Veritas Backup Reporter Administrator's Guide

Veritas Backup Reporter Administrator's Guide

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

Documentation version 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/. 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

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

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

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

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
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: 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

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

Index

Chapter 1

Understanding Veritas Backup Reporter architecture

This chapter includes the following topics:

About the Veritas Backup Reporter Management Server

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

The VBR Management Server comprises the following components:

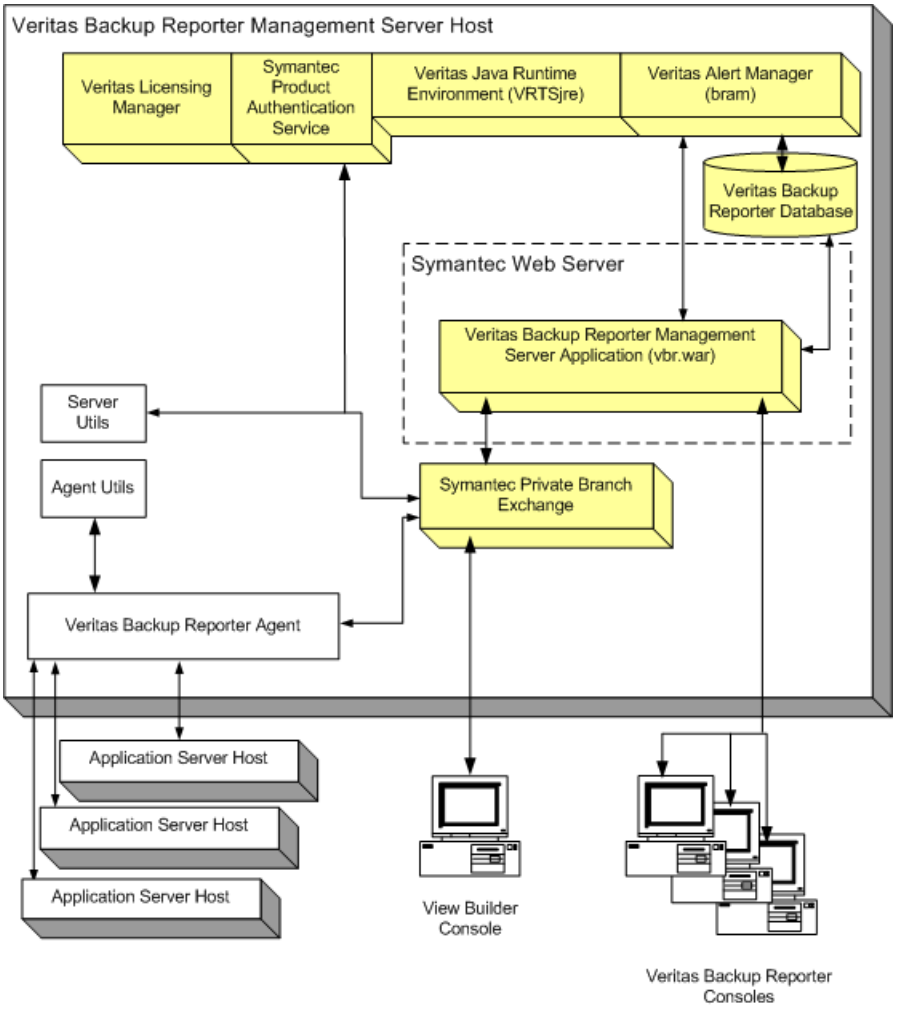
VBR database

A Sybase ASA (Adaptive Server Anywhere) database management system containing data related to backup service usage and expenditure, cost metrics and chargeback formulas, and alerts.

See "About the Veritas Backup Reporter database " on page 19.

Symantec Product Authentication Service	A set of common authentication runtime libraries and processes that enable users to log on once to access multiple products; also validates identities based on NT, NIS, or private domains. See "About the Symantec Product Authentication Service " on page 20.
Veritas Alert Manager	Component that provides policy-based alert management, including notification, custom actions, and SNMP management capabilities.
Symantec Web Server and Java Runtime Environment (JRE)	A common Web server (that uses Java Server Pages) and a JRE to serve the VBR console.
Veritas Licensing Manager	A common Veritas licensing module and API used to add, change, and remove Veritas product license keys. See " Adding license keys" on page 35.
Symantec Private Branch Exchange	A common component that uses socket passing to reduce the number of ports required to be open across a firewall. Symantec Private Branch Exchange uses a paradigm similar to that of a telephone switchboard in which calls placed to a switchboard are redirected to a known extension. In the PBX exchange, client connections that are sent to the exchange's port are redirected to an extension associated with the VBR Management Server.

Figure 1-1 VBR Management Server: Architecture



About the Veritas Backup Reporter database

VBR receives data from two primary sources:

- VBR Agents
- VBR database

The VBR Agents gather information from discoverable backup applications residing on remote host systems, such as Veritas NetBackup, Veritas BackupExec, CommVault Galaxy Backup & Recovery, and EMC Legato Networker.

See "About the Veritas Backup Reporter Agent " on page 21.

The VBR database is a rich repository of information about your data storage network. This Sybase ASA (Adaptive Server Anywhere) database management system contains service usage and expenditure reports, cost metrics, chargeback formulas, and alerts.

See "Managing VBR database activities" on page 48.

About the Symantec Product Authentication Service

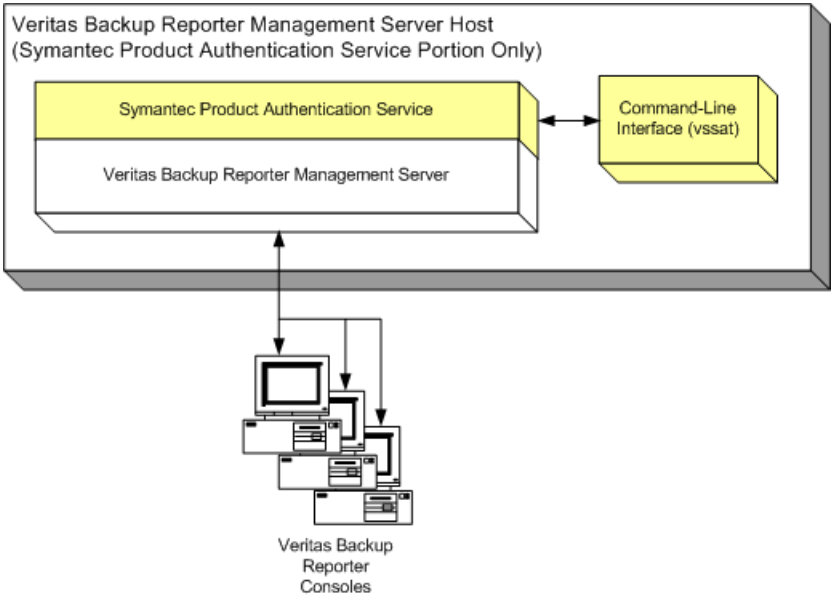
The Symantec Product Authentication Service validates identities based on NT, NIS, or private domains.

For port usage information, see the *Veritas Backup Reporter Installation Guide*.

The VBR Management Server relies on Symantec Product Authentication Service for user authentication for client connections (such as the VBR Agent and the VBR View Builder).

When the Symantec Product Authentication Service library authenticates a user for VBR, it returns a Web credential that VBR passes along when cross-linking to other products such as CommandCentral Storage. The Web credential provides a limited form of user authentication so that products do not prompt the user to log in again.

Figure 1-2 Symantec Product Authentication Service: Architecture



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

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

VBR also uses several other private domains, for various Managemnet Server and Agent components to communicate. These are accounts that don't correspond to physical users but to processes and daemons. These domains are used internally by each product for interaction between its processes and Symantec Product Authentication Service.

To get a list of private domains known to the Symantec Product Authentication Service

- Type this command (depending on your operating system) on a VBR Management Server:

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

To find more information about vssat, the Symantec Product Authentication Service command-line interface

- Type the following from the command line:

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

  or

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

About the Veritas Backup Reporter Agent

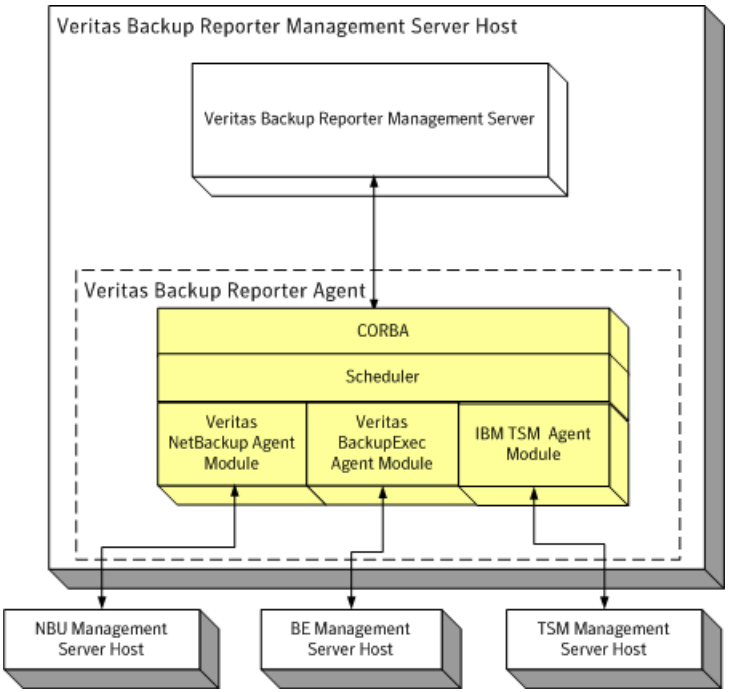
The VBR Agent collects data from various Veritas and third-party backup applications. The backup applications can reside on the VBR Agent host or on remote hosts. The VBR Agent relies on the JRE to perform its functions.

VBR formats the information collected from the following backup applications and displays it through the VBR console:

- Veritas NetBackup
- Veritas BackupExec (Windows only)

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

Figure 1-3 VBR Agent:Architecture

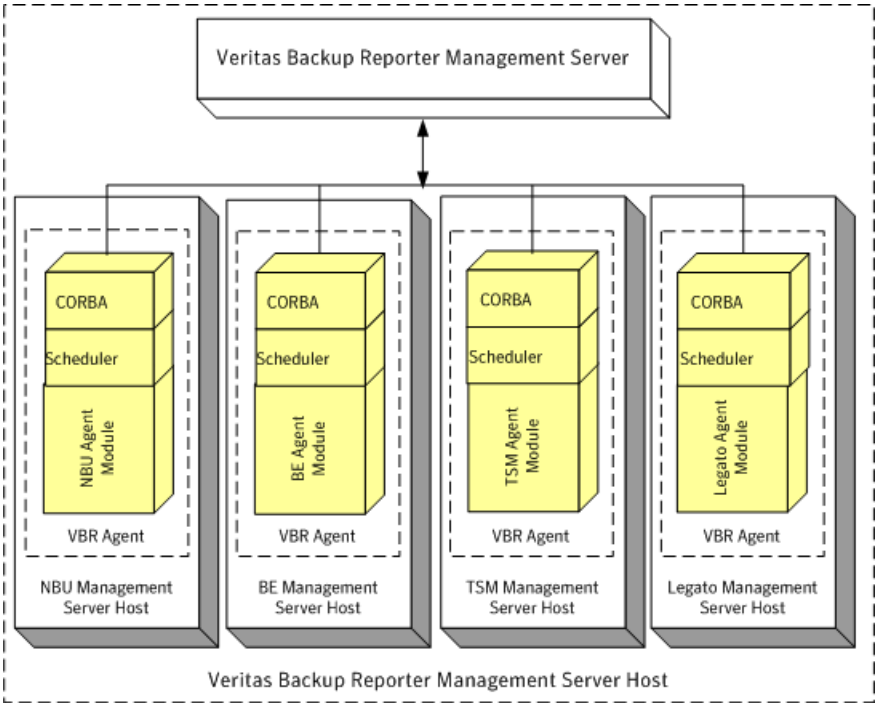


The VBR Agent can reside on the same host as the VBR Management Server, or can be installed on a remote host. All VBR Agent modules are installed on every Agent. Configure and run only those modules for the applications that you want to monitor.

Numerous combinations of VBR Agent and Management Server installations are possible. For example, you can install an Agent on the Management Server host and configure the NetBackup Agent module to collect data from a remote NetBackup master server. Altrenatively, you can install an Agent on the NetBackup master server host and configure the NetBackup Agent module to collect data from the local NetBackup master server.

Note: Legato Agent module does not support remote data collection. Therefore, the Agent must be installed on the Legato server host.

Figure 1-4 VBR Agent: Alternate installation



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

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

The VBR Agent constitutes of Scheduler, CORBA Client/Server, and Agent modules that collect backup data from all available backup applicatons. The Scheduler and CORBA form the Agent core. These parts of the Agent are described as follows:

- About the Scheduler
- About the CORBA Client/Server
- About Agent modules

About the Scheduler

The Scheduler performs three basic functions for the VBR Agent:

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

About the CORBA Client/Server

The VBR Agent implements a CORBA server that allows a backup client (such as a VBR CLI) to get the runtime status of the Agent and have limited control over Agent activity. The CORBA server tells an Agent module to collect a type of data, and that type of data is returned from the Agent module. The connection to the Agent is stateless.

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

About Agent modules

The Agent modules convert the data specific to backup products into a format that can be used by the VBR Management Server. Each module must conform to an interface that defines its interaction with the Agent. Other than those limitations, the agent module is implemented in a way that suits the underlying product.

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

Agent modules must implement an interface that has methods so that the Agent can control what the module is doing. There are methods that correspond to each data collection event type. The data that is returned by the modules must conform to the proper interface for the specific type of data so that the Agent and the VBR Management Server can properly transmit and store the data, respectively.

See "About configuring VBR Agent" on page 57.

About Agent configuration and logging

An Agent's configuration is stored in the VBR database and the Agent caches the most recent version of its configuration locally in `agent.conf`. The Agent compares `agent.conf` with the one stored in the database only when the Agent process is started. So if the Agent process is already started, and a user manually edits the

local `agent.conf`, the changes will not go into effect until the agent is restarted. However, if the changes to the configuration are done using the VBR console, the Agent will know about the change and take appropriate action.

Logging for the Agent core and individual Agent module is administered in the same fashion but written to different log files.

See vxccsvcagent on page 127.

About the Veritas Backup Reporter console

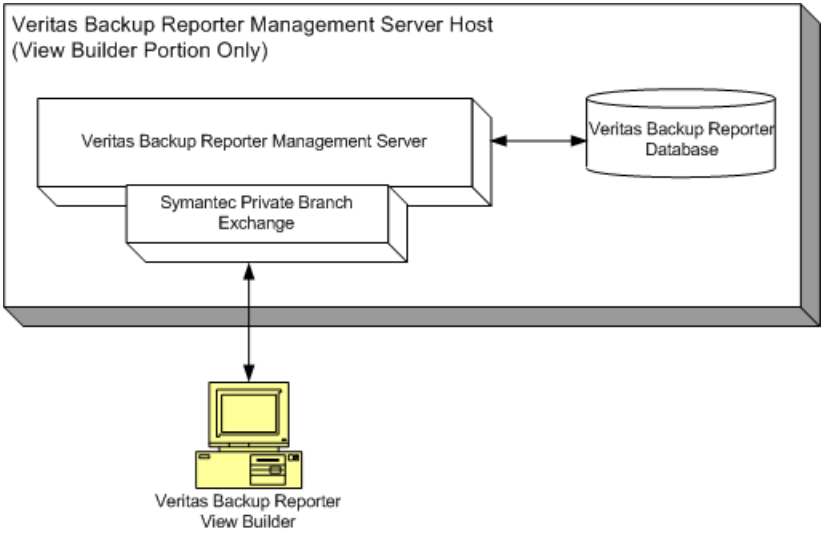
The VBR console is a graphical user interface that displays the Management Server information through a standard Web browser. You can view IT assets, generate reports, manage cost analysis and chargeback for services, view filter events, and so on.

See the *Veritas Backup Reporter User's Guide*.

About the Veritas Backup Reporter View Builder

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

Figure 1-5 VBR View Builder: Architecture



As the VBR Management Server relies on Symantec Product Authentication Service to authenticate Agent - Management Server connections, the Symantec Product Authentication Service client libraries reside on the View Builder host.

When run, the Java View Builder directly connects to the VBR Management Server; however, the JRE is required on the View Builder host. The View Builder queries the VBR database and displays current object view definitions. Actions performed via the View Builder console are then stored in the VBR database.

Chapter 2

Managing Veritas Backup Reporter user accounts

This chapter includes the following topics:

Creating new user accounts

Once you install Veritas Backup Reporter (VBR), you need to create user accounts. The Symantec Product Authentication Service validates user credentials in Veritas Backup Reporter based on NT, NIS, or private domains.

See "About the Veritas Backup Reporter database " on page 19.

If you are authenticating users based on a pre-existing NT, NIS, or localhost domain, use the Add User option. If you are implementing a private domain, create Veritas Backup Reporter users with the Create Private Domain User option.

See " Creating new private domain user accounts " on page 28.

Note: We recommend that you immediately create one or more administrator accounts to replace the default administrator account that ships with Veritas Backup Reporter. The default account has the username `admin` and the password `password`.

To create a new Veritas Backup Reporter user account:

1. In the VBR console, log on to a VBR Management Server host, on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Click **Add User**.
5. In the New User Details window, type information (such as first name and last name) of a new user in the corresponding fields.

   For more information, click **Help**.

   Most fields are optional; however the following fields require values:

Login	Enter any alphanumeric or special character (maximum 255)
Domain Name	Select a domain from the drop-down list. See "About the Veritas Backup Reporter database " on page 19.
Access Level	Select User, Administrator (Read Only), or Administrator.

   Administrator has the read and write privileges on all Veritas Backup Reporter functionalities.

   Administrator (Read Only) has the read privileges on all functionalities and write privileges on limited functionalities in Veritas Backup Reporter.

   User has the read and write privileges on limited functionalities in Veritas Backup Reporter.
6. Once you have typed the required user information, click **Save** to create the new user account.

Creating new private domain user accounts

Once you install Veritas Backup Reporter, you need to create user accounts. The Symantec Product Authentication Service validates user credentials in Veritas Backup Reporter based on NT, NIS, or private domains.

