ago to today, and you set the daysPerImageFetch variable to 30 days, then bpimagelist is called three times with different time options:</p> <ul style="list-style-type: none"> <li>■ 3 months ago to 2 months ago</li> <li>■ 2 months ago to 1 month ago</li> <li>■ 1 month ago to today</li> </ul> <p>A default value of five years (1800 days) will be sufficient for most users, but users with larger environments where bpimagelist does not successfully return the default, can have this value set lower.</p> <p>The drop down will consist of the following values:</p> <ul style="list-style-type: none"> <li>■ 1800 days (default)</li> <li>■ 360 days</li> <li>■ 180 days</li> <li>■ 90 days</li> <li>■ 30 days</li> <li>■ 7 days</li> </ul>
role	<p>Informs the module how to collect media data.</p> <p>If the host is both a master server and a media server, then use <i>Master</i>.</p>

## About the Veritas Backup Exec module

The following variable is required for the Veritas Backup Exec module:

Module variable	Description
homeDirectory	The absolute home directory for the Veritas Backup Exec installation.
password	The password required to connect to database.
userName	The user name required to connect to database.
version	The version of Veritas Backup Exec.

## About the EMC Legato Networker module

[Table 5-2](#) describes the required variables for the EMC Legato Networker module.

**Table 5-2** EMC Legato Networker module required variables

Module variable	Description
homeDirectory	The absolute home directory for the EMC Legato Networker installation.
messagesFile	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 module, it is recommended that you configure Networker to create a log that contains only 'group complete messages', and point <code>messagesFile</code> to this log.
mminfoBinary	The directory path of the <code>mminfo</code> Command-Line Interface (CLI), absolute or relative to <code>homeDirectory</code> .
mminfoFile	(Optional) Output of <code>mminfo</code> .
nsrAdminBinary	The directory path of the <code>nsradmin</code> CLI, absolute or relative to <code>homeDirectory</code> .
nsrFile	(Optional) Output of an <code>nsradmin</code> command.  The VBR 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.
nsrResFile	(Optional) Networker resource file to use instead of the default that <code>nsradmin</code> uses.

## About the IBM Tivoli Storage Manager module

[Table 5-3](#) describes the required variables for the Tivoli Storage Manager module.

**Table 5-3** IBM Tivoli Storage Manager Module Required Variables

Module variable	Description
dsmConfig	The path to the <code>dsm.opt</code> file.
dsmDir	The path where files necessary to run <code>dsmadm</code> reside.
dsmadmLoc	The path of TSM administrative client ( <code>dsmadm</code> ).

**Table 5-3** IBM Tivoli Storage Manager Module Required Variables (*continued*)

Module variable	Description
homeDirectory	The absolute home directory for the Tivoli Storage Manager installation. (This variable can be left blank.)
tcpPort	(Windows only) The TCP port on the TSM server through which the module establishes a connection.  tcpPort has no effect on Solaris. The Solaris module uses the product host settings only.
tsmId	An administrator-level login used to connect to the Tivoli Storage Manager server. (The default is admin.)
tsmPassword	The password for the account (specified in tsmId) for connecting to the TSM server. (The default is admin.)

## About the CommVault Galaxy & Backup Agent module

[Table 5-4](#) describes the required variables for the CommVault Galaxy & Backup Agent module.

**Table 5-4** CommVault Galaxy & Backup Agent module required variables

Module variable	Description
password	The password required to connect to database.
port	The optional port required for database connection.
username	The username required to connect to database.

## Configuring the SMTP Mail server

You may need to change the SMTP Mail server you specified when installing Veritas Backup Reporter Service. The following procedures describe how to configure SMTP Mail on Solaris and Windows platforms.

### To configure SMTP Mail on Solaris

- 1 Open a Solaris console and log on to the VBR Management Server host as **root**.
- 2 In the console, change to the /bin subdirectory in the Symantec Web Server installation directory.

By default, the installation directory is: /opt/VRTSweb

For example:

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

- 3 Type the following command, and then press **Enter**.

```
./webgui smtp setserver <serverName>
```

where <serverName> is the IP address or fully qualified DNS name of the SMTP Mail server host.

- 4 Stop and restart the VBR Management Server.

You have finished configuring SMTP Mail on your Solaris system.

### To configure SMTP Mail on Windows

- 1 Log on to the VBR Management Server host as a user with Administrator privileges.
- 2 Open a command prompt and change to the /bin subdirectory in the Symantec Web Server installation directory.