See “About the Veritas Backup Reporter database ” on page 19.

If you are implementing a private domain, then create Veritas Backup Reporter users with the Create Private Domain User option; if you are authenticating users based on a pre-existing NT, NIS, or localhost domain, then use the Add User option.

See “ Creating new user accounts ” on page 27.

Note: We recommend that you immediately create one or more administrator accounts to replace the default administrator account that ships with Veritas Backup Reporter. The default account has the username `admin` and the password `password`.

To create a new Veritas Backup Reporter private domain user account

1. In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Click **Create Private Domain User**.
5. In the New User Details window, type information (such as first name and last name) for the new user in the corresponding fields.

   Most fields are optional; however the following fields require values:

Login	Enter any alphanumeric or special character (maximum length 255)
Domain Name	Select a domain from the drop-down list. See “About the Veritas Backup Reporter database ” on page 19.
Access Level	Select User, Administrator (Read Only), or Administrator, to set the access level or privileges for the user.

   Administrator has the read and write privileges on all functionalities in Veritas Backup Reporter.

   Administrator (Read Only) has the read privileges on all functionalities and write privileges on limited functionalities in Veritas Backup Reporter.

   User has the read and write privileges on limited functionalities in Veritas Backup Reporter.
6. Once you have typed the required user information, click **Save** to create the new private domain user account.

Viewing user account information

You can view a list of the Veritas Backup Reporter users and their information such as, name, user name, access level, authentication domain, and so on. This list is arranged in a tabular form, which you can sort by the user details appearing as columns.

To view Veritas Backup Reporter user account information

1. In the VBR console, log on to a VBR Management Server host, on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Click **Report**.

   This displays a list of the Veritas Backup Reporter users in a tabular form.

Editing user accounts

You can modify the password, permission level, and user information for the user accounts you have already created.

To edit a Veritas Backup Reporter user account

1. In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management.**
4. Next to the user account that you want to edit, click **Edit**.
5. In the User Information window, make the necessary changes to the user account.
6. When you are finished, click **Save** to save the changes made to the user account.

Deleting user accounts

You can delete user accounts that do not need to be maintained.

Warning: Do not inadvertently delete all your administrator accounts.

To delete a Veritas Backup Reporter user account

1. In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Check the user account you want to delete.
5. Click **Delete**.

   This displays a confirmation window.
6. Select one of the following:
   - OK: To confirm the deletion.
   - Cancel: To stop the deletion.

Creating user groups

If you want to give the same privileges to multiple users, add them to a single user group. This user group can then be assigned read-write privileges on Veritas Backup Reporter views, as required. All users in this user group will be attributed with the same access rights at once.

To create a Veritas Backup Reporter user group

1. In the VBR console, log on to a VBR Management Server host, on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings.**
3. Click **Users/Groups Management**.
4. Click the Groups tab.
5. On the Groups tab, click **Add Group**.
6. In the New Group Details window, type the group name, and click **Save**. The new user group is created.

   Click the Users tab. You can now go to the Users tab and add user accounts to the group.

   See " Adding users to groups " on page 31.

Adding users to groups

You can add user accounts to groups that have been created.

To add a user account to a Veritas Backup Reporter user group

1. In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Select one or more users you want to add to a group.
5. Click **Add Users to Group**.
6. In the new window, select one or more user groups to which you want to add the selected users.
7. Click **Add.**

   The selected users are added to the selected user groups.

Editing user groups

You can modify an existing user group.

To edit a Veritas Backup Reporter user group

1. In the VBR console, log on to the VBR Management Server host, on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Users/Groups Management**.
4. Click the Groups tab.
5. On the Groups tab, next to the user account that you want to edit, click **Edit**.

   This displays the Group Information window.
6. In the Group Information window, make the necessary changes to the user group.
7. Click **Rename Group** to save the changes made to the user group.

Deleting user groups

You can delete a user group that you no longer need.

To delete a Veritas Backup Reporter user group

1. In the VBR console, log on to the VBR Management Server host on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.

3 Click **Users/Groups Management**.

4 On the Groups tab, select one or more user groups that you want to delete.

5 Click **Delete**. This displays confirmation window.

6 On the confirmation window, select one of the following:

- OK to confirm the deletion. This displays a window stating that the user group has been deleted.
- Cancel to stop the deletion.

Chapter 3

Managing Veritas Backup Reporter licenses

This chapter includes the following topics:

Adding license keys

An administrator can use the console to install Veritas Backup Reporter license keys and activate additional product features, or to delete license keys that are no longer needed.

You can add one or more Veritas Backup Reporter license keys to the VBR Management Server on which you are connected as an administrator.

To add Veritas Backup Reporter license keys

1. In the VBR console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Licensing**.

   A new window displays a table containing license keys installed on the VBR Management Server host.

4 In the Add new License Key text box, type a valid Veritas Backup Reporter license key.

For more information, click **Help**.

5 Click **Add Key**.

Veritas Backup Reporter adds the new license key to the VBR Management Server.

Viewing license keys

You can view license keys installed on the VBR Management Server host, on which you are connected.

To view Veritas Backup Reporter license keys

1 In the VBR console, log on to the VBR Management Server host, on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings**.

3 Click **Licensing**.

A new window displays a table containing license keys installed on the VBR Management Server host.

Deleting license keys

You can remove one or more Veritas Backup Reporter license keys from the VBR Management Server, on which you are connected as an administrator.

To delete Veritas Backup Reporter license keys

1 In the VBR console, log on to the VBR Management Server host, on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings**.

3 Click **Licensing**.

A new window displays a table containing license keys installed on the VBR Management Server host.

4 Select the check box in front of the license key you want to delete.

5 Click **Delete**.

6 In the confirmation window, select one of the following:

- OK to confirm the deletion. This displays a window stating that the key has been deleted.

- Cancel to stop the deletion.

Chapter 4

Managing Veritas Backup Reporter views

This chapter includes the following topics:

Understanding views

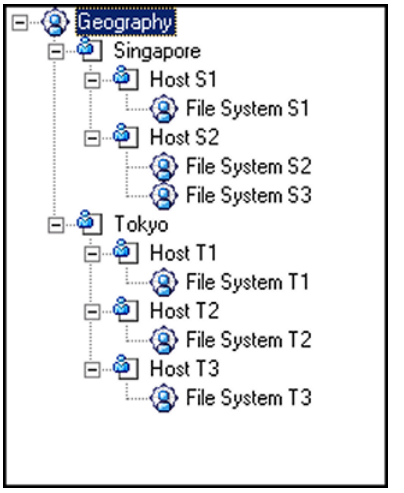
The Veritas Backup Reporter (VBR) View Builder is used to create views that are logical groups of IT assets (hosts or file systems) organized in a hierarchical manner.

In a VBR view, IT assets - scattered across organization - can be arranged according to their locations, business units, and so on. You can generate various VBR reports filtered by views. With these reports, you can identify the locations or departments that with hosts containing business critical data.

After you install and run the VBR Management Server and the Agent, IT assets are detected by Veritas Backup Reporter, which will then be stored in the database. The VBR View Builder makes these IT assets available while creating a view.

Note: To run the VBR View Builder, you need Java Runtime Environment (JRE) installed on the host.

In a view hierarchy, between top and bottom levels you can create a number of user-defined levels. For example, you can create a view called Geography as follows:



This example contains two nodes, Singapore and Tokyo, which are at the first level of the tree structure. The hosts are at the second level and the file systems are at the third level of the structure.

Running the VBR View Builder

To run the VBR View Builder:

1. From the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. From the console, click the Views tab, and then click **Java View Builder**.

Note: In addition to the procedure given, you can run the VBR View Builder in several other ways. However, to run the View Builder, you need to log on to Veritas Backup Reporter with valid user credentials.

Creating views

Create an empty view for example, Application, which is termed as node of the view. The Application view can contain logical categories (referred to as levels) such as ERP, database, and Email, which are at level 2. You can create as many intermediate levels of logical or physical categories as you want before adding actual IT assets.

Note: To create views in the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To create views:

1. On the View Builder toolbar, click**Create View**, or from the menu, click **Actions > New > Create New View**.
2. In the Create new View dialog box, in the View Name field, type the name of the new view.

   The name must be unique.
3. Click **OK**.

   The new view appears in the left pane of the View Builder window.

Creating levels in views

A newly created view has only one level. View objects or IT assets such as, hosts, file systems, or applications are at lowest levels in the view.

Between the top level and the bottom levels, you can create multiple intermediate levels to organize view objects into logical groups, creating a hierarchical structure in the view.

Note: To create levels to a view in the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To create levels in views:

1. In the VBR View Builder window, from the Available Object Views drop-down list box, select the view in which you want to create a new level.
2. Right-click the view name.
3. On the right-click menu, click **Create New Object**.

4 In the Add Object dialog box, in the Name field, type the name of the new level (or a logical category).

The name must be unique.

5 Click **OK**.

A new object appears under the selected view.

Adding objects to views

Once you add objects to a view in the View Builder, you can view them in the VBR console.

Note: To add objects to view in the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To add objects to views:

1 In the View Builder window, select the view and the level or logical category (if any) in which you want to add view objects.

2 On the Unassigned Objects tab, select one or more objects in the table that you want to add to the view.

You can select objects in succession using click + SHIFT, or distinct objects using click + CTRL.

3 Drag the selected objects and drop it onto the view or level.

The View Builder increments the number directly beneath the view or level to which you added the object.

Note: To view a list of all recently modified objects, click the **Recently Accessed Assets** tab.

Searching for objects

You can search for objects (IT assets) in the VBR database.

Note: To access the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To search for objects:

1. In the View Builder window, on the Search Objects tab, in the Search text box, type a name (or part of a name) for an object that you want to locate.

   The search is case-insensitive.

2. Click **Search**.

   The View Builder displays the matching view objects.

Removing views, levels, or objects

You can delete views, levels, or objects from the View Builder. If you delete a view (or a level), all objects under the view (or the level) will also be deleted.

Note: To access the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To remove views, levels, or objects:

1. In the View Builder window, select the view, level, or the object that you want to delete.
2. Right-click the view, level, or object.
3. On the right-click menu, click **Delete**.
4. In the Delete All dialog box, click **OK**.

Renaming views, levels, and objects

You can rename views, levels, and objects which are stored in the VBR database.

Note: To access the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To rename views and levels:

1. In the View Builder window, select the view or the level that you want to rename.
2. Right-click the view, level, or object that you want to rename.

3 On the right-click menu, click **Rename**.

4 Type the new name for the view, level, or object and then press **Enter**.

The new name must be unique.

The new name for the view, level, or object appears in the left pane.

Managing user access to views

You can specify which user accounts and/or user groups should have access to a view.

Note: To access the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To manage user and group access to views:

1 In the View Builder window, select the view for which you want to set access rights.

Setting access rights for the view has precedence over access rights set at the object level.

2 Right-click the view that you want to set access right for.

3 On the right-click menu, click **Properties**.

4 On the User Security tab, add available users to the Granted Read Permission list box or the Granted Write Permission list box, and click **Ok**. The selected users have the read or write privileges on the selected view.

5 On the Group Security tab, add available user groups to the Granted Read Permission list box or the Granted Write Permission list box, and click **Ok**. The users in the selected groups have the read or write privileges on the selected view.

Managing user access to levels or objects

You can specify which user accounts and/or user groups should have access to a level or an object.

Note: To use the VBR View Builder, you must have administrator-level privileges on the VBR Management Server.

To manage user and group access to views:

1. In the View Builder window, select the level or the object for which you want to set access right.
2. Right-click the level or the object that you want to set access right for.
3. On the right-click menu, click **Properties**.
4. On the User Security tab, add available users to the Granted Write Permission list box, and click **Ok**. The selected users have the write privilege on the selected level or object.
5. On the Group Security tab, add available user groups to the Granted Write Permission list box, and click **Ok**. The users in the selected groups have the write privilege on the selected level or object.

Chapter 5

Managing Veritas Backup Reporter data

This chapter includes the following topics:

Setting data retention policies

Use the Veritas Backup Reporter (VBR) console to set the number of days for which you want to retain records of each type of data in the VBR database.

You can set the data retention policies for the following data types:

- Backup job data
- Backup log data
- Backup job skipped files data
- Tape drive usage data
- Media Data

Note: Select the Disable Purging check box if you do not want VBR to automatically delete the records after the days specified in the data retention policies.

To modify data retention settings

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Data Retention**.
4. In the Data Retention Policies window, make the required changes in the data retention settings.
5. Click **Save**.

   VBR saves the data retention modifications.

Disabling demo database purging

The sample data that ships with VBR 4.2 FP1 has database purging enabled. This means that when the VBR Management Server starts, all media data is purged.

In VBR 4.2 FP1, sample database purging is disabled by default. The Solaris sample database swap script prompts you to run the timeshift tool after the database has been swapped, but before the VBR Management Server has restarted. You can enable or disable database purging at any time through the VBR console.

Warning: Do not use this feature while connected to the VBR database in a production environment. Loss of important data can result.

To disable demo database purging

1. With the console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Data Retention**.
4. In the Data Retention Policies window, click **Disable Purging**.
5. Click **Save**.

   Database purging is disabled.

Managing VBR database activities

Carry out the following tasks to manage VBR database:

- Starting and stopping the VBR database

- Backing up the VBR database
- Restoring the VBR database

Starting and stopping the VBR database

When the database is down, the Alert Manager server will log errors for some operations and may fail to log some statistical information to the database (the information will be lost), as well as fail to create alerts that might occur while the database is down. When the database is restarted, Alert Manager will reconnect and resume normal operation. If the database is in any way modified while it is down (for example, a backup restored or an upgrade performed), you must restart the Alert Manager server.

To stop and restart the VBR database on Solaris

1. Open the Solaris console, log on to the VBR database host as `root`, and change to the Veritas Database Server (ASA database server) directory:

   ```
   cd /opt/VRTSdbms3
   ```

2. Depending on the shell you are running, source the database script:

Bourne shell and Korn shell	`. vxdbms_env.sh`
C shell	`source vxdbms_env.csh`

3. Within the /opt/VRTSdmbs directory, change directory to /bin
4. To stop the database, type the following command:

   `vxdbms_start_db.pl veritas_dbms3_<hostName> -stop vxcc -force`

   where <hostName> is the name of the database server host.

5 To stop or start the VxDBMS server completely, type one of the following commands depending on if you want to stop or start the server:

```
/opt/VRTS/bin/vxccsvc stop vxdbms_d
```

```
/opt/VRTS/bin/vxccsvc start vxdbms_d
```

Note: Use the steps for stopping or starting the VxDBMS server completely unless another product for which you have installed is also using VxDBMS.

See vxccsvc on page 124.

6 To restart the database, type the following command:

```
vxdbms_start_db.pl veritas_dbms3_<hostName>
<databaseDirectory>/ccsvc.db -truncatelog
```

where <hostName> is the name of the VBR Management Server and <databaseDirectory> is the location where the database resides (by default:/var/Veritas/ccs_data).

For example:

```
vxdbms_start_db.pl veritas_dbms3_myhost
/var/Veritas/ccs_data/ccsvc.db -truncatelog
```

To stop and restart the VBR database on Windows

1 Open a Windows command prompt, log on to the VBR database host as an administrator or user in the Administrators group, and change to the Veritas Database Server (ASA database server) directory:

```
cd \Program Files\VERITAS\VxDBMS3\Win32
```

2 To stop the database, type the following command:

```
vxdbms_start_db.exe "C:\Program Files\VERITAS\VxDBMS3\Win32"
Veritas_DBMS3_%ComputerName% -stop ccsvc -force
```

where <%ComputerName%> is the name of the database server host.

3 To restart the database, type the following command:

```
vxdbms_start_db.exe "C:\Program Files\VERITAS\VxDBMS3\Win32"
Veritas_DBMS3_%ComputerName% "c:\Program Files\Symantec\Veritas
Backup Reporter\CC Data\db\ccsvc.db" ccsvc -truncatelog
```

where <%ComputerName%> is the name of the database server host.

Changing the VBR database password

Veritas Backup Reporter 6.0 provides the change password utility that is used to change password of the VBR database.

Veritas Backup Reporter relies on the Sybase ASA (Adaptive Server Anywhere) database to store backup data. You require a username and a password to access the data stored in the database. There are three main database user accounts that are included as part of Veritas Backup Reporter:

- guest - A read-only account with "guest" as a password. The guest account is not used by the VBR Management Server.
- ccsvc - An account used by the VBR Management Server to access the database. This account owns all database tables of Veritas Backup Reporter.
- dba - The database administrator account. The dba account is required by the database queries that are used to update the database schema, upgrade to a new release, and so on.

Table 5-1 Location of the ccsvc-changedbpassword utility

Platform	Directory Location
Windows	<serverInstallDir>\util

Syntax

Use the following syntax for issuing ccsvc-changedbpassword utility commands.

```
changedbpassword.exe [--setGuestPassword=<guest password>]
[--setDBAPassword=<DBA password>] [--setServerPassword=<server
password>] | [--restoreDefault] | [-h|-?|--help]
```

```
--setGuestPassword
```

Change the database guest password.

```
--setDBAPassword
```

Change the database dba password.

```
--setServerPassword
```

Change the password used by the server to log into the database.

```
--restoreDefault
```

Reset all the passwords to default passwords.

```
-h|-?|--help
```

Print this usage statement and exit.

If any of the --set* options are specified, only those passwords will be changed. Ideally, you should change all passwords. To specify the password on the command line, use an equals sign (=) and type the password.

Example

If you issued the following command at the command-line:

```
changedbpassword.exe --setGuestPassword=testpassword

--setDBAPassword
```

the ccsvc-changedbpassword utility sets the guest password to “testpassword” and asks for a dba password.

After running the ccsvc-changedbpassword utility, it is recommended that the system administrators set the permissions for the `vbr_conf.properties` file for system administrator use only to read the file.

Updated entries in the vbr_conf.properties file

Two new configuration property entries will be added to the `vbr_conf.properties` file:

- database.password.obfuscated.dba
- database.password.obfuscated.ccsvc

These parameters will store the obfuscated (encrypted) versions of the database passwords for the DBA and members of the ccsvc_user account.

If the database.password.obfuscated.ccsvc parameter is set in the vbr_conf.properties file, the server reads the obfuscated value, determines the password, and then uses the password for connecting to the database instead of using the default password.

Note: If the `vbr_conf.properties` file is missing or corrupt, or the database password for the DBA user is missing from the file, the default database password for the DBA user will be used for password changes. If the default password also does not work, the ccsvc-changedbpassword utility prompts the user for the current database password for the DBA user.

Updates to support

ccsvc-support is a script used for collecting VBR data used by Veritas Technical Support for troubleshooting.

If the ccsvc-changedbpassword utility has been run, support will include the updated vbr_conf.properties file when gathering information about the VBR Management Server.

Backing up the VBR database

VBR is shipped with a database backup script that performs backups without interrupting database operations. On both platforms, the script overwrites any existing db files (the files noted in this list:`ccsvc.db`, `vxdmbulk.db`, and `ccsvc.log`) before backing up or restoring, and only backs up or restores `ccsvc.log` if it exists.

To back up the VBR database

1. Log on to the VBR database server host in one of the following ways:

Solaris	`root`
Windows	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/VRTSdbms3/bin/dbbackup/my_db_backup_dir`
Windows	`"C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util\DbBackup.bat"` `c:\MyDbBackupFolder`

   The backup script creates `ccsvc.db`, `vxdmbulk.db`, and `ccsvc.log` (if `ccsvc.log` exists) in the backup directory you specified.

Restoring the VBR database

After you backup the VBR database, you can restore it. On Solaris hosts, the restore operation automatically stops the database, restores the backup database files, and restarts the database. On Windows hosts, you issue a series of commands that stop the database, restore individual backup database files, and restart the database. On both platforms, the script overwrites any existing db files (the files noted in this list:`ccsvc.db`, `vxdmbulk.db`, and `ccsvc.log`) before backing up or restoring, and only backs up or restores `ccsvc.log` if it exists.

To restore a backed up VBR database

1. On the VBR Management Server whose backup data you want to restore, open a UNIX console or a Windows command prompt and log in as `root` (on UNIX) or as an administrator or user in the Administrators group (on Windows).

   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 VBR processes, do one of the following:

Solaris	Type the following command to stop the server: ■ **/opt/VRTS/bin/vxccsvc stop force**
Windows	Use the Windows Service Control Manager (SCM) to stop all VBR services

3. To restore the backed up database, do one of the following:

Solaris	Type the following command: **/opt/VRTSccsvs/bin/dbbackup.sh /my_db_backup_dir**
Windows	Type the following command: **C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util\DbBackup.bat<backupDir> -restore <restoreDir>**

   where <backupDir> is the directory where the backed up database resides, and <restoreDir> is the location of the current VBR database. <restoreDir> is optional. If not used, dbbackup and ccDbBackup.bat restores to the default database directory: /var/Veritas/ccs_data (on Solaris), \Program Files\Symantec\Veritas Backup Reporter\CC Data\db (on Windows).

   The script prompts you with a message similar to the following:

   ```
   WARNING: this operation will overwrite the active VBR data on
   this host. Do you wish to continue ? [y/n] (n)
   ```

4. To continue with the restore, type **y**.

   vx_ccdb_backup and ccDbBackup.bat automatically stops and restarts the database.

5. To restart all VBR processes, do one of the following:

Solaris	Type the following commands: ■ `/opt/VRTS/bin/vxccsvc start`
Windows	Use the Windows Service Control Manager (SCM) to start all VBR services.

Chapter 6

Configuring Veritas Backup Reporter Agents

This chapter includes the following topics:

About configuring VBR Agent

Veritas Backup Reporter (VBR) is designed to provide extensive reporting on the backup data received from multiple backup products. VBR Agents contain product-specific modules that collect data from these products and return it to the VBR Management Server.

The VBR Agent contains modules that monitor the following Veritas and third-party backup applications:

- Veritas NetBackup
- Veritas BackupExec (Windows only)
- EMC Legato Networker
- IBM Tivoli Storage Manager (TSM)
- CommVault Galaxy Backup & Recovery

See "About the Veritas Backup Reporter Agent " on page 21.

When you install the VBR Agent, Agent modules for all backup products are automatically installed. However, you need to configure and run an Agent module to be able to collect data from the respective backup product.

In case of EMC Legato Networker, the Agent must reside on the same host as the EMC Legato Networker application. For all other backup applications, the Agent and the applications can reside on different machines.

The VBR Agent and a backup product cannot reside on the same host in some situations as follows:

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

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

Note: If the VBR Agent is installed on the remote host, it must have a backup application component installed in order to communicate with the application. For example: The VBR Management Server is installed on Host A, the VBR Agent is installed on Host B, and NetBackup is installed on Host C. You must install NetBackup component that is a NetBackup client (.exe) on the Agent host to be able to collect data from NetBackup.

Table 6-1 Remote VBR Agent host configuration list

Monitored Backup Application	Remote VBR Agent configuration possible?
Veritas NetBackup	Yes
Veritas BackupExec	Yes
IBM Tivoli Storage Manager	Yes
EMC Legato Networker	No
CommVault Galaxy Backup & Recovery	Yes

Carry out the following tasks to enable and configure VBR Agent modules:

1 Plan where to install VBR Agents on your network.

See the *Veritas Backup Reporter Installation Guide*.

2 Add VBR Agent configurations to the VBR Management Server.

See "Configuring VBR Agent on the VBR Management Server" on page 59.

3 Enable and configure VBR Agent modules as follows:

- If the VBR Agent and the backup application to be monitored reside on the same host, enable and configure the VBR Agent module locally.
  See "Enabling and configuring VBR Agent modules (local)" on page 60.
- If the VBR Agent and the backup application to be monitored reside on different hosts, enable and configure the VBR Agent module remotely.
  See "Enabling and configuring VBR Agent modules (remote)" on page 69.

Configuring VBR Agent on the VBR Management Server

You need to configure VBR Agent on the VBR Management Server before configuring Agent modules.

To configure VBR Agent on the VBR Management Server:

1 With the VBR console, log on to the VBR Management Server with the administrator-level privileges.

2 In the console, click **Settings > Global Settings > Agent Configuration**.

3 On the Settings page, click **Create**.

4 On the Create Agent Configuration page, in the Agent Host Fully Qualified Name text box, type the fully qualified name of the VBR Agent host.

5 Click **Save**.

This displays a confirmation message after successfully saving the Agent configuration.

After you add a VBR Agent, the next step is to configure the Agent modules for the respective backup applications.

See "Enabling and configuring VBR Agent modules (local)" on page 60.

See "Enabling and configuring VBR Agent modules (remote)" on page 69.

Configuring the VBR Agent and NetBackup Agent module to collect library capacity data

Using Veritas Backup Reporter 6.0, you can collect library capacity data.

In order to collect library capacity data, the VBR Agent must communicate with the host on which NetBackup volume database resides. The NetBackup volume database can be on a separate media server, or on the master server host acting as a media server.

Note: In order to collect tape drive information from all media servers, the VBR Agent must be configured on the master server.

The VBR Agent needs to be authorized to connect to the master server along with all media servers. If it is not authorized, one of the following situations arises:

- Data can not be collected from the tape drives attached to the media server.
- The tape drive usage collection event is failed.

Note: Data collection for library capacity data can be performed locally as well as remotely.

Managing VBR Agent module configurations

Carry out the following tasks necessary to enable, modify, or disable VBR Agent modules:

- Enabling and configuring VBR Agent modules (local)
- Enabling and configuring VBR Agent modules (remote)
- Modifying VBR Agent modules
- Forcing VBR Agent module poll updates
- Copying VBR Agent module configurations
- Pausing VBR Agent modules
- Disabling VBR Agent modules

Enabling and configuring VBR Agent modules (local)

Veritas Backup Reporter (VBR) is designed to provide extensive reporting on the backup data received from multiple backup products. Veritas Backup Reporter consists of Management Server, Agent, and console. The Agent contains

product-specific modules collecting data from the backup products and returning it to the VBR Management Server. You can generate various business reports on this backup data.

When you install the VBR Agent, all Agent modules are automatically installed. After you have configured the VBR Agent on the VBR Management Server, enable and configure Agent modules.

The Agent contains modules that you can enable and configure for the following Veritas and third-party backup applications:

- Veritas NetBackup
- Veritas BackupExec (Windows only)
- EMC Legato Networker
- IBM Tivoli Storage Manager (TSM)
- CommVault Galaxy Backup & Recovery

Depending on the backup application you are monitoring, you have two options for deploying VBR Agent modules:

- Installing the VBR Agent on the backup application host (local)
- Installing the VBR Agent on a host different than the backup application host (remote)

This topic describes how to enable and configure VBR Agent module on the monitored application's host. You can also enable and configure VBR Agent modules remotely.

See "Enabling and configuring VBR Agent modules (remote)" on page 69.

To enable and configure VBR Agent modules (local):

1. With the VBR console, log on to the VBR Management Server, on which you have configured the VBR Agent, with the administrator-level privileges.

   See "Configuring VBR Agent on the VBR Management Server" on page 59.

2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. On the Settings page, click the VBR Agent for which you want to enable and configure a module.
4. On the Agent/Server Information Configuration page, click **Create**.

5 On the Create Agent Module Configuration page, from the Module drop-down list box, select the appropriate module type.

Note: The options in the Module drop-down list box comprises the backup product name and the operating system on which the Agent is running. Select the appropriate option from the list box. For example, if you want to collect data from a NetBackup master server running on a Solaris host and the VBR Agent is running on a Windows host, you need to select Veritas NetBackUp - Windows as a module type.

---

6 In the Module Host Name text box, type the name of the backup application host, from which the Agent module collects the data.

7 Click **Next**.

8 In the Module Details page, depending on the selected module type, module variables are displayed. You must configure these module variables.

Refer to the following sections for more information:

- See "Configuring Agent modules for Veritas NetBackup " on page 63.
- See "Configuring Agent modules for Veritas BackupExec " on page 66.
- See "Configuring Agent modules for EMC Legato Networker " on page 66.
- See "Configuring IBM Tivoli Storage Manager modules " on page 67.
- See "Configuring CommVault Galaxy Backup & Recovery Agent module" on page 68.

Note: See the *Veritas Backup Reporter Release Notes* for any updates to module variables.

---

9 For NetBackup, the Do Not Qualify options should only be used if the VBR Agent host and the NetBackup host use different DNS servers.

If the environment is set up in such a way that every host can resolve any other host, you should use this option.

You can test the Do Not Qualify options you have set by trying to run the command `nslookup <NBUclient>` on the VBR Agent computer, where <NBUclient> is a name of a host that NetBackup backs up.

10 Select the reports (data collection events) you want enabled and specify the collection interval (in seconds).

For more information about the options in 10 and 11, see the VBR console online Help.

11 Optionally, to choose a blackout period—a time of day when the VBR Agent does not poll for data—select a start time and duration of the blackout.

12 Click **Save**.

This displays a confirmation message.

Configuring Agent modules for Veritas NetBackup

Note: The version of NetBackup client binaries installed on the VBR Agent host must be the same as the remote NetBackup Server host, from which the Agent module collects data.

Table 6-2 describes the required variables for the Veritas NetBackup module.

Table 6-2 Veritas NetBackup Agent 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: `cli`. The `cli` method uses the CLI `bpdbjobs` 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 6-2 Veritas NetBackup Agent module required variables *(continued)*

Module variable	Description
daysPerImageFetch	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: Example of daysPerImageFetch time options: ■ 3 months ago to 2 months ago ■ 2 months ago to 1 month ago ■ 1 month ago to today 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. The drop down will consist of the following values: ■ 1800 days (default) ■ 360 days ■ 180 days ■ 90 days ■ 30 days ■ 7 days
role	Informs the module how to collect media data. If the host is both a master server and a media server, then use `Master`.

Enabling and configuring NetBackup Agent module for collecting library capacity data

You can configure the NetBackup Agent module either on the NetBackup master / media server host or a remote host. It is recommended that you configure the Agent module remotely.

The NetBackup master / media server is connected to the actual backup device, for example, tape drive or tape library.

To enable and configure the NetBackup Agent module for collecting Library Capacity data

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. In the Agents Settings page, click the VBR Agent for which you want to enable and configure a module.
4. In the Agent/Server Information Configuration page, click **Create**.
5. In the Create Agent Module Configuration page, on the Module drop-down list, select the appropriate module type.

   Note: The options in the Module drop-down list box comprises the backup product name and the operating system on which the Agent is running. Select the appropriate option from the list box. For example, if you want to collect data from a NetBackup master server running on a Solaris host and the VBR Agent is running on a Windows host, you need to select Veritas NetBackUp - Windows as a module type.

   ---

6. In the Module Host Name field, type the name of the Veritas NetBackup host.
7. Click **Next**.

   This displays the Module Details page. The module variables displayed vary depending on the module type selected.
8. Specify the variables for the NetBackup Agent module.
9. Select the Do Not Qualify option if the VBR Agent host and the NetBackup host use different DNS servers.

   If the environment is set up in such a way that every host can resolve any other host, you should select the Do Not Qualify option.

   You can test the Do Not Qualify option you have set by running the command `nslookup <NBUclient>` on the VBR Agent host, where <NBUclient> is the name of the host, from which NetBackup collects data.
10. Select the reports you want enabled, Tape Drive and Media, for collecting library capacity data.
11. Specify the Collection Interval in seconds. The data is collected from NetBackup with the interval specified.

12 Select the Blackout Period Start Time and Duration to specify the time of day when you do not want to collect data from the NetBackup host. The Blackout Period overrides the Collection Interval specified.

13 Click **Save**.

This displays a confirmation message after successfully saving the Agent module configuration.

Configuring Agent modules for Veritas BackupExec

Table 6-3 describes the required variables for the Veritas BackupExec module.

Table 6-3 Veritas BackupExec module required variables

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

Configuring Agent modules for EMC Legato Networker

Table 6-4 describes the required variables for the EMC Legato Networker module.

Table 6-4 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 `homeDirectory`. The default file name is `messages`. 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 `messagesFile` to this log.

Table 6-4 EMC Legato Networker module required variables *(continued)*

Module variable	Description
mminfoBinary	The directory path of the mminfo Command-Line Interface (CLI), absolute or relative to `homeDirectory`.
mminfoFile	(Optional) Output of `mminfo`.
nsrAdminBinary	The directory path of the nsradmin CLI, absolute or relative to `homeDirectory`.
nsrFile	(Optional) Output of an `nsradmin` command. The VBR console displays `nsrResFile`, `nsrFile`, and `mminfoFile` 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 `nsradmin` uses.

Configuring IBM Tivoli Storage Manager modules

Table 6-5 describes the required variables for the Tivoli Storage Manager module.

Table 6-5 IBM Tivoli Storage Manager module required variables

Module variable	Description
dsmConfig	The path to the `dsm.opt` file.
dsmDir	The path where files necessary to run `dsmadmc` reside.
dsmadmcLoc	The path of TSM administrative client (`dsmadmc`).
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`.)

Note: The TSM product environment variables `DSM_CONFIG` and `DSM_SYS` point to the `dsmadmc` required files `dsm.opt` and `dsm.sys` (Solaris and AIX). For more information, refer to your TSM documentation.

The TSM server host (also called product host) value for the TSM Agent module must be specified in the following manner:

Windows

Use the fully qualified host name. In short, product host is the value that you can use with the `dsmadmc -tcpserveraddress` option. For example, the following entries are valid for product host:

```
Host.sample.domain.com
```

```
Host
```

assuming that `Host` can be fully qualified.

Solaris and AIX

The product host must be the value specified in the `dsm.sys` file, for tag `SErvername` (note the case). In short, product host is the value that you can use with the `dsmadmc -se` option. The following is a sample `dsm.sys` file:

```
****************************************
SErvername server_a COMMmethod
CoMMmethod TCPip
TCPPort 1500
TCPServeraddress 255.255.255.255
SERVERNAME MYHOST.Veritas.COM
TCPSERVERADDRESS 255.255.255.255
NODENAME myhost.mycompany.com
****************************************
```

Configuring CommVault Galaxy Backup & Recovery Agent module

Table 6-6 CommVault Galaxy Backup & Recovery Agent Module required variables

Module variable	Description
password	The password required to connect to database.

Table 6-6 CommVault Galaxy Backup & Recovery Agent Module required variables *(continued)*

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

Note: Because CommVault uses an MS SQLServer 2000 database to store data collected by the module, you will need to download the MS SQL Server 2000 JDBC drivers at: http://www.microsoft.com/downloads/details.aspx?FamilyID=07287b11-0502-461a-b138-2aa54bfdc03a&displaylang=en.

Copy the following three files to $CCSVC_INSTALL/lib:

- msbase.jar
- msutil.jar
- mssqlserver.jar

Enabling and configuring VBR Agent modules (remote)

When you install the VBR Agent, all Agent modules are automatically installed. After the Agent installation, enable and configure the Agent modules that are used to collect data from backup products.

Depending on the application you are monitoring, you have two options for deploying VBR Agent modules:

- Install the VBR Agent on the monitored application's host (local)
- Install the VBR Agent on a host that is not the monitored application's host (remote)

The following table lists the backup applications that support a remote VBR Agent configuration.

Table 6-7 Remote VBR Agent host configuration list

Monitored Backup Application	Remote VBR Agent configuration possible?
Veritas NetBackup	Yes
Veritas BackupExec	Yes

Table 6-7 Remote VBR Agent host configuration list *(continued)*

Monitored Backup Application	Remote VBR Agent configuration possible?
IBM Tivoli Storage Manager	Yes
EMC Legato Networker	No
CommVault Galaxy Backup & Recovery	Yes

This topic describes how to enable and configure VBR Agent modules installed on remore Agent. You can also enable and configure VBR Agent modules locally.

See "Enabling and configuring VBR Agent modules (local)" on page 60.

To enable and configure VBR Agent modules (remote)

1. Ensure that the VBR Agent supports a remote configuration for the backup application you want to monitor.
2. If you have not done so already, install the VBR Management Server on a Solaris or a Windows host.

   For more information, see the *Veritas Backup Reporter Installation Guide*.
3. Install the VBR Agent on either the VBR Server host or on another Solaris or Windows host that has network access to both the VBR Management Server and the backup application hosts.

   For more information, see the *Veritas Backup Reporter Installation Guide*.