By default, the installation directory is: C:\Program Files\VERITAS\VRTSweb

For example:

```
cd C:\Program Files\VERITAS\VRTSweb\bin
```

- 3 Type the following command, and then press **Enter**.

```
webgui smtp setserver serverName
```

where <serverName> is the IP address or fully qualified DNS name of the SMTP Mail server host.

- 4 Stop and restart the VBR Management Server.

You have finished configuring SMTP Mail on your Windows system.

## Disabling error log collection on VBR Agents

The error logs a VBR Agent collects can consume a large amount of storage space. If you are not interested in collecting these error logs, you can disable them using the console.

### To disable VBR Agent error log collection

- 1 In the navigation bar of the Veritas Backup Reporter console, click **Settings > Global Settings**.
- 2 In the console's Administration page, click **Agent Configuration**.
- 3 Select the Agent for which you want to disable error log collection.
- 4 In the Agent Log Configuration panel, click **Off** from the drop-down list in the Level field.
- 5 Click **Save**.

You have disabled error log collection for the VBR Agent.

## About creating and importing object views in XML

You can use the console to create Object Views on the VBR Management Server, but some users may find it faster or more convenient to create XML files that describe the Views they want to create, and then import the XML into Veritas Backup Reporter Service.

Veritas Backup Reporter provides an XML utility to import and export your XML files. This utility resides in the following locations on the VBR Management Server host:

- `<serverInstallDir>/bin/xml.sh` (on Solaris)
- `<serverInstallDir>\util\xml.bat` (on Windows)

Run the utility with no arguments to view a command-usage summary.

For detailed information on creating valid XML files that you can import into Veritas Backup Reporter Service, refer to the *Veritas Backup Reporter Administrator's Guide*.

# Backing up and restoring Veritas Backup Reporter data

This chapter includes the following topics:

- [Backing up the VBR database](#)
- [Restoring the VBR database](#)

## Backing up the VBR database

Veritas Backup Reporter (VBR) ships with a database backup script that performs hot backups without interrupting database operations. On both platforms, the script first deletes any existing db files (vxcc.db, vxdbbulk.db, and vxcc.log) before backing up or restoring, and only backs up or restores vxcc.log if it exists.

### To back up the VBR database

**1** Do one of the following:

Solaris                      Log on as `root`

Windows                    Log on as an administrator or user in the Administrators group.

**2** Open a Solaris console or a Windows command prompt.

**3** Run the backup script appropriate for your platform, specifying a backup directory.

For example:

Solaris                      `/opt/VRTSccsvs/bin/dbbackup /my_db_backup_dir`

Windows                    `"C:\Program  
Files\VERITAS\VxDBMS\Server\Win32\ccDbBackup.bat"  
C:\MyDbBackupFolder`

The backup script creates `ccsvc.db` and `vxdbbulk.db` in the backup directory you specified.

## Restoring the VBR database

After you back up the VBR database, you can restore it. On both Solaris and Windows platforms, the script first deletes any existing database (.db) files (`vxcc.db`, `vxdbbulk.db`, and `vxcc.log`) before backing up or restoring, and only backs up or restores `vxcc.log` if it exists.