4 If you are monitoring NetBackup, do the following:

Solaris	On the NetBackup target host, with a text editor open the NetBackup configuration file, `/usr/openv/netbackup/bp.conf`, and add the following line: `SERVER=<agentHostName>` where `<agentHostName>` is the fully qualified domain name of the VBR Agent host that will monitor the NetBackup target host.
Windows	On the NetBackup target host, use the NetBackup Administration console to set this value.
Tivoli Storage Manager (TSM)	Configure the TSM administrative client to access data remotely from all the TSM master servers you want to monitor; then, skip to 7. See your *Tivoli TSM* documentation.

5 Stop and restart the monitored processes on both NetBackup target host and the remote Agent host.

6 Verify the link between the VBR Agent host and the target NetBackup host by running the following command from the VBR Agent host:

Solaris	`/usr/openv/netbackup/bin/admincmd/bpdbjobs -report -all_columns -M localhost`
Windows	`C:\Program Files\Veritas\NetBackup\bin\admincmd\bpdbjobs -report -m NBUserver`

If the command in 6 returns NBU data from the NBU server, then the link is functioning correctly, otherwise check the following:

- Make sure the Agent host is correctly declared in the `bp.conf` on the target NBU server (the host in 4).
- Make sure that NBU binaries are installed in the default location on the target NBU server (the host in4):

Solaris	`/usr/openv/netbackup`
Windows	`C:\Program Files\Veritas\NetBackup`

7 Configure the VBR Agent on the VBR Server.

See "Configuring VBR Agent on the VBR Management Server" on page 59.

8 Enable and configure VBR Agent modules as described in the topic, Enabling and configuring VBR Agent modules (local)

9 If the command in 6 returns NBU data from the NBU server, it indicates that the link is functioning correctly. In case the data is not returned, on the Module Details page (8) provide the values for the module variables as follows:

- NetBackup

Collection Method	Click **CLI**.
homeDirectory	Paths that are on the monitored application host, not paths on the remote VBR Agent host.
volumeManagerHome	Paths that are on the monitored application host, not paths on the remote VBR Agent host.
Discovered Hosts - Name Qualification Options:	Click **Do Not Qualify**.

- Tivoli Storage Manager (Windows)

Module Host Name	TCP server address of TSM master server
tcpPort	TCP port for accessing the above master server
tsmId	Administrative client user name
tsmPassword	Password for the administrative client user name

- Tivoli Storage Manager (Solaris)

Module Host Name	The server name specified by `-se` tag in the `dsm.sys` file
tsmId	Administrative client user name
tsmPassword	Password for the administrative client user name

10 Select the reports (data collection events) you want enabled and specify the collection interval in seconds.

See the VBR online Help for more information.

11 Click **Save**.

Modifying VBR Agent modules

You can use the VBR console to modify modules for a VBR Agent.

To modify VBR Agent modules:

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration.**.
3. On the Settings page, click the VBR Agent to be modified.
4. On the Agent/Server Information Configuration page, in the Modules table, select the module you want to modify.
5. In the Agent Configuration panel, to modify the settings in the event discovery table, do the following:
   - Enable or disable data collection of each information type by selecting or clearing it in the Enabled column.
   - Modify the length of time between data collection of each information type by typing the interval length in seconds in the Interval column.
6. Click **Save** in the data collection table.
7. Modify the settings in the module variables table by typing or clicking the appropriate value for each variable in the Value column.
8. Click **Save** in the module variables table.

Forcing VBR Agent module poll updates

You can use the VBR console to force poll updates for a particular module on a VBR Agent.

Warning: For force polls to work, the VBR Management Server needs to be able to reach the VBR Agent on the Agent CORBA port. The default port is 7806. If this port is changed, force polls will not work.

To force poll updates for a particular module on a VBR Agent:

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. On the Settings page, click the link for the VBR Agent for which you want to force poll a module update.

4 On the Agent/Server Information Configuration page, in the Settings table, select the module for which you want to force poll an update.

5 Click **Show Agent Status** at the bottom of the screen.

6 On the Complete Agent Status page, click the module for which you want to force poll an update.

7 On the Complete Agent Status page, for Force Poll, click **Poll**.

Viewing VBR Agent alerts

You can use the VBR console to view VBR Agent alerts for a particular module on a VBR Agent.

To view VBR Agent alerts for a particular module:

1 With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings > Agent Configuration**.

3 On the Agent Settings page, click the link for the VBR Agent for which you want to view Agent alerts.

4 On the Agent/Server Information Configuration page, in the Settings table, select the module for which you want to view VBR Agent alerts.

5 Click **Show Agent Status** at the bottom of the screen.

6 On the Complete Agent Status page, click **Alerts**.

The Alerts configuration panel is displayed with information of the VBR Agent you have selected.

Copying VBR Agent module configurations

You can use the VBR console to copy a module configuration on a VBR Agent. In this way, you can quickly duplicate module settings for various Agent hosts.

To copy module configurations on VBR Agents:

1 With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings > Agent Configuration**.

3 In the Agent Settings page, click the VBR Agent for which you want to copy one or more module configurations.

4 In the Agent/Server Information Configuration page, in the Settings table, select the modules you want to copy.

5 On the drop-down list, click **Copy Items**, and then click **Go**.

6 On the alert message box, click **OK**.

7 Specify the host name of the target agent module.

Pausing VBR Agent modules

You can use the VBR console to pause data collection by VBR Agent modules.

To pause VBR Agent modules:

1 With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings > Agent Configuration**.

3 On the Agent/Server Information Configuration page, in the Settings table, click the Agent module you want to pause.

4 Click **Show Agent Status**.

5 On the Complete Agent Status page, click the link for the Agent module you want to pause.

The Complete Agent Status is displayed with detailed information about the core agent status.

6 To pause a running module, click either **Data Collection** (also known as Scheduler) or **Communication** (queue for handling data collection events).

When you click Data Collection, the system stops queuing new data collection events. The VBR Agent stops sending heartbeats to the VBR Management Server. However, the existing data collection events continue to run, and the associated backup data is sent to the Management Server.

If you click Data Communication, the communication between the Management Server and the Agent is paused. The Management Server does not receive backup data associated with any of the data collection events. However, the data collection events are queued and they will remain in the queue until Data Communication is resumed. The text will change depending on the current state.

Disabling VBR Agent modules

You can use the VBR console to disable a module on a VBR Agent.

To disable modules on VBR Agents:

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. On the Agent Settings page, click the VBR Agent from which you want to delete a module.
4. In the Agent/Server Information Configuration panel, in the Settings table, select the module you want to delete.
5. From the drop-down list, click **Delete**, and then click **Go**.
6. On the alert message box, click **OK**.

Modifying VBR Agent and Management Server port information

With the VBR console you can modify the VBR Agent CORBA port and the VBR Management Server port.

Note: The VBR Management Server port is different than the port used for communicating with the VBR console.

See "Changing the Web Server port " on page 83.

To modify the VBR Management Server and the VBR Agent CORBA port:

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. In the Agent Settings page, click the VBR Agent for which you want to modify ports.

   See the *Veritas Backup Reporter Installation Guide* for port information.
4. On the Agent/Server Information Configuration page, for the Backup Reporter Server Port text box, type a new port number.
5. In the Agent Host CORBA Port text box, type a new port number.
6. Click **Save**.

Modifying log configurations for VBR Agents

The error logged by the VBR Agent can consume a large amount of disk space. If you do not want to retain these error logs, you can disable them using the Web console. You can also configure the granularity of the data in a log, its rollover count, and the maximum size of its log file.

To modify log settings for VBR Agents:

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. On the Agent Settings page, click the VBR Agent whose log settings you want to configure.
4. On the Agent/Server Information Configuration page, in the Agent Log Configuration panel, modify the default settings.

   For more information, click **Help**.
5. To disable error log collection, in the Agent Configuration panel, click **Off** from the drop-down list in the Level text box.
6. Click **Save**.

Removing VBR Agent configurations from the VBR Management Server

To remove a VBR Agent configuration from a VBR Management Server, follow these steps.

To remove VBR Agent configurations from the VBR Management Server:

1. With the VBR console, log on to the VBR Management Server from which you want to remove one or more VBR Agents, with the administrator-level privileges.
2. In the console, click **Settings > Global Settings > Agent Configuration**.
3. On the Agents Settings page, in the Settings table, select one or more Agents that you want to remove from the VBR Management Server, by selecting check boxes next to them.

4 Click **Delete**.

An alert message is displayed before deleting the Agent.

5 In the Create Agent Configuration window, click **OK**.

The Agent configuration is removed from the Management Server, and the Agent name is no longer displayed in the Settings table.

Chapter 7

Configuring Veritas Backup Reporter

This chapter includes the following topics:

Editing links to Veritas products

Use the Veritas Backup Reporter (VBR) console to perform various VBR Management Server configuration tasks.

You can use the links in the VBR console header to navigate to other Veritas products. If other Veritas products are installed on the same host, you do not need to configure the links manually . However, if a product is installed on a different host, or if the default port for the product changes, you will need to configure the URL. After the initial configuration if the port or host changes, you need to modify the URL settings again.

To edit the link to another Veritas product

1. With the VBR console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Module Links**.
4. In the table, select the Veritas product to edit the link.
5. From the Protocol drop-down list box, select one of the following:
   - http
   - https (secure)
6. In the Host text box, type a valid host name, qualified host name, or a host IP address of the server.

   If you do not specify a host name, Veritas Backup Reporter clears the host and port text boxes.
7. In the Port text box, type the port through which you want to connect to the product's server.

   See the *Veritas Backup Reporter Installation Guide* if you need to look up the default port number.

   If you do not specify port or protocol, Veritas Backup Reporter uses the current values contained in the URL in the address field of your browser.
8. Click **OK**.

Configuring data retention

You can use the VBR console to configure VBR Management Server retention periods for data types that are logged such as, Job, Policy, and Skipped Files.

To configure the time for which the VBR Management Server retains data:

1. With the console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.

3 Click **Data Retention**.

4 In the Data Retention dialog box, type the number of days to retain the data in the VBR database.

5 Click **Save** to finish.

Configuring global system settings

You can configure your own settings for the VBR console and apply them globally for all users.

To configure global system settings for the VBR console

1 With the console, log on to the VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings**.

3 Click **System Settings**.

4 Edit the information in any of the following text boxs:

- System Name
- Email Address
- Email Address Name

5 Click **Save** to save your changes.

Defining view level aliases

You can use the console to give descriptive names to the various levels of an Object View's tree structure. These aliases replace the default labels such as "Level 1" and "Level 2" that appear in the Custom Report Wizard.

To define aliases for the levels in an Object View

1 With the console, log on to a VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings**.

3 Click **Alias View Levels**.

4 Select an Object View from the View Name drop-down list.

5 Type an alias for each level of the Object View in the corresponding fields.

6 Click **Save**.

Copying user-defined content and settings

Most user-definable content, such as reports and chargeback formulas, is accessible only by the user who created it. To make such content available to other users, an administrator can use the Copy User Profile feature. This copies information - such as, reports, chargeback rates and formulas, event list settings, and the user's default view - from one user account to another, .

Note: As of the 6.0 version, if you are not an administrator, you will not be able to copy reports that are not based on views. You will also not be able to copy view-based reports if you do not have the correct access to the view. If you need to run non-view-based reports, you need to have at least Administrator (Read-Only) privileges. An Administrator with Read-Only privileges can still be given permission to modify a particular view.

To copy settings and content from one user account to another

1. With the console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Copy User Profile**.
4. Select the source user account from the From drop-down list box.
5. Select the target user account from the To drop-down list box.
6. In the Copy Items window, do one of the following:
   - Select the items you want to copy for example, Reports, Cost Rates and Formulas, Default View, or Event List Settings.
   - Click **Select All** to select all items at once.
7. Click **Next**.
8. Click **Save** to finish.

Configuring the SMTP Mail server

You may need to change the SMTP Mail server for Veritas Backup Reporter.

To configure SMTP Mail

1. With the console, log on to the VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.

3 Click **Web Console Configuration**.

4 In the Veritas Web console window, on Configuration tab, click **Configure SMTP Server**.

5 Type the necessary information in the following fields:

SMTP Server	The valid name of the SMTP server
Username	The user account used to connect to the SMTP server
Password	The password associated with the user account

6 Click **OK**.

Managing Veritas Backup Reporter ports

The following topic describes how to change ports on various VBR components that communicate with the VBR Management Server:

- Changing the Web Server port

Changing the Web Server port

You may need to change a port that the VBR Management Server uses to communicate with the VBR console. First you add a new port and then delete the old port.

Note: This Server port is not the same port through which communication is handled with the VBR Agent and some of the other VBR components.

See "Modifying VBR Agent and Management Server port information" on page 76.

To configure VBR Management Server ports

1 With the console, log on to a VBR Management Server on which you have administrator-level privileges.

2 In the console, click **Settings > Global Settings**.

3 Click **Web Console Configuration**.

4 In the Veritas Web console window, on the Configuration tab, click **Add Port**.

5 Enter the necessary information in the following fields:

Port Number	Type the port number that you want the VBR Management Server to use. For more information about ports Veritas Backup Reporter uses, see the *Veritas Backup Reporter Installation Guide*.
Protocol	Select one of the following: ■ http (unsecured) ■ https (secure)
IP Address	(Optional)Type the IP address for the Server.
Username	Type a user account that has superuser (administrative) privileges on the Server.
Password	Type the password associated with the user account.

6 Click **OK**.

7 To delete the old port, do the following:

- Repeat 1–4.
- In 4, click **Delete Port**.

8 Type the necessary information in the following fields:

Port Number	Type the port number that you want to delete. (You cannot delete the port being used to access the Web page.) For more information about ports Veritas Backup Reporter uses, see the *Veritas Backup Reporter Installation Guide*.
IP Address	If the port was bound to a particular IP address, type the IP address.
Username	Type a user account that has superuser (administrative) privileges on the Server.
Password	Type the password associated with the above user account.

9 Click **OK**.

Configuring VBR Management Server logging

You can change VBR Management Server logging with the VBR console.

To configure VBR Management Server logging

1. With the console, log on to a VBR Management Server on which you have administrator-level privileges.
2. In the console, click **Settings > Global Settings**.
3. Click **Web Console Configuration**.
4. In the Veritas Web console window, on the Configuration tab, click **Configure Logging**.
5. In the Web Applications drop-down list, select one of the following log levels:
   - Fine
   - Finer
   - Finest
   - Config
   - Info
   - Warning
   - Severe

   Set the level to a lower value to generate more logs. Finest is the lowest level while Severe is the highest level.
6. Click **OK**.

About creating and importing views in XML

You can use the console to create views in the Veritas Backup Reporter, but you may find it faster and more convenient to create XML files that describe the views you want to create. You can then import the XML into Veritas Backup Reporter.

Veritas Backup Reporter provides an XML utility to import and export your XML files.

This utility resides in the following locations on the VBR Management Server host:

Solaris	`<serverInstallDir>/bin/xml.sh`
Windows	`<serverInstallDir>\util\xml.bat`

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

See "About the XML API" on page 133.

Setting the default export directory for scheduled reports

The `exportDirectoryPrefix` setting in the `vbr_conf.properties` file controls the default export path (Directory Prefix) that VBR console users see when they attempt to save scheduled reports (Settings > User Settings > Email/Export Reports > Edit).

See the *Veritas Backup Reporter User's Guide* for more information about archiving reports.

This attribute gives Veritas Backup Reporter administrators the ability to confine users to a specific export directory, preventing them from exporting the reports to any arbitrary and potentially harmful system directory. If `exportDirectoryPrefix` is not defined, then Veritas Backup Reporter defaults to whatever is defined in `web.xml`, or to the VBR Management Server temp directory.

By default, this is one of the following:

Solaris	/opt/VRTSccsvs/web/vbr/temp
Windows	\Program Files\Symantec\Veritas Backup Reporter\Server\web\vbr\temp

If the specified prefix directory is not present on the host, the VBR Management Server will create it.

To change the default export path for saving scheduled reports

1. On the VBR Management Server on which you want to change the default export path, do one of the following:

Solaris	Open a Solaris console and log in as `root`
Windows	Open a Windows command prompt and log in as an administrator or a user in the Administrators group.

2. Using a text editor, open vbr_conf.properties in the following default location for your platform:

Solaris	/opt/VRTSccsvs/conf
Windows	\Program Files\Symantec\Veritas Backup Reporter\Server\conf

3 Using your text editor, search for the following string:

```
exportDirectoryPrefix=
```

If the string is not present, add it.

4 Type a valid path that exists on the VBR Management Server.

For example on Solaris:

```
exportDirectoryPrefix=/var/reports
```

For example on Windows:

```
exportDirectoryPrefix=C:\\Shared\\Reports
```

On Windows systems, you will need to insert an extra backslash because the configuration information is stored in a Java properties file.

5 Save your changes and close vbr_conf.properties.

6 Anytime you modify vbr_conf.properties, the VBR Management Server must be restarted to commit your changes.

Windows	Use the Services application to restart the VBR Management Server.
Solaris	Type one of the following commands: ■ `/opt/VRTSccsvs/bin/vxccsvc stop` ■ `/opt/VRTSccsvs/bin/vxccsvc start`

Cleaning temporary files generated with reports

While generating a report, the system creates other related information, such as report images and html files. These temporary files are stored in the following locations on the VBR Management Server host:

Solaris	`<serverInstallDir>/web/vbr/temp/reports`
Windows	`<serverInstallDir>\server\web\vbr\temp\reports`

With each new report, the size of the `reports`directory increases. Veritas Backup Reporter 6.0 provides a means to periodically delete the temporary files and clean the `reports` directory. The Report Clean Up Schedule is shipped with default settings, which runs internally and deletes all temporary files that are generated in the `reports` directory.

The `application.properties` file contains the location of the `reports`directory.

Note: Only temporary files that are older than a day are deleted.

The administrator can edit the Report Clean Up Schedule.

To edit the Report Clean Up Schedule

1. Log on to the VBR Management Server, on which you have administrator-level privileges.
2. In the console, click **Settings**.
3. On the Settings tab, click **Schedules**.
4. Select the check box in front of Report Clean Up Schedule.
5. Click the Edit icon.
6. Edit schedule or recurrence pattern as required.
7. Click `Save`.

Warning: Do not delete the Report Clean Up Schedule.

Configuring authentication for multiple Veritas products

If you have installed the Web servers of multiple Veritas products on different hosts, you must configure the Symantec Product Authentication Service to allow the authentication brokers to exchange information. Configuring these authentication broker trusts allows cross-product linking in the VBR console without additional user logins.