### To restore a backed up VBR database

- 1 On the VBR Management Server whose data you want to restore, open a Solaris console or a Windows command prompt and log in as `root` (Solaris) or as an administrator or user in the Administrators' group (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 might be different 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/vxccsvc 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:

```
cd <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/VRTScsvs/bin/dbbackup <backupDir> -restore <restoreDir>

Windows         Type the following command and press **Enter**.  
                  \Program  
                  Files\VERITAS\VxDBMS\Server\Win32\ccDbBackup.bat  
                  <backupDir> -restore <restoreDir>

where <backupDir> is the directory where the backed up database resides,  
and <restoreDir> is the location of the current VBR database.

<restoreDir> is optional.

If not used, `vxcc_db_backup` and `ccDbBackup.bat` restores to the default  
database directory:

Solaris           /var/VERITAS/ccs\_data

Windows         \Program Files\Symantec\Veritas Backup Reporter\DB\Data

If you specified a non-default directory location, you will need to 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 If you want to continue with the restore, type **y**  
`vx_ccdb_backup` and `ccDbBackup.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 then press **Enter**.  
`/opt/VRTS/bin/vxccsvc`

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:

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



# Veritas Backup Reporter install packages

This appendix includes the following topics:

- [About Veritas Backup Reporter install packages](#)
- [Veritas Backup Reporter UNIX component packages](#)

## About Veritas Backup Reporter install packages

[Table A-1](#) and [Table A-2](#) lists the directories containing Veritas Backup Reporter install packages.

**Table A-1** Veritas Backup Reporter install packages for Solaris (Solaris Server CD—pkgs)

Install package	Description
VRTSbrsh	Installable package of VERITAS Shared Utilities
VRTSvlic.tar.gz	Compressed package of VERITAS License Utilities
VRTSdbms3.tar.gz	Compressed package of VERITAS Database Management Server
VRTSbram.tar.gz	Compressed package of VERITAS Alert Manager
VRTScddb.tar.gz	Compressed package of Veritas Backup Reporter database
VRTSicsco.tar.gz	Compressed package of VERITAS Infrastructure Core Services Common
VRTSspbx.tar.gz	Compressed package of Symantec Private Branch Exchange
VRTSat.tar.gz	Compressed package of Symantec Product Authentication Service

**Table A-1** Veritas Backup Reporter install packages for Solaris (Solaris Server CD—pkgs) (continued)

Install package	Description
VRTSjre15.tar.gz	Compressed package of VERITAS Java Runtime Environment Redistribution
VRTSweb.tar.gz	Compressed package of VERITAS Java Web Server
VRTSccsvs.tar.gz	Compressed package of VBR Management Server
VRTSccdc.tar.gz	Compressed package of VBR documentation
VRTSccsva.tar.gz	Compressed package of VBR Agent
VRTSbrdc.tar.gz	Compressed package of VBR Java View Builder

**Table A-2** Veritas Backup Reporter install packages for Windows (Windows Server CD)

Install package	Description
setup.exe	Install utility for Veritas Backup Reporter components
Veritas Backup Reporter Agent.msi	Installable package of the VBR Agent.
Veritas Backup Reporter View Builder.msi	Installable package of the VBR Java View Builder.

## Veritas Backup Reporter UNIX component packages

Different packages install with each of the following Veritas Backup Reporter components on Solaris computers:

- [Table A-3](#)
- [Table A-4](#)
- [Table A-5](#)

**Table A-3** UNIX packages installed with VBR Management Server

Package installed	Description	Relocatable
VRTSbrsh	VERITAS Shared Utilities	Yes

**Table A-3** UNIX packages installed with VBR Management Server *(continued)*

Package installed	Description	Relocatable
VRTSvlic	VERITAS License Utilities	No
VRTSdbms3	VERITAS Database Management Server	No
VRTSbram	VERITAS Alert Manager	Yes
VRTSccdb	Veritas Backup Reporter database	Yes
VRTSat	Symantec Product Authentication Service	No
VRTSjre15	VERITAS Java Runtime Environment Redistribution	Yes
VRTSweb	VERITAS Java Web Server	No
VRTSccsvs	VBR Management Server	Yes
VRTSbrdc	Veritas Backup Reporter documentation	Yes
VRTSspb	Symantec Private Branch Exchange	No
VRTSicsco	VERITAS Infrastructure Core Services Common	No

**Table A-4** UNIX packages installed with VBR Agent

Package installed	Description	Relocatable
VRTSbrsh	VERITAS Shared Utilities	Yes
VRTSat	Symantec Product Authentication Service	No
VRTSjre15	VERITAS Java Runtime Environment Redistribution	Yes
VRTSccsva	VBR Agent	Yes

**Table A-5** UNIX packages installed with VBR Java View Builder

Package installed	Description	Relocatable
VRTSat	Symantec Product Authentication Service	No
VRTSjre15	VERITAS Java Runtime Environment Redistribution	Yes
VRTSccsvb	VBR Java View Builder	Yes