Using the Symantec Product Authentication Service command-line interface, `vssat`, you can set up trust relationships between each pair of hosts.

Note: You must perform this procedure for each pair of hosts. For example, if you have Veritas Backup Reporter installed on host A, NetBackup Operations Manager (NOM) installed on host B, and Command Central Storage installed on host C, perform this procedure three times, once for the A-B pair, again for the B-C pair, and a third time for the C-A pair.

Table 7-1 lists the Veritas product component for which you must set up trusts.

Table 7-1 Veritas product components (trust relationships)

Veritas product	Product component host on which to establish trust
NetBackup Operations Manager	NOM Management Server
Veritas Backup Reporter	VBR Management Server
CommandCentral Storage	CommandCentral Storage Web Engine

To set up trust relationships between Veritas Backup Reporter authentication brokers on different hosts

1 On the Veritas product host on which you want to set up a trust relationship (see Table 7-1), do one of the following:

Solaris	Open a Solaris console and log in as `root`
Windows	Open a Windows command prompt and log in as an administrator or a user in the Administrators group .

2 Change to the Symantec Product Authentication Service CLI (vssat) directory.

By default this is:

Solaris	/opt/VRTSat/bin
Windows	\Program Files\Veritas\Security\Authentication\bin

3 Type the following command, and then press **Enter**:

```
vssat setuptrust -broker remoteHost:2821 -securitylevel low
```

where <remoteHost> is either a host name, qualified domain host name, or host IP address of the remote host with which you are establishing the trust.

The entry 2821 is the registered port number for Symantec Product Authentication Service.

4 Repeat 1–3 for the second host.

To view a list of hosts trusted by the local host

- On the appropriate Veritas product host (see earlier table) on which you have administrator privileges, type the command appropriate for the operating system, and then press **Enter**:

Solaris	/opt/VRTSat/bin/vssat showalltrustedcreds
Windows	\Program Files\Veritas\Security\Authentication\bin\vssat showalltrustedcreds

After removing a trust, you must restart Symantec Product Authentication Service, before the changes take effect.

To remove trust relationships between Veritas authentication brokers

1. On the Veritas product host (see earlier table) on which you want to remove a trust relationship,

Solaris	Open a Solaris console and log in as `root`
Windows	Open a Windows command prompt and log in as an administrator or a user in the Administrators group.

2. Change to the Symantec Product Authentication Service CLI (vssat) directory.

   By default this is:

Solaris	/opt/VRTSat/bin
Windows	\Program Files\Veritas\Security\Authentication\bin

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

   `vssat removetrust -broker remoteHost:2821`

   where `<remoteHost>` is either a host name, qualified domain host name, or host IP address of the remote host with which you are establishing the trust.

   The entry 2821 is the registered port number for Symantec Product Authentication Service.

4 Repeat 1–3 for the second host.

5 Restart the VBR Management Server on the hosts on which you removed the trusts:

Solaris	/opt/VRTSccsvs/bin/vxccsvcweb restart
Windows	Using the Windows Services application, restart the VBR Management Server.

Managing VBR Management Server SSL certificates

The VBR Management Server uses Secure Sockets Layer (SSL) to communicate with Web browser clients. The keystore certificate with which the Web Engine ships causes your Web browser to display a security alert. You can delete this certificate and generate one appropriate for your site.

When serving content over the secure port, the VBR Management Server presents a self-signed SSL certificate (issued by Veritas) to the browser. Unless you generate a new certificate, your Web browser displays a security alert.

Note: Certificate management commands are available only via the command-line interface. Commands that modify the certificate require a Server restart.

Viewing SSL certificate information

You can view SSL certificate information.

To view information about the configured SSL certificate

- Run the following command on the computer where the VBR Management Server is installed:

```
%VRTSWEB_HOME%\bin>webgui cert display
```

where the default locations for `%VRTSWEB_HOME%` are as follows:

Solaris	`/opt/VRTSweb`
Windows	`C:\Program Files\VERITAS\VRTSweb`

Creating a self-signed SSL certificate

You can create a self-signed SSL certificate.

To create a custom self-signed SSL certificate for VBR Management Server and the CommandCentral Storage Web Engine

- Run the following interactive command on the system where the VBR Management Server is installed:

  ```
  %VRTSWEB_HOME%\bin>webgui cert create
  ```

  The command guides you through the process of creating a new certificate.

  ```
  Please answer the following questions to create a self-signed
  certificate.

  This is required to enable the HTTPS protocol for the web server.

  ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

  With what hostname/IP will you access this web server?
  [thor106]:thor106

  What is the name of your organizational unit?
  [Unknown]:Engineering

  What is the name of your organization? [Unknown]:Your Company

  What is the name of your City or Locality? [Unknown]: Mountain
  View

  What is the name of your State or Province? [Unknown]:California

  What is the two-letter country code for this unit? [Unknown]:US

  Is CN=thor106, OU=Engineering, O=Your Company, L=Mountain View,

  ST=California, C=US correct? [no]:yes

  Certificate created successfully
  ```

  You must restart the server for the new certificate to take effect.

Exporting an SSL certificate to a file

You can export the public key associated with an SSL certificate to a file. This key can then be imported into other applications that will trust the VBR Management Server instance.

To export an SSL certificate to a file

- Run the following command on the system where the VBR Management Server is installed:

  %VRTSWEB_HOME%\bin>webgui cert export<cert_file>[rfc]

  If the VBR Management Server SSL certificate does not exist, the command prompts you to create one. If you specify the RFC option, the key output is encoded in a printable format, defined by the Internet RFC 1421 standard.

  For example:

  ```
  %VRTSWEB_HOME%\bin> webgui cert export C:\myapp\vrtsweb.cer rfc
  ```

Configuring a CA-signed SSL certificate

By default, VBR Management Server presents a self-signed SSL certificate every time you access VBR Management Server over the SSL port. You can install a certificate signed by a Certificate Authority (CA) like Verisign.com or Thawte.com.

To configure a CA-signed SSL certificate

1. If you do not have a self-signed certificate with information that can be verified by the CA, create one.

   %VRTSWEB_HOME%\bin>webgui cert create

   See "Creating a self-signed SSL certificate" on page 91.

2. Generate a Certificate Signing Request (CSR) for the certificate by running the following command on the system where VBR Management Server is installed:

   %VRTSWEB_HOME%\bin>webgui cert certreq <certreq_file>

   where <certreq_file> specifies the file to which the CSR will be written. The file is written using the Public-Key Cryptography Standard PKCS#10.

   For example:

   ```
   %VRTSWEB_HOME%\bin> webgui cert certreq c:\myapp\vrtsweb.csr
   ```

3. Submit the CSR to a certification authority, who will issue a CA-signed certificate.

4 Import the CA-issued certificate to VBR Management Server by running the following command on the system where VBR Management Server is installed:

%VRTSWEB_HOME%\bin>webgui import <ca_cert_file>

where `<ca_cert_file>` represents the certificate issued to you by the certification authority.

For example:

```
%VRTSWEB_HOME%\bin>webgui cert import c:\myapp\vrtsweb.cer
```

Note that the import command fails if the CA root certificate is not a part of the trust store associated with the VBR Management Server. If the command fails, add the CA root certificate to VBR Management Server trust store:

%VRTSWEB_HOME%\bin>webgui cert trust ca_root_cert_file

For example:

```
%VRTSWEB_HOME%\bin>webgui cert trust c:\myapp\caroot.cer
```

Once the certificate used to sign the CSR is added to the VBR Management Server trust store, you can import the CA-assigned certificate into VBR Management Server.

5 Restart VBR Management Server:

%VRTSWEB_HOME%\bin>webgui restart

About cloning SSL certificates

You can clone the VBR Management Server SSL keypair into a keystore and use the cloned VBR Management Server and the Web Engine certificate for another application or Web server. Visit http://java.sun.com for more information about keystores.

```
%VRTSWEB_HOME%\bin> webgui cert clone <keystore> <storepass> <alias>
<keypass>
```

If a clone keystore exists, the command renames it to keystore.old. If the VBR Management Server SSL certificate does not exist, the command prompts you to create one.

For example:

```
%VRTSWEB_HOME%\bin>webgui cert clone
c:\myapp\myserv.keystoremystorepass myalias mykeypass
```

Appendix A

Command and configuration file reference

This appendix includes the following topics:

Command and configuration file locator

Veritas Backup Reporter (VBR) provides commands that you can run from a UNIX shell or a command prompt (Windows), as well as configuration files that are integral to its operation. This section lists the VBR commands and configuration files in alphabetical order.

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

The following table maps the VBR command and configuration file with its respective VBR host and default installation directory:

Table A-1 VBR commands and configuration file locations

File	Default Locations
vbr_conf.properties	VBR Management Server: /opt/VRTSccsvs/conf \Program Files\Symantec\Veritas Backup Reporter\Server\conf

Table A-1 VBR commands and configuration file locations *(continued)*

File	Default Locations
eventposter	VBR Management Server: /opt/VRTSccsvs/bin/goodies \Program Files\Symantec\Veritas Backup Reporter\Server\util
jobutility	VBR Management Server: /opt/VRTSccsvs/bin/goodies \Program Files\Symantec\Veritas Backup Reporter\Server\util
runstoredquery	VBR Management Server: /opt/VRTSccsvs/bin/goodies \Program Files\Symantec\Veritas Backup Reporter\Server\util
support	VBR Management Server: /opt/VRTSccsvs/bin \Program Files\Symantec\Veritas Backup Reporter\Server\util VBR Agent: /opt/VRTSccsva/bin \Program Files\Symantec\Veritas Backup Reporter\Agent\bin
xml	VBR Management Server: /opt/VRTSccsvs/bin \Program Files\Symantec\Veritas Backup Reporter\Server\util
agentauth	VBR Agent: /opt/VRTSccsva/bin \Program Files\Symantec\Veritas Backup Reporter\Agent\bin

Table A-1 VBR commands and configuration file locations *(continued)*

File	Default Locations
xml	VBR Management Server: /opt/VRTSccsvs/bin \Program Files\Symantec\Veritas Backup Reporter\Server\util
agentauth	VBR Management Server: /opt/VRTSccsvs/bin
dbbackup	VBR Agent: /opt/VRTSccsva/bin \Program Files\Symantec\Veritas Backup Reporter\Agent\bin
vxccsvc	VBR Management Server: /opt/VRTSccsvb/bin
vxccsvcagent	VBR Management Server: /opt/VRTSccsvs/bin

vbr_conf.properties

`vbr_conf.properties` – a general purpose configuration file for the VBR Management Server.

DESCRIPTION

`vbr_conf.properties` is a general purpose configuration file for the VBR Management Server. For VBR installations made highly available against system failure on a clustered network, `vbr_conf.properties` should contain Symantec Product Authentication Service settings that identify the broker host.

OPTIONS

authentication.services.broker.host=*hostname*

The fully-qualified host name of the Symantec Product Authentication Service broker host or the fully-qualified DNS name for the virtual IP or the cluster name of the Symantec Product Authentication Service broker host.

authentication.services.broker.port=*port*

The port for the Symantec Product Authentication Service broker host that the VBR Management Server connects to. By default, Symantec Product Authentication Service listens to port 2821.

authentication.services.domain.suffix=*brokerHostName*

Modifies the Symantec Product Authentication Service broker host name in situations when the VBR Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are not fully qualified in Symantec Product Authentication Service.

*brokerHostName*is either the Symantec Product Authentication Service broker host cluster name or the Symantec Product Authentication Service broker fully qualified host name.

authentication.broker.domain.conf.file=*domainBrokerMappingPathname*

Used when the VBR Management Server is clustered or when the Symantec Product Authentication Service broker is on a host remote from the VBR Management Server host.

Path and filename for the file that maps Veritas Backup Reporter domains to their brokers. By default, *domainBrokerMappingPathname* is:

`/opt/VRTSccsvs/conf/domain_broker.txt`

exportDirectoryPrefix=*path*

Controls the default export path (Directory Prefix) that VBR console users see when they attempt to save scheduled reports. If the specified prefix directory is not present on the host, the VBR Management Server will create it.

corba.external.ip=*port*

Identifies the actual public IP address (the “natted” address) for the VBR Management Server, when a firewall is configured to act as a Network Address Translation (NAT) device to route packets to hidden addresses behind the firewall.

bram.corba.port=*port*

The port that the VBR Management Server uses to communicate with the Veritas Alert Manager Object Request Broker (ORB). (The default is 5431.)

internal.trap.receiver.enabled=TRUE|FALSE , vxtrapd.enabled=TRUE|FALSE

Controls which trap processor the VBR Management Server uses to receive SNMP traps: the Veritas Trap Processor (`vxtrapd`) and a second, internal trap receiver. Only one of the trap processors can be used (TRUE) at a time.

NOTES

`vbr_conf.properties` resides by default in: /opt/VRTSccsvs/conf (Solaris) and \Program Files\Symantec\Veritas Backup Reporter\Server\conf

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

`vbr_conf.properties` uses the standard Java properties file format. Each option inside the file must begin on a new line.

On Windows systems, you will need to insert an extra backslash.

For example on Windows:

```
exportDirectoryPrefix=C:\\Shared\\Reports
```

To get a list of private domains known to the Symantec Product Authentication Service, type this command on a VBR Management Server:

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

EXAMPLES

EXAMPLE 1: The following is an example of a `vbr_conf.properties` entry:

```
authentication.services.broker.host=myhost.example.com
authentication.services.broker.port=2821
authentication.broker.domain.conf.file=/opt/VRTSccsvs/conf
 /domain_broker.txt
authentication.services.domain.suffix=myhost.example.com
```

EXAMPLE 2: The following example is a `vbr_conf.properties` entry, when the VBR Management Server is made highly available with clustering software (such as Veritas Cluster Server). When the VBR Management Server is clustered, authentication.services.domain.suffix is the Symantec Product Authentication Service broker host cluster name:

```
authentication.services.broker.host=myhost.example.com
authentication.services.broker.port=2821
authentication.services.domain.suffix=ccservicecluster
authentication.broker.domain.conf.file=/opt/VRTSccsvs/conf
 /domain_broker.txt
```

EXAMPLE 3: The following example is a `vbr_conf.properties` entry, when one or more of the Veritas Backup Reporter private domains is not fully qualified in Symantec Product Authentication Service:

```
authentication.services.broker.host=myhost.example.com
authentication.services.broker.port=2821
authentication.services.domain.suffix=myhost.example.com
authentication.broker.domain.conf.file=/opt/VRTSccsvs/conf
 /domain_broker.txt
```

SEE ALSO

agentauth

vxccsvc

eventposter

`eventposter` – a Veritas Backup Reporter utility that allows you to post alerts to the VBR Console Alerts Summary

SYNOPSIS

```
eventposter -server -port -usr -passwd -domainName -domainType
-severity -summary -node [-agent|-ip
|-alertGroup|-alertKey|-otherInfo1|-otherInfo2|-eventTime|-notify]
```

DESCRIPTION

`eventposter` is a Veritas Backup Reporter utility that allows you to post alerts to the VBR Console Alerts Summary (Monitoring tab).

OPTIONS

-server *`serverName`*

(Required) Name of the VBR Management Server host you want to connect to.

-port *`number`*

(Required) Server port to use for the connection. The default port is `1556`.

-usr *`userName`*

(Required) The valid username for the Server login credentials.

-passwd *`password`*

(Required) The valid password for the Server login credentials.

-domainName *`domainName`*

(Required) The domainName for the Server login credentials.

-domainType *`domainType`*

(Required) The type of domain against which to authenticate the Server login credentials.

Valid domains are: `nis`, `nt`, `vx`, or a user-defined Symantec Product Authentication Service-authenticated domain.

-severity *`severityLevel`*

(Required) Severity of the event.

`severityLevel` must be an integer, 1-5 that represent the following on the event console:

5 - critical, 4 - error, 3 - warning, 2 or 1 - info

-summary *"string"*

(Required) Text that displays in the summary field. *string* must be an exact match and enclosed in quotes.

-node *nodeName*

(Required) Node name on which the events occurred. The VBR Management Server will attempt to match this alert against Veritas Backup Reporter's business views based on this value.

-agent *agentName*

VBR Agent on which the events occurred.

-ip *IPAddress*

(Optional) IP address on which the events occurred.

IPAddress must be a valid IP address.

-alertGroup *groupName*

(Optional) Alert group to which the events belong, that is, failure, partial success.

-alertKey *key*

(Optional) Alert key to which the events belong, usually used for error code information.

-otherInfo1 *fieldName*

(Optional) Custom field for extra information.

-otherInfo2 *fieldName*

(Optional) Custom field for extra information.

-eventTime *time*

(Optional) Time (in milli-seconds) that the event occurred.

The valid format is a number.

-notify true | false

(optional) `true` or `false`; (replaces sendTrap parameter in version 3.5) internally sets different alert types - you can configure notification (that is, SNMP traps, email, write to the system log, perform commands through a policy on the Server). If set to `true`, the type is set against `Event Poster - Notify`, otherwise, against `Event Poster – No Notify`.

NOTES

`eventposter` resides by default in /opt/VRTSccsvs/bin/goodies (Solaris). The Windows version is named `eventposter.bat` and resides in \Program Files\Symantec\Veritas Backup Reporter\Server\util

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

EXAMPLE

The following example demonstrates posting of an alert that will have a severity of three, will be in the Failure alert group, and contain the string, "Error Occurred:". It will be created against the alert type `Event Poster - Notify` that can be defined through a policy on the VBR Management Server to send traps, emails, write to system log, or perform commands:

```
eventposter -server myServer -port 1556 -usr admin -password mypswd
-domainName myDomain -domainType nt -agent myAgent -node myNode -ip
127.0.0.1 -alertGroup Failure -severity 3 -otherInfo1 23 -otherInfo2
31s -Summary "Error Occurred" -notify true
```

SEE ALSO

jobutility

jobutility

`jobutility` – a VBR script used to report on backup job activity residing in the VBR database.

SYNOPSIS

(Optional)

`jobutility.sh [--host hostName] --server serverName --port portNumber --usr username--passwd password--domain domainName--domaintype domainType`

DESCRIPTION

`jobutility` is a script that queries the VBR database and reports on backup activity.

OPTIONS

--host *hostName*

Name of the host for which you want backup job information. (Use the host name only, not the host IP address or qualified host name.)

Omit the `--host` option if searching over all backup jobs.