**Table A-5** UNIX packages installed with VBR Java View Builder *(continued)*

<b>Package installed</b>	<b>Description</b>	<b>Relocatable</b>
VRTSbrsh	VERITAS Shared Utilities	Yes

# Index

## A

- Agent. *See* VBR Agent
  - resolving authentication failures manually 44
- arrays. *See* storage arrays
- authentication failures
  - resolving manually 44

## B

- backing up
  - VBR database 67
- browser requirements 30

## C

- communication protocols 26
- configuration
  - Veritas Backup Reporter
    - typical 20
- configuring 23
  - See also* interoperability
  - SMTP Mail server 64
- CORBA 26

## D

- data
  - configuring retention 59
- demo. *See* Veritas Backup Reporter Demo 51
- disabling
  - error log collection 65
  - VBR Agent modules 60
- discovery 23
  - See also* interoperability
  - configuring VBR Agent modules 60
- disk space requirements
  - Veritas Backup Reporter 24

## E

- enabling
  - VBR Agent modules 60
- error log
  - disabling collection 65

## F

- firewalls
  - ports 26
  - Veritas Backup Reporter requirements 26

## H

- hosts
  - interoperability 23
    - See also* hosts
- HTTP 26
- HTTPS 26

## I

- installation prerequisites 33
- installation/uninstallation log directory data
  - Solaris 39
  - Windows 44
- installing
  - packages 73
  - Veritas Backup Reporter
    - Solaris 35
    - Windows 41
  - Veritas Backup Reporter Demo 51
- installing Veritas Backup Reporter
  - where Symantec Product Authentication Service is already installed on host 34
- installvbr 35
- interoperability
  - hosts 23

## M

- management. . *See* interoperability
- memory requirements
  - Veritas Backup Reporter 24
- modifying
  - Veritas Backup Reporter
    - Solaris 39
    - Windows 46
- monitoring. *See* interoperability

**O**

operating system requirements  
 Veritas Backup Reporter 23

**P**

physical connections. *See* interoperability  
 ports

1556 26  
 1885 26  
 25 26  
 2821 26  
 2993 26  
 5431 26  
 60389 26  
 7806 26  
 8181 26  
 8443 26  
 8453 26

changing VRTSweb HTTP port 28  
 firewalls 26

protocols

communication 26

**R**

requirements

disk space  
 Veritas Backup Reporter 24  
 firewalls  
 Veritas Backup Reporter 26  
 memory  
 Veritas Backup Reporter 24  
 operating system  
 Veritas Backup Reporter 23  
 setup  
 Veritas Backup Reporter 30  
 Web browser 30

restoring

VBR database  
 Solaris 68  
 Windows 68

**S**

sanity check after installing  
 Veritas Backup Reporter 47

scripts

installvbr 35  
 vxccsvc 53  
 vxccsvcagent 56

setup requirements

Veritas Backup Reporter 30

SMTP 26

SMTP Mail server

configuring 64

Solaris

finding installation/uninstallation log directory  
 data 39

installing

Veritas Backup Reporter 35

modifying

Veritas Backup Reporter 39

VBR Agent

starting 56

stopping 56

VBR Management Server

starting 53

stopping 53

space requirements

Veritas Backup Reporter 24

starting

VBR Agent

Solaris 56

Windows 57

VBR Management Server

Solaris 53

Windows 55

Veritas Backup Reporter services 55–56

stopping

VBR Agent

Solaris 56

Windows 57

VBR Management Server

Solaris 53

Windows 55

Veritas Backup Reporter services 55–56

Symantec Private Branch Exchange 33

**T**

TCP/IP 26

**U**

UDP 26

uninstalling

Veritas Backup Reporter

Solaris 40

Veritas Backup Reporter on Windows 47

- upgrading
  - VBR Agent
    - Solaris 49
  - VBR Management Server
    - Solaris 49
  - Veritas Backup Reporter 48–49
  - View Builder
    - Solaris 49

**V**

- VBR Agent
  - discovery modules
    - enabling and disabling 60
  - Solaris
    - starting 56
    - stopping 56
    - upgrading 49
  - startup script 56
  - Windows
    - starting 57
    - stopping 57
- VBR database
  - backing up 67
  - restoring
    - Solaris 68
    - Windows 68
- VBR Management Server
  - ports 26
  - Solaris
    - starting 53
    - stopping 53
    - upgrading 49
  - Windows
    - stopping 55
- Veritas Backup Reporter
  - firewall requirements 26
  - installing
    - Solaris 35
    - Windows 41
  - modifying
    - Solaris 39
    - Windows 46
  - performing a sanity check after installing 47
  - requirements
    - disk space 24
    - memory 24
    - operating system 23
    - setup 30
  - starting services 55–56

- Veritas Backup Reporter *(continued)*
  - stopping services 55–56
  - uninstalling
    - Solaris 40
    - Windows 47
  - upgrading 48–49
- Veritas Backup Reporter Demo
  - installing 51
- View Builder
  - Solaris
    - upgrading 49
- VRTScستا
  - install package 73
- VRTScsts
  - install package 73
- VRTSob
  - install package 73
- VRTSweb HTTP port
  - changing 28
- vxccsvc 53
- vxccsvcagent 56

**W**

- Web browser
  - requirements 30
- Windows
  - finding installation/uninstallation log directory
    - data 44
  - installing
    - Veritas Backup Reporter 41
    - Veritas Backup Reporter Demo 51
  - modifying
    - Veritas Backup Reporter 46
  - uninstalling
    - Veritas Backup Reporter 47
  - VBR Agent
    - starting 57
    - stopping 57
  - VBR Management Server
    - starting 55
    - stopping 55