--server *serverName*

Name of the VBR Management Server host to which you want to connect.

--port *portNumber*

Port number to use to connect to the specified Server. The default is 1556.

--usr *username*

A valid user account with which to connect to the specified Server.

--passwd *password*

The password for the specified username used to connect to the Server.

--domain *domainName*

Name of the network domain of which the specified user account is a member.

The default is the private domain name (`cc_users`).

--domaintype *domainType*

The type of network domain specified: NIS, NT, or a private domain. Valid entries are: `nis`, `nt`, or `vx`.

The default is private domain (`vx`).

NOTES

If you specify `host`*`hostName`*, then `jobutility.sh` outputs information about the *`hostName`*'s first and last backup job. If you specify no `host` *`hostName`* option, then `jobutility.sh` outputs information about the first and last job (across all hosts) in the database.

To display a help page listing script options and a brief description for each, specify no options when running `jobutility.sh`.

`jobutility.sh` resides by default in /opt/VRTSccsvs/bin/goodies (Solaris). The Windows version is named `jobutility.bat` and resides in \Program Files\Symantec\Veritas Backup Reporter\Server\util

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

EXAMPLE

When you use the following command:

```
jobutility --usr Administrator --pass mypaswd --server myHost --port
1556 --domain cc_users@myHost.myCompany.com --domaintype nis
```

returns output similar to the following:

```
------------------------------------------------------------------------
SubJob Information (Entry for Each SubJob)
------------------------------------------------------------------------
Directory/Filesystem Name :
Primary ID                :
Size                      :
File Count                :
Management Groups         :
------------------------------------------------------------------------
Attempt Information (Entry for Each Attempt)
------------------------------------------------------------------------
Attempt Sequence          :
Secondary ID              :
Throughput                :
Size                      :
File Count                :
Status                    :
Status Code               :
```

```
Start Time                :
Finish Time               :
------------------------------------------------------------------------
Finished Job Information
------------------------------------------------------------------------
Primary Id          :
Secondary Id        :
Client Name         :
Client ProductID    :
Master Server Name  :
Media Server Name   :
Product Name        :
Product Version     :
Agent Host          :
Job Type            :
Level               :
Throughput          :
Total Size          :
Try Count           :
File Count          :
Status              :
Status Code         :
Start Time          :
Finish Time         :
Expiration Time     :
Policy Domain name  :
Policy Name         :
Policy Keyword      :
Schedule Name       :
```

SEE ALSO

eventposter

runstoredquery

runstoredquery

`runstoredquery` – a VBR script used to run queries created with the Saved Query Tool in the VBR console.

SYNOPSIS

```
runstoredquery.sh -qid
queryID [-filetype {htm} | {csv [-noheader]}]
```

DESCRIPTION

`runstoredquery.sh` is a VBR script you can use to run custom SQL queries of VBR's database of logged events, backup jobs, media usage, and change requests. The custom query is first created with the Saved Query Tool in the VBR console. runstoredquery.sh outputs the data to the Solaris console, or as HTML or comma-delimited format (CSV) files. As with most shell scripts, you can schedule runstoredquery.sh and email its output. (For more information, see your Solaris documentation for the `cron` and `mail`/`mailx` commands.)

OPTIONS

-qid *queryID*

Specifies the query ID for the custom query you want to run.

queryID must be a valid identifier for the custom query created with the Saved Query Tool. For more information, refer to the *Veritas Backup Reporter User's Guide*.

-filetype htm | csv

Specifies the type of output runstoredquery.sh generates. `htm` causes runstoredquery.sh to output the query in HTML format. `csv` causes runstoredquery.sh to output the query in comma-delimited format.

-noheader

Applies to `-filetype csv` only. Causes runstoredquery.sh to create the comma-delimited file without a heading line. (`-noheader` can be useful for customers who want to import the script output into an external billing application without having to manually remove the header line.)

NOTES

If you execute runstoredquery.sh without the `-filetype` option, runstoredquery.sh outputs to the Solaris console.

You specify the output file and path with the Saved Query Tool in the VBR console.

runstoredquery.sh resides by default in /opt/VRTSccsvs/bin/goodies (Solaris). The Windows version is named `runstoredquery.bat` and resides in \Program Files\Symantec\Veritas Backup Reporter\Server\util

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

EXAMPLES

EXAMPLE 1:

The following example displays to a Solaris console the results from query ID 7:

```
sh runstoredquery.sh -qid 7
```

EXAMPLE 2:

This example causes `runstoredquery.sh` to output query ID 7 in HTML format:

```
sh runstoredquery.sh -qid 7 -filetype htm
```

The output path and filename is defined when the query is created.

EXAMPLE 3:

This command outputs query ID 7 in comma-delimited (CSV) format:

```
sh runstoredquery.sh -qid 7 -filetype csv
```

SEE ALSO

jobutility

support

`support` – a script used for collecting Veritas Backup Reporter data used by Veritas Technical Support in troubleshooting. You can also use support for running EMC Legato Networker Command-Line Interfaces (CLIs). Detailed information is collected for the following agent modules: EMC Legato Networker, and Veritas NetBackup.

SYNOPSIS

`support [ options]`

DESCRIPTION

`support` is a script used for collecting Veritas Backup Reporter data used by Veritas Technical Support in troubleshooting. You can also use support for running EMC Legato Networker Command-Line Interfaces (CLIs). `support` produces a compressed file with the following types of information: log files, VBR Management Server and Agent configuration files, and Veritas NetBackup Command-Line Interface (CLI) summaries.

OPTIONS

-s [true|false]
: Include VBR Management Server information.

-a [true|false]
: Include Agent information.

-c [true|false]
: Include View Builder information.

-f *filename*
: Compresses output (zip format) to *.filename*

-d *directoryName*
: Overrides the default directory where `support` writes its compressed output file and its log.

  If the specified directory does not exist, `support` terminates.

-noconsole
: Do not log to console.

  The created zip file will have the machine's hostname in the name: `support-`*hostName*

-h

Displays help information for `support`.

NOTES

`support` resides on the VBR Management Server, Agent, and View Builder host in the following locations by default:

VBR Management Server:`/opt/VRTSccsvs/bin`

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

VBR Agent:

`/opt/VRTSccsva/bin`

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

View Builder:

`/opt/VRTSccsvb/bin`

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

The Windows version is named: `support.exe`

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

Unless changed with the `-f` and`-d` options, support compresses its output to the following default path and filename:

Solaris	`/var/tmp/support-`*`hostname`*`.zip`
Windows	`\Documents and Settings\`*`username`*`\Temp\support-`*`hostname`*`.zip`

EXAMPLE

The following examples show output similar to what you see when you run `support`. The first three lines are for the three major components of Veritas Backup Reporter. After that, if the VBR Agent is installed, you are given a menu of all your configured Veritas NetBackup Agent modules, and you can select whichever modules you are troubleshooting.

EXAMPLE 1:

The following input and output is representative of an interactive session where the user has specified `support` to collect information for all three Veritas Backup Reporter components and one configured Veritas NetBackup Agent module:

```
C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util>support.exe
Do you want to include server information (yes/y/no/n)[yes]?y
Do you want to collect data from the DB (must be running) (yes/y/no/n)[yes]
Do you want to include agent information (yes/y/no/n)[yes]?y
Do you want to include agent module information (yes/y/no/n)[yes]?y
Please select the module(s) for which you wish to collect debugging informa

  0) VERITAS BackupExec on server1.domainname.com
  1) VERITAS BackupExec on server2.domainname.com
  2) VERITAS BackupExec on server3.domainname.com
  3) VERITAS NetBackup on server4.domainname.com
  4) Select All
  5) Commit Selection
?:2
Please select the module(s) for which you wish to collect debugging informa

  0) VERITAS BackupExec on server1.domainname.com
  1) VERITAS BackupExec on server2.domainname.com
  2) VERITAS BackupExec on server3.domainname.com [SELECTED]
  3) VERITAS NetBackup on server4.domainname.com
  4) Select All
  5) Commit Selection
?:5
Do you want to include view builder information (yes/y/no/n)[yes]?y
Gathering server logs...
        Added 19 log files from the server
Gathering server configuration...
        Added Web-App configuration file from the server
Gathering agent listing...
Gathering CCSvc DB data..
Connecting to DB on localhost:2994 ...
ran 23 queries from properties file.
ran 0 queries from disk.
Disconnecting from DB localhost ...
Gathering CCSvc DB data complete.
Gathering agent logs...
Agent log directory is :C:\Program Files\Symantec\Veritas Backup Reporter\A
logs
```

```
        Added 14 log files from agent directory
Gathering agent configuration...
        Added 1 agent configuration files.
Gathering agent listing...
Collecting VERITAS BackupExec Agent Module data for server3.domainname.com..
.
Gathering view builder logs...
Gathering agent listing...
Gathering install/uninstall logs...
Gathering agent version...
Picking up log file.

The Veritas Backup Reporter support data has been collected and placed in:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\support-host.zip
Please send it to your Symantec contact.



Collector Successful

C:\Program Files\Symantec\Veritas Backup Reporter\Server\Util>
```

EXAMPLE 2:

The following input and output is representative of an interactive session where the user has specified `support` to collect information for all three VBR components and no configured Veritas NetBackup Agent module:

```
Do you want to include server information (yes/y/no/n)[yes]?
Do you want to include agent information (yes/y/no/n)[yes]?
Do you want to include agent module information (yes/y/no/n)[yes]?
No Agent Modules were found...
Do you want to include view builder information (yes/y/no/n)[yes]?
Gathering server logs...
  Added 26 log files from the server
Gathering server configuration...
  Added configuration files from the server
Gathering agent listing...
Gathering agent logs...
Agent log directory is :C:\Test Directory\Veritas Products\
Veritas Backup Reporter\Service\Agent\logs
  Added 4 log files from agent directory
Gathering agent configuration...
  Added 1 agent configuration files.
```

```
Gathering agent listing...
No valid modules were executed.
Gathering view builder logs...
No Client log file found.
Gathering agent listing...
Gathering install/uninstall logs...
Gathering agent version...
Picking up log file.

The Veritas Backup Reporter support data has been
collected and placed in:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\support-host.zip
Please send it to your Symantec contact.
```

xml

`xml` – a script used to import and export object views to and from VBR Management Servers.

Synopsys

```
xml {-I | -e} {-f filename [--hosthostname] [--port port] --usr
username [--pass password] --domaindomainName --domaintype domainType
[--broker brokerHostname] [--brokerport port] [-v errorLevelNumber
] [-l logFilename]}
```

Description

`xml` is a script used to import and export object views to and from VBR Management Servers.

Options

-I
: Import XML mode.

-e
: Export XML mode.

-f *filename*
: Name of the XML file to use for import or export.

--host *hostname*
: (Optional) name of the VBR Management Server you want to connect to. *Hostname* can be either a hostname, IP address, or a fully qualified domain name. For example: `myHostname`, `0.0.0.0`, or `myhost.example.com`

  If no *Hostname* is supplied, the script defaults to the local host.

--port *port*
: (Optional) the port for the VBR Management Server you are connecting to. If no *port* is specified, the script uses port 1556.

--usr *username*
: The user account name used for authenticating your connection to the VBR Management Server host. Specify a system account valid for the host you are connecting to.

--pass *password*

The user account password used for authenticating your connection to the VBR Management Server host.

`xml` checks for the stored password in its first attempt to connect to the VBR Management Server. If the password is not present, then re-run `xml` and supply the password for the specified account.

--domain *domainName*

The name of the domain to which the user belongs (default, `cc_users`) and that the Symantec Product Authentication Service uses to authenticate users.

--domaintype *domainType*

The type of the domain to which the specified user belongs. Valid domain types are: `nis`, `nt`, or `vx` (default).

--broker *brokerHostname*

(Optional) the name of the Symantec Product Authentication Service broker host. The default is the VBR Management Server host.

-brokerport *port*

(Optional) the port for the Symantec Product Authentication Service broker host you are connecting to. If no *portNumber* is specified, the script uses port 2821.

---select *options*

(Optional) object selection options that can be the following: view (`view=`*name*), object name (`objname=`*name*), object type (`objname=`*name*), object ID (`objid=`*name*).

-v *errorLevelNumber*

(Optional) turns logging on (default) and off and controls the type of errors that the script outputs.

ErrorLevelNumber is a number 0-8, whose meaning is described below:

0—(Off)

1—Severe

2—Warning

3—Info

4—Config

5—Fine

6—Finer

7—Finest

8—All error messages

-l *logFilename*

(Optional) a log file that the XML script creates to capture script error messages. By default, logging is on and outputs to the console or command prompt. *logFilename* can be any valid filename. The script writes the log file to the current directory.

Notes

`xml` resides by default in: /opt/VRTSccsva/bin (Solaris only). Its Windows counterpart (`xml.bat`) resides by default in: \Program Files\Symantec\Veritas Backup Reporter\Server\util

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

Examples

EXAMPLE 1:

In the following example, `xml` selects the `tape_drive` object in the `backup_view` to export to a file in `/var` named `export.xml`. Logging is turned on and outputs to the operating system console or command prompt for all error levels:

```
xml.bat -e -f /var/export.xml --host myhost1.example.com
 --usr admin --pass
password --domain cc_users@myhost1.example.com --domaintype vx
 --select
view=backup_view;objname=tape_drive --l backup_view_export.log
 -v 8
```

EXAMPLE 2:

In the following example, `xml` imports an object view (`export.xml`) to a VBR Management Server host (`myhost2`). Logging is turned off:

```
xml --host myhost2.example.com --usr admin
 --pass password --domain
cc_users@myhost2.example.com --domaintype vx -I -f /var/export.xml
 -v 0
```

See also

vxccsvcbuilder

vxccsvc

agentauth

`agentauth` – authenticates the VBR Agent with the Symantec Product Authentication Service.

Synopsys

```
agentauth { [password] -server serverHostName [-port port] [{
-brokerhost brokerhostName [-brokerport port] [-domainnamesuffix
brokerHostName] }] | h
```

Description

`agentauth` authenticates the VBR Agent with the Symantec Product Authentication Service (SPAS).

Options

password

(Optional) password associated with the account used by SPAS to authenticate the VBR Agent. Required only when this internal account (`ccsvc_agent`) has been changed.

-server *serverHostName*

(Required) name of the VBR Management Server against which you are authenticating the VBR Agent.

serverHostName should be the fully qualified host name, or in clustered situations, the cluster name. If no serverHostName is supplied, `agentauth` defaults to the local host.

-port *port*

(Optional) port number on the VBR Management Server used to connect with the VBR Agent. (The default port is 1556.)

-brokerhost *brokerHostname*

The fully qualified host name of the SPAS broker host or the fully qualified DNS name for the virtual IP or the cluster name of the SPAS broker host.

`-brokerhost` requires `-server`

Use `-brokerhost` when the VBR Agent resides on a host other than the VBR Management Server host. Use `-brokerhost` with `-domainnamesuffix` when the VBR Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are *not* fully qualified in SPAS.

-brokerport *port*

(Optional) the port for the SPAS broker host that the VBR Management Server connects to. By default, SPAS listens to port 2821.

-domainnamesuffix *brokerHostName*

Modifies the SPAS broker host name in situations when the VBR Management Server is clustered, or when one or more of the Veritas Backup Reporter private domains are *not* fully qualified in SPAS.

`-domainnamesuffix` requires `-brokerhost` and `-server`

brokerHostName is either the SPAS broker host cluster name or the SPAS broker fully qualified host name.

-h

Displays command-line help information for `agentauth`.

Notes

`agentauth` resides by default in: /opt/VRTSccsva/bin (Solaris only). Its Windows counterpart (`agentauth.exe`) resides by default in: \Program Files\Symantec\Veritas Backup Reporter\Agent\bin

On UNIX, Veritas Backup Reporter creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

If the VBR Agent cannot connect to the VBR Management Server, a message such as the following will appear in the VBR Agent log:

```
Authentication failed
The user or password are not valid in the given domain.
Domain="ccsvc_services@myServer", User="ccsvc_agent"
```

By default, the VBR Agent logs are located:

Solaris	`/opt/VRTSccsva/logs`
Windows	`\Program Files\Symantec\Veritas Backup Reporter\Agent\logs`

The Agent should have been authenticated during installation, but could have failed for a number of reasons, including the VBR Management Server not having been started when the VBR Agent was installed.

`agentauth` can fail for a number of reasons. Below are two of the most common issues:

The SPAS libraries are not in the PATH. In this case, reboot the VBR Agent machine or specify the absolute path to the libraries:

Solaris	Update `LD_LIBRARY_PATH` to include `/opt/VRTSat/lib`
Windows	`\Program Files\Veritas\Security\Authentication\bin` `PATH` changes do not take affect over Windows Terminal Services unless you log out and back in.

The VBR Management Server cannot be connected with. Make sure the Server is running, and can be reached on port 1556.

To get a list of private domains known to the Symantec Product Authentication Service (SPAS), type this command on a VBR Management Server:

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

Examples

The following examples assume that SPAS is installed on the same machine as the VBR Management Server.

EXAMPLE 1:

The following command authenticates the VBR Agent with the Symantec Product Authentication Service (SPAS). Both the VBR Agent and the VBR Management Server reside on the same host, `VBR.example.com`:

```
agentauth mypasswd -server VBR.example.com
```

EXAMPLE 2:

The following command authenticates the VBR Agent with SPAS, when the VBR Agent is installed on a different host than the VBR Management Server (`VBR.example.com`):

```
agentauth mypasswd -server VBR.example.com -brokerhost
VBR.example.com
```

EXAMPLE 3:

The following command authenticates the VBR Agent with SPAS, when the VBR Management Server is made highly available with clustering software (such as Veritas Cluster Server). When the VBR Management Server is clustered, `-domainNameSuffix` is the SPAS broker host virtual IP, as the VBR Agent has to authenticate with the SPAS broker host using the cluster name or the virtual IP:

```
agentauth mypasswd -server ccservicecluster -brokerhost
ccservicecluster -domainNameSuffix ccservicecluster
```

EXAMPLE 4:

The following command authenticates the VBR Agent with SPAS, when the VBR private domain (`cc_users`) is not fully qualified in SPAS:

```
agentauth mypasswd -server VBR.example.com -brokerhost
VBR.example.com -domainNameSuffix VBR.example.com
```

See also

vbr_conf.properties

vxccsvcagent

dbbackup

`dbbackup` – a script used for backing up the VBR database (Solaris only).

Synopsys

`dbbackup {backupDir | -restore [restoreDir]} [-o [logfile]]`

Description

`dbbackup` is a script used for backing up the VBR database.

Options

`backupDir`

(Required) *`backupDir`* is the directory where the VBR database will be backed up to, or restored from. *`backupDir`* should be an absolute path.

restore *`restoreDir`*

(Optional) *`restoreDir`* is the directory where the VBR database will be restored. If not included, `dbbackup` restores the database to the default data directory (/var/Veritas/ccs_data). *`restoreDir`* should be an absolute path.

-o *`logfile`*

Record backup and restore actions to a log file. If *`logfile`* is unspecified, output is written to the current directory.

Notes

`dbbackup` resides by default in: /opt/VRTSccshd/bin (Solaris).

On Windows, you perform backups with the `CCDbBackup.bat` batch file.

For more information, see the *Veritas Backup Reporter Installation Guide*.

The backup script creates three files (ccsvc.db, `vxdmbulk.db`, and `ccsvc.log`) in the backup directory.

`vxdmbulk.db` is a data space file and part of the database. Data spaces are started when the main database (ccsvc.db) is started; therefore, starting and stopping the data space file is not required.

Both the Solaris and the Windows scripts automatically stop and restart the database.

On UNIX, VBR creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

Examples

EXAMPLE 1: The following command backs up the VBR database to the `my_db_backups` directory:

```
/opt/VRTSccshd/bin/dbbackup /my_db_backups
```

EXAMPLE 2: The following command restores a previously backed up VBR database to the /var/Veritas/ccs_data directory. Logging is turned on to write restore-related messages to a log. Because a log directory is not specified, the log is written to the current directory (/opt/VRTSccshd/bin):

```
/opt/VRTSccshd/bin/dbbackup/my_db_backups -restore
/data/cc_database -o
```

See also

vxccsvc

vxccsvc

vxccsvc – startup and shutdown script for all VBR Management Server and its dependencies (Solaris only).

Synopsys

vxpbx-Symantec Private Branch Exchange

vas- Symantec Product Authentication Service

vxdbms_d-Symantec Shared DBMS

bram-Veritas Backup Reporter Alert Manager

vxccsvc-Veritas Backup Reporter Server

[NULL]-All processes, stops the following processes: vxccsvc and force

force-All processes, including shared

```
vxccsvc { stop | start | status} [serverProcess]
```

Description

vxccsvc is the startup/shutdown script (Solaris only) for the VBR Management Server and one or all of its dependencies: VBR Alert Manager, VBR database, Symantec Product Authentication Service (SPAS), VBR Trap Processor, Symantec Private Branch Exchange, and the VBR Active Practices.

On Windows, use the Windows Services applet.

Options

stop [*serverProcess*]

Terminates the Server and its dependencies.

If *serverProcess* is omitted, vxccsvc terminates the VBR Management Server and Active Practices only. stop force terminates the VBR Management Server and all its dependencies (including dependencies shared with other Veritas products).

(Optional) *serverProcess* can be one of the following values: vxccsvs (VBR Management Server), vas (Symantec Product Authentication Service), vxdbms_d (Server DBMS only), bram (Alert Manager), vxtrapd (Trap Processor), pm (Active Practices), vxpbx (Symantec Private Branch Exchange), and force (use with stop only).

start [*serverProcess*]

Invokes the Server and its dependencies.

If *serverProcess* (see earlier definition) is omitted, starts the VBR Management Server and all its dependencies. Otherwise, starts only the Server process specified.

status *[serverProcess]*

Identifies whether the VBR Management Server and its dependencies are running without starting or stopping a Server process.

If *serverProcess* (see earlier definition) is omitted, displays status for all the VBR Management Server and all its dependencies. Otherwise, shows status for the Server process specified only.

Notes

`vxccsvc` can start and stop the VBR Management Server and one or all of its dependencies (shared or otherwise), while its companion script, `vxccsvcweb` only starts and stops the Server. The VBR Management Server is a Symantec Web Server application. `vxccsvc` and `vxccsvcweb` will only terminate the Web Server if no other Symantec Web Server applications are running on the host.

You can specify only one *serverProcess* argument at a time. For example, to stop two VBR Management Server dependencies, you would have to issue two separate commands. For example, the command stops the Alert Manager, and the second command stops the Symantec Product Authentication Service:`vxccsvc stop bramvxccsvc stop vas`

`vxccsvc` resides by default in: /opt/VRTSccsvs/bin (Solaris only).

On UNIX, VBR creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

On Windows, the VBR Management Server is installed as a service that starts automatically.

Examples

EXAMPLE 1:

The following command stops VBR Management Server and all its dependencies (including dependencies shared with other Veritas products):

```
vxccsvc stop force
```

EXAMPLE 2:

The following command stops the VBR Management Server and Active Practices only. The remaining VBR Management Server dependencies (see earlier list) are not stopped:

```
vxccsvc stop
```

EXAMPLE 3:

The following command stops the Trap Processor only:

```
vxccsvc stop vxtrapd
```

EXAMPLE 4:

The following command starts the VBR Management Server and all its dependencies (see earlier list):

```
vxccsvc start
```

EXAMPLE 5:

The following command starts the Veritas Database Management System only:

```
vxccsvc start vxdbms_d
```

EXAMPLE 6:

The following command indicates if the VBR Management Server and any of its dependencies are running:

```
vxccsvc status
```

See also

vbr_conf.properties

xml

vxccsvcagent

vxccsvcbuilder

vxccsvcweb

vxccsvcagent

`vxccsvcagent` – startup and shutdown script for the VBR Agent (Solaris only).

Synopsys

```
vxccsvcagent { start | stop | status | version }
```

Description

`vxccsvcagent` is the (Solaris-only) startup and shutdown script for the VBR Agent.

Options

start
: Invokes the VBR Agent.

stop
: Terminates the VBR Agent.

restart
: Stops and then starts the VBR Agent.

status
: Identifies whether the VBR Agent is running.

version
: Displays `vxccsvcagent` version and copyright information.

Notes

`vxccsvcagent` resides by default in: /opt/VRTSccsva/bin (Solaris only).

On UNIX, VBR creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

An Agent's configuration is stored in the VBR database and the Agent caches the most recent version of its configuration locally in `agent.conf`. The Agent periodically compares `agent.conf` with the one stored in the database, uses whichever is most recent, and modifies the earlier version to keep it up-to-date. If the last modified time for `agent.conf` is later than the timestamp for the configuration stored on the Server, the Agent uses the local configuration and updates the configuration stored on the Server. Otherwise, the Agent uses the

configuration stored on the Server host and overwrites the locally cached configuration.

Logging for the core agent and individual Agent explorers is administered in the same fashion but written to different log files. The core agent writes to `ccsvcAgent-core-#.log`. Individual Agent explorers write to `ccsvcAgent-<ExplorerName>-<InstanceNumber>-<ProductHost>-#.log`. Standard error output (stderr) is redirected to `ccsvcAgent-err-#.log`.

InstanceNumber is the instance identifier that was given to the module when it was configured. ProductHost is the host that the agent module is using to collect data with all periods ('.') replaced by underscores ('_').

When the log file reaches a certain maximum file size, it is rolled over (purged). The pound sign (#) in the log file name indicates the number of times that the log file has been rolled over. The lower the rollover number, the more recent the log file.

On Windows, `vxccsvcagent` is installed as a service that starts automatically.

By default, the VBR Agent logs are located:

Solaris	`/opt/VRTSccsva/logs`
Windows	`\Program Files\Symantec\Veritas Backup Reporter\Agent\logs`

See also

agentauth

vxccsvcbuilder

vxccsvcbuilder

`vxccsvcbuilder` – runs the VBR View Builder (Java) GUI.

Synopsys

```
vxccsvcbuilder [version]
```

Description

`vxccsvcbuilder` runs the VBR View Builder GUI—a Java application in which an administrator creates, modifies, and manages access to object views that users see in the VBR Console. VBR also ships with a Flash-based View Builder.

For more information, see "Managing Veritas Backup Reporter Views."

Options

version
: Displays `vxccsvcbuilder` version and copyright information.

Notes

vxccsvcbuilder resides by default in: /opt/VRTSccsva/bin (Solaris only).

On UNIX, VBR creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's `PATH` environment variable to avoid having to change directory in order to run the VBR command or script.

On Windows, you access the View Builder from either the VBR Console or directly from the Windows Start menu.

See also

vxccsvcagent

vxccsvc

vxccsvcweb

vxccsvcweb – startup and shutdown script for the VBR Management Server.

Synopsys

```
vxccsvcweb start | stop | restart | status | version
```

Description

vxccsvcweb is the (Solaris-only) startup and shutdown script for the VBR Management Server.

Options

start
: Invokes the VBR Management Server.

stop
: Terminates the VBR Management Server.

restart
: Stops and then starts the VBR Management Server.

status
: Identifies whether the VBR Management Server is running.

  status does *not* report on any processes on which the Server is dependent.

version
: Displays vxccsvcweb version.

Notes

vxccsvcweb can start and stop the VBR Management Server only, while its companion script, vxccsvc can start and stop the Server and one or all of its dependencies (shared or otherwise). The VBR Management Server is a Symantec Web Server application. vxccsvc and vxccsvcweb will only terminate the Web Server if no other Symantec Web Server applications are running on the host.

vxccsvcweb resides by default in: /opt/VRTSccsvs/bin (Solaris only).

On UNIX, VBR creates symbolic links to all its scripts and commands in the /opt/VRTS/bin directory at installation. Add /opt/VRTS/bin to your host's PATH environment variable to avoid having to change directory in order to run the VBR command or script.

On Windows, the VBR Management Server is installed as a service that starts automatically.

See also

xml

vxccsvc

vxccsvcagent

vxccsvcbuilder

Appendix B

XML interface reference

This appendix includes the following topics:

About the XML API

You can create views in the Veritas Backup Reporter (VBR) by creating and importing XML files that describe the views.

With the Veritas Backup Reporter XML API, IT asset data and their relationships that you maintain through in-house or third-party systems (for example, Peregrine AssetCenter) can be imported into Veritas Backup Reporter. The XML import capability enables you to import arbitrary groupings of hosts and file systems, for example, groupings defined around business units. For example, you might use a spreadsheet to define Host A as the marketing host and Host B as the sales host. Using the XML import feature, you can import the data, create a view into that data, and charge back services based upon business units.

As another example, you might want to build a view of a chart of accounts showing server ownership by company department for chargeback purposes. With large enterprises, the chart of accounts can easily exceed a thousand. Having to re-key this data into Veritas Backup Reporter is cumbersome and error-prone. Importing this data directly from your native systems is much more efficient and allows the maintenance of the data to continue in the upstream (native) system while Veritas Backup Reporter is refreshed with the changes.

Importing using the XML API offers a clean and efficient example of Veritas Backup Reporter's open architecture that enables integration with other systems.

About the XML DTD

The XML DTD is constructed as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT application (objects?,view*,user*,mergeitems*)>1
 <!ATTLIST application version CDATA #REQUIRED>
<!ELEMENT objects (object+)>
<!ELEMENT view (node*,aliaslevels?)>
 <!ATTLIST view identifier CDATA #REQUIRED>
 <!ATTLIST view action (add|delete|update|declare) "declare">
 <!ATTLIST view id ID #IMPLIED>
<!ELEMENT object (attribute*)>
 <!ATTLIST object id ID #IMPLIED>
 <!ATTLIST object name  CDATA #IMPLIED>
 <!ATTLIST object action (add|delete|update|declare) "declare">
 <!ATTLIST object type CDATA #IMPLIED>
 <!ATTLIST object master IDREF #IMPLIED>
 <!ATTLIST object dbid CDATA #IMPLIED><!ELEMENT node (object?,node*)>
 <!ATTLIST node id ID #IMPLIED>
 <!ATTLIST node action (add|delete|declare) "declare">>
 <!ATTLIST node object IDREF #IMPLIED>
 <!ATTLIST node parents IDREFS #IMPLIED>
<!ELEMENT aliaslevels (level*)>
 <!ATTLIST aliaslevels action (add|update|delete|declare) "declare">
<!ELEMENT level EMPTY>
 <!ATTLIST level number CDATA #REQUIRED>
 <!ATTLIST level label CDATA #REQUIRED>
<!ELEMENT user EMPTY>
 <!ATTLIST user action (add|delete) "add">
 <!ATTLIST user login CDATA #REQUIRED>
 <!ATTLIST user domainName CDATA #REQUIRED>
 <!ATTLIST user domainType CDATA #REQUIRED>
 <!ATTLIST user firstName CDATA #IMPLIED>
 <!ATTLIST user lastName CDATA #IMPLIED>
 <!ATTLIST user email CDATA #IMPLIED>
 <!ATTLIST user accessLevel (admin|adminReadOnly|user|default) "default">
 <!ATTLIST user department CDATA #IMPLIED>
 <!ATTLIST user costCenter CDATA #IMPLIED>
 <!ATTLIST user workNumber CDATA #IMPLIED>
 <!ATTLIST user mobileNumber CDATA #IMPLIED>
 <!ATTLIST user pagerNumber CDATA #IMPLIED>
<!ELEMENT mergeitems (mergeitem+)>
```

```
<!ELEMENT mergeitem EMPTY>
 <!ATTLIST mergeitem toobject IDREF #IMPLIED>
 <!ATTLIST mergeitem fromobject IDREF #IMPLIED>
<!ELEMENT attribute (name,value*)>
 <!ATTLIST attribute name CDATA #IMPLIED>
 <!ATTLIST attribute value CDATA #IMPLIED>
<!ELEMENT value (#PCDATA)>
```

About the DTD elements

Following are the elements of the XML DTD:

- About the <application> element
- About <objects> and <object> elements
- About <attribute> elements
- About the <view> element
- About <node> elements
- About <user> elements
- About < mergeitems> and < mergeitem> elements

About the <application> element

The <application> element is the root level tag that encloses rest of the XML definitions. This tag will contain an `<objects>` tag and zero or more other tags, namely `<view>`, `<users>`, and `<mergeitems>` in this order. These tags and their structures are defined in the sections that follow.

About <objects> and <object> elements

The `<objects>` tag holds the definition of the objects to be acted on, and so contains a number of `<object>` tags. Each object tag represents a single asset in the Veritas Backup Reporter configuration.

Each object has the following properties that define it in the XML file:

`id`	The ID of the object. This is not the actual object ID but a unique value that identifies the object in the working XML.
`name`	The actual name of the object.

action	The action to be taken for the object. Following are the predefined actions that are allowed with respect to Veritas Backup Reporter configuration:
add	Add the object.
delete	Delete the object.
update	Update the properties of the object.
declare	No action. This object might be needed in XML at a later stage. In some cases, another object already present in the Veritas Backup Reporter configuration may be required to take action using this object (for example, setting it as a master object for a newly defined object). To be able to do that, the object must first be “declared” in the XML.
type	The type of the object. Currently, an object can be one of four types:
Generic_Object	A generic object such as a hierarchical node in the View tree.
Host	A host object.
File_System	A file system object.
Application	An application object.
master	The ID of the master object. An object with this ID should have been in the XML.
dbid	The database ID of the object. This is an optional field and will be written out when the data is exported. It is very useful in cases where we might want to update or declare objects. Because the dbid is actually an ID in the database, lookups are much faster. So, it is recommended to use the dbid to speed up the overall XML processing whenever possible. This ID is entirely database dependant and is created when the object is created. One cannot specify an object to have a specific dbid.

About <attribute> elements

Each object has a set of attributes that defines it in the Veritas Backup Reporter configuration. These attributes are defined in the <attribute> tag. Each attribute

tag can contain a <name> tag and multiple <value> tags. The <name> tag defines the name of the attribute and a <value> tag defines a value for it. There are several ways by which the attribute tags can be defined, such as in the following example:

```
<attribute>
  <name>attrname</name>
  <value>attrvalue 1</value>
</attribute>
```

Or, more simply:

```
<attribute name=”attrname” value=”attrvalue”/>
```

About the <view> element

The <view> tag defines a view in the Veritas Backup Reporter configuration. A view is a hierarchical association of objects. So, this tag contains multiple nested <node> tags that define the nodes of the tree. The tree tag contains the following properties:

identifier	The name of the view.
action	The action to be taken for the tree. Following are the predefined actions that are allowed with respect to Veritas Backup Reporter configuration:
add	Create a new view.
delete	Delete an existing view.
update	Update the view.
declare	No action. This just defines an already existing tree in the XML.
id	This is deprecated and no longer used.

About <node> elements

A node can be viewed as a container that holds a single object. The same object can be contained in more than one node in the tree, but a node can contain only one object. The properties of nodes are as follows:

id	The unique identifier of the node in XML.

`object`	The ID of the object that the node contains. This is the ID given to that object in the working XML file and not the actual ID. There can be multiple parents for a node. In such a case, the parent node IDs should be separated by spaces in the XML.
`parent`	The node ID of this node's parent node. The current node will be added as a child to the specified parent node. This is the ID given to the parent node in the working XML file and not the actual ID.
`action`	The action to be taken for the node. Following are the predefined actions that are allowed with respect to Veritas Backup Reporter configuration:
`add`	Add the node to the tree.
`delete`	Delete the node.
`declare`	No action. This node might be needed in XML at a later stage. In some cases, another node already present in the Veritas Backup Reporter configuration may be required to take action using this node (for example, adding a child node). To be able to use the node in XML as a parent for some other node, the node must first be "declared" in the XML.

About <aliaslevel> elements

In Veritas Backup Reporter 6.0, you can set aliases or labels for levels in views. Using the `aliaslevel`element, you can specify names for view levels. A view contains number levels. By default, the levels are labeled Level 1, Level 2, and Level 3, which is not very intuitive. To name the levels as per your requirements, you can use the `aliaslevel`element.

`action`	The action to be taken for the aliaslevel. Following are the predefined actions that are allowed with respect to Veritas Backup Reporter configuration:
`add`	Add the level number and level label.
`update`	Update the level number and level label.
`delete`	Delete the level number and level label.
`declare`	Default action.
`level number`	Enter the level number, for example, 1 or 2.
level label	Enter the label for the level.

About <user> elements

The <user> tag holds the information about the user to be added to or deleted from the system. The attributes of the <user> tag are explained below. The first four attributes (action, login, domainName, and domainType) are mandatory and rest all are optional.

action	Action to be taken for the user. Following are the allowed actions.
add	Add the user. Specified user gets added in the VBR database as well as to the VERITAS Security Services.
delete	Delete the user. Specified user gets deleted from the VBR database as well as from the VERITAS Security Services.
login	Login name of the user.
domainName	Domain name for the user.
domainType	Domain type for the user
firstName	First name of the user.
lastName	Last name of the user.
email	Email address of the user.
accessLevel	Access level assigned to the user. Following are the predefined access levels that a user can have.
admin	Administrator user. An administrator user has all privileges.
adminReadOnly	Administrator user with read-only access. This user can view everything that an administrator can view, yet cannot modify everything.
user	User who does not have administrator or administrator read-only privileges.
default	System default accesslevel. The default is set to user.
department	Department of the user.
costCenter	Optional text field that could be used to store information, such as cost center of the user.
workNumber	Work phone number of the user.
mobileNumber	Mobile phone number of the user.
pagerNumber	Pager number of the user.

About < mergeitems> and < mergeitem> elements

The <mergeitems> tag holds a number of <mergeitem> tags. Each <mergeitem> tag represents a pair of objects to be merged. The source object is merged into the destination object and the source object is deleted. Merging through the XML file allows a merge of multiple pairs at the same time.

You might want to merge objects in cases where the same object (such as a host or file system) is discovered by different discovery mechanisms and has different values for the same property, different properties of the object are discovered by different discovery mechanisms, or both. In this case we might need to merge these objects so that one object can be referenced as a single entity in the system.

Note: Once objects are merged, the operation cannot be reversed. One should be extremely careful merging objects, because incorrect usage may result in data corruption. We recommend that you do not merge objects while Agents are discovering data, since Agents might not be able to report some data.

The <mergeitems> tag includes these properties:

`toobject`	Destination object ID. This is the ID of the object in which the source object is merged.
`fromobject`	Source object ID. This is the ID of the object that is merged into the destination object. After the merge, this source object is deleted.

Examples of XML files

You can create several types of XML files, including the following:

- Add several host and file system objects and use them to create a tree.
  See "Example 1: Adding objects and a tree " on page 141.
- Update the properties of two host objects.
  See "Example 2: Updating two hosts " on page 144.
- Delete a single host object.
  See "Example 3: Deleting a host" on page 144.
- Merge two objects into a single object.
  See "Example 4: Merging objects" on page 145.

Examples also ship with Veritas Backup Reporter in the following location (by default):

Solaris	/opt/VRTSccsvs/xml-examples
Windows	\Program Files\Symantec\Veritas Backup Reporter\Server\xml-examples

Example 1: Adding objects and a tree

Example 1, when imported into Veritas Backup Reporter, creates a simple view with two top-level branches, each of which contains two host objects (“alpha” and “bravo”, “charlie”, and “delta”). The host “alpha” contains two file system objects.

```
<?xml version="1.0"?>
<!DOCTYPE application [
<!ELEMENT application (objects?,view*,user*,mergeitems*)>
 <!ATTLIST application version CDATA #REQUIRED>
<!ELEMENT objects (object+)>
<!ELEMENT view (node*)>
 <!ATTLIST view identifier CDATA #REQUIRED>
 <!ATTLIST view action (add|delete|update|declare) "declare">
 <!ATTLIST view id ID #IMPLIED>
<!ELEMENT object (attribute*)>
 <!ATTLIST object id ID #IMPLIED>
 <!ATTLIST object name  CDATA #IMPLIED>
 <!ATTLIST object action (add|delete|update|declare) "declare">
 <!ATTLIST object type CDATA #IMPLIED>
 <!ATTLIST object master IDREF #IMPLIED>
 <!ATTLIST object dbid CDATA #IMPLIED>
<!ELEMENT node (object?,node*)>
 <!ATTLIST node id ID #IMPLIED>
 <!ATTLIST node action (add|delete|declare) "declare">
 <!ATTLIST node object IDREF #IMPLIED>
<!ELEMENT user EMPTY>
 <!ATTLIST node parents IDREFS #IMPLIED>
 <!ATTLIST user action (add|delete) "add">
 <!ATTLIST user login CDATA #REQUIRED>
 <!ATTLIST user domainName CDATA #REQUIRED>
 <!ATTLIST user domainType CDATA #REQUIRED>
 <!ATTLIST user firstName CDATA #IMPLIED>
 <!ATTLIST user lastName CDATA #IMPLIED>
 <!ATTLIST user email CDATA #IMPLIED>
 <!ATTLIST user accessLevel (admin|adminReadOnly|user|default) "default">
 <!ATTLIST user department CDATA #IMPLIED>
 <!ATTLIST user costCenter CDATA #IMPLIED>
```

```
 <!ATTLIST user workNumber CDATA #IMPLIED>
 <!ATTLIST user mobileNumber CDATA #IMPLIED>
 <!ATTLIST user pagerNumber CDATA #IMPLIED>
<!ELEMENT mergeitems (mergeitem+)>
<!ELEMENT mergeitem EMPTY>
 <!ATTLIST mergeitem toobject IDREF #IMPLIED>
 <!ATTLIST mergeitem fromobject IDREF #IMPLIED>
<!ELEMENT attribute (name,value*)>
 <!ATTLIST attribute name CDATA #IMPLIED>
 <!ATTLIST attribute value CDATA #IMPLIED>
<!ELEMENT name (#PCDATA)>
<!ELEMENT value (#PCDATA)>
]>
<application version="2.0">
<objects>
<object id="o1" action="add" type="Host">
<attribute name="Hostname" value="alpha.veritas.com" />
<attribute name="IP Address" value="10.10.10.1" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version"value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o2" action="add" type="Host">
<attribute name="Hostname" value="bravo.veritas.com" />
<attribute name="IP Address" value="10.10.10.2" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version"value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o3" action="add" type="Host">
<attribute name="Hostname" value="charlie.veritas.com" />
<attribute name="IP Address" value="10.10.10.3" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version"value="unknown" />
<attribute name="Discovered Master Server" value="false" />
```

```
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o4" action="add" type="Host">
<attribute name="Hostname" value="delta.veritas.com" />
<attribute name="IP Address" value="10.10.10.4" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version"value="unknown" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="fs1" action="add" type="File_System" master="o1">
<attribute name="name" value="/" />
<attribute name="Discovered" value="false" />
<attribute name="Backed Up" value="true" />
</object>
<object id="fs2" action="add" type="File_System" master="o1">
<attribute name="name" value="/export" />
<attribute name="Discovered" value="false" />
<attribute name="Backed Up" value="true" />
</object>
<object id="cat1" action="add" type="Generic_Object">
<attribute name="name" value="Cat1" />
</object>
<object id="cat2" action="add" type="Generic_Object">
<attribute name="name" value="Cat2" />
</object>
</objects>
<view identifier="TestA1" action="add">
<node id="n1" action="add" object="cat1" />
<node id="n2" action="add" object="cat2" />
<node id="n3" action="add" object="o1" parents="n1" />
<node id="n10" action="add" object="fs1" parents="n3" />
<node id="n11" action="add" object="fs2" parents="n3" />
<node id="n4" action="add" object="o2" parents="n1" />
<node id="n5" action="add" object="o3" parents="n2" />
<node id="n6" action="add" object="o4" parents="n2" />
```

```
</view>
</application>
```

Example 2: Updating two hosts

Example 2, when imported into Veritas Backup Reporter, updates the properties of the two host objects (“Master Server 3” and “Host 3_8”) defined in the XML file.

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o2" action="update" type="Host">
<attribute name="Hostname" value="Master Server 3" />
<attribute name="IP Address" value="unknown" />
<attribute name="Operating System" value="unknown" />
<attribute name="Operating System Version"value="unknown" />
<attribute name="Discovered Master Server" value="true" />
<attribute name="Discovered Media Server" value="true" />
<attribute name="Discovered Backup Client" value="false" />
<attribute name="Discovered Online Storage Client" value="false" />
<attribute name="Discovered Agent Server" value="false" />
</object>
<object id="o3" action="update" type="Host">
<attribute name="Hostname" value="Host 3_8" />
<attribute name="IP Address" value=" " />
<attribute name="Operating System" value="Solaris" />
<attribute name="Operating System Version"value="2.6" />
<attribute name="Discovered Master Server" value="false" />
<attribute name="Discovered Media Server" value="false" />
<attribute name="Discovered Backup Client" value="true" />
<attribute name="Discovered Online Storage Client" value="true" />
<attribute name="Discovered Agent Server" value="false" />
</object>
</objects>
</application>
```

Example 3: Deleting a host

Example 3, when imported into Veritas Backup Reporter, deletes the host object “Host 8_0” from the data store.

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o1" action="delete" type="Host">
<attribute name="Hostname" value="Host 8_0" />
</object>
</objects>
</application>
```

Example 4: Merging objects

Example 4, when imported into Veritas Backup Reporter, merges object “o2” into the object “o1”. Objects “o1” and “o2” represent the same host. One was discovered having a host name of “hostA.veritas.com” and the other was discovered having host name as “hostXYZ.somedomain.veritas.com”. While merging object “o2” into object “o1”, you can specify “hostXYZ.somedomain.veritas.com” as an alias for object “o1”. After merging object “o2”, it is deleted and only object “o1” will remain.

In Example 4, a host object has the hostname “hostA.veritas.com” which also goes by the name “hostXYZ.somedomain.veritas.com”. The XML export of this object would look like the following:

(The DTD header has been snipped.)

```
<object id="o1" action="declare" type="Host" dbid="50">
<attribute>
 <name>Hostname</name>
 <value>hostA.veritas.com</value>
 <value>hostXYZ.somedomain.veritas.com</value>
 </attribute>
<attribute>
 <name>IP Address</name>
 <value>UNKNOWN</value>
 </attribute>
<attribute>
 <name>Operating System</name>
 <value>Windows</value>
 </attribute>
<attribute>
 <name>Operating System Version</name>
 <value>Windows 2000</value>
 </attribute>
<attribute>
 <name>Discovered Master Server</name>
 <value>false</value>
 </attribute>
```

```
<attribute>
 <name>Discovered Media Server</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Backup Client</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Online Storage Client</name>
 <value>true</value>
 </attribute>
<attribute>
 <name>Discovered Agent Server</name>
 <value>false</value>
 </attribute>
</object>
```

This example has another host object whose hostname is just “hostA” and whose XML export would be the following:

```
<object id="o2" action="declare" type="Host" dbid="70">
<attribute>
 <name>Hostname</name>
 <value>hostA</value>
 </attribute>
<attribute>
 <name>IP Address</name>
 <value>10.10.10.1</value>
 </attribute>
<attribute>
 <name>Operating System</name>
 <value>UNKNOWN</value>
 </attribute>
<attribute>
 <name>Operating System Version</name>
 <value>UNKNOWN</value>
 </attribute>
<attribute>
 <name>Discovered Master Server</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Media Server</name>
```

```
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Backup Client</name>
 <value>true</value>
 </attribute>
<attribute>
 <name>Discovered Online Storage Client</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Agent Server</name>
 <value>false</value>
 </attribute>
</object>
```

If you are certain that these two host objects are indeed the same host, we can merge them. But, before we simply merge the underlying objects, we must take care to update the surviving object with data that would make sure no future objects with the name “hostA” get created. To do this, we update the first host record as such. The hostname attribute is now a union of the two objects, and the IP address is set to the actual discovered IP address.

```
<objects>
<object id="o1" action="update" type="Host" dbid="50">
<attribute>
 <name>Hostname</name>
 <value>hostA.veritas.com</value>
 <value>hostXYZ.somedomain.veritas.com</value>
 <value>hostA</value>
 </attribute>
<attribute>
 <name>IP Address</name>
 <value>10.10.10.1</value>
 </attribute>
<attribute>
 <name>Operating System</name>
 <value>Windows</value>
 </attribute>
<attribute>
 <name>Operating System Version</name>
 <value>Windows 2000</value>
 </attribute>
<attribute>
```

```
 <name>Discovered Master Server</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Media Server</name>
 <value>false</value>
 </attribute>
<attribute>
 <name>Discovered Backup Client</name>
 <value>true</value>
 </attribute>
<attribute>
 <name>Discovered Online Storage Client</name>
 <value>true</value>
 </attribute>
<attribute>
 <name>Discovered Agent Server</name>
 <value>false</value>
 </attribute>
</object>
</objects>
```

Now, whenever a particular VBR Agent refers to a host as “hostA”, the server will know that we’re talking about this one object since one of its host names is an exact match. After this important object update, we can merge the two hosts with the following syntax:

```
<mergeitems>
<mergeitem toobject = "o1" fromobject = "o2"/>
</mergeitems>
```

This moves all data that pointed to the initial hostA object to the newly updated object and delete the hostA object when its done.

Appendix C

About Veritas Backup Reporter database tables

This appendix includes the following topics:

About Veritas Backup Reporter database architecture

The Veritas Backup Reporter (VBR) database is a rich repository of information about your storage network. This section gives an overview of the VBR database, and describes the tables in the VBR namespace.

The VBR Management Server uses Sybase Adaptive Server Anywhere (ASA) database to store backup data collected from various backup products.

The `ccsvc` database uses several database user names in which database objects (tables, views, and stored procedures) are organized.

Each database user provides a namespace for database objects defined by Veritas Backup Reporter and the Veritas Alert Manager:

- Veritas Backup Reporter uses the database to store service usage and expenditure reports, cost metrics, cost formulas, and alerts.
- The Veritas Alert Manager (bram) stores data related to performance and monitoring.

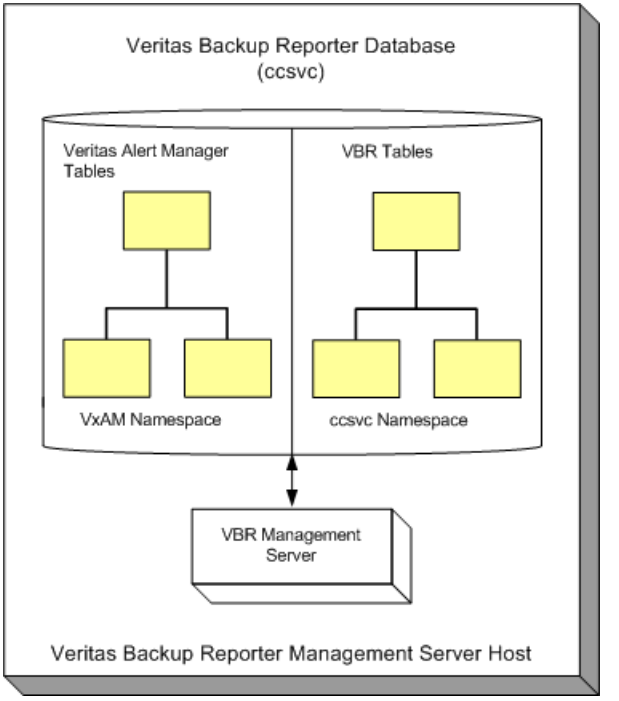
The install script creates the required namespaces depending on which Veritas products are installed.

About namespaces for the Veritas Backup Reporter Management Server

When the VBR Management Server is the only Veritas product installed on a host, the following namespaces are created in the database instance:

- `bram` namespace
- `ccsvc` namespace

Figure C-1 Database namespaces created on a VBR Management Server



About querying the Veritas Backup Reporter database

Table C-1 provides the connection information and credentials for accessing the VBR database through either dbisql, ODBC, or JDBC.

Table C-1 Connection information and credentials for accessing the VBR database

Item	Value
Database Name	ccsvc

Table C-1 Connection information and credentials for accessing the VBR database *(continued)*

Item	Value

Server	■ Solaris:
	`Veritas_dbms3_<hostname>`
	where <hostname> is not the fully qualified domain name.
	■ Windows:
	`Veritas_dbms3_%COMPUTERNAME%`

Database port	2994
Default User Name	guest
Default Password	guest

Note: `guest` is an account with read-only permissions.

About accessing the database using dbisql

The Sybase Interactive SQL program, `dbisql`, is the client interface for querying the database. `dbisql` is installed by default in:

Solaris	`/opt/VRTSdbms3/bin`
Windows	`\Program Files\VERITAS\VxDBMS3\Win32`

Before running `dbisql`, remember to set the necessary ASA environment variables:

Solaris:
Bourne, K shells
	`/opt/VRTSdbms3/vxdbms_env.sh`
	For example:
	`cd /opt/VRTSdbms. ./vxdbms_env.sh`

Solaris:
C shell
	`/opt/VRTSdbms3/vxdbms_env.csh`
	For example:
	`cd /opt/VRTSdbms`
	`source vxdbms_env.csh`

Windows:	For example:
ASANY9	`ASANY9=C:\Program Files\VERITAS\VxDBMS3\Win32`
ASANYSH9	`ASANYSH9=C:\Program Files\Symantec\vxdbms\server\shared`

Examples:

Solaris dbisql	Following is an example connect string for `dbisql` on Solaris:
	`dbisql -c "UID=guest;PWD=guest;`
	`ENG=Veritas_dbms3_hostname;`
	`DBN=ccsvc;links=tcpip (port=2994)"`
	Replace hostname with the host running the database.

Windows dbisql	Following is an example connect string for dbisql on Windows:
	`dbisql -c "UID=guest;`
	`PWD=guest;ENG=Veritas_dbms3_%COMPUTERNAME%;`
	`DBN=ccsvc; links=tcpip(port=2994)"`

About accessing the database using ODBC

You can perform VBR database queries with ODBC.

You will need the following VBR database information to create an ODBC DSN:

- `DRIVER=Veritas DBMS Adaptive Server Anywhere 9.0.2`
- `UID=GUEST`
- `PWD=guest`
- `DBN=ccsvc`
- Solaris: `ENG=Veritas_DBMS3_hostname`
- Windows: `ENG=Veritas_DBMS3_%COMPUTERNAME%`
- `LINKS=all`

For more information, refer to the following URLs:

- ASA 9.0.2 documentation:
  http://sybooks.sybase.com/nav/detail.do?docset=766
- ODBC connection documentation:
  http://sybooks.sybase.com/onlinebooks/group-sas/awg0802e/dbpgen8/@Generic__BookTextView/21966;pt=21966?DwebQuery=odbc#X

About accessing the database using JDBC

JDBC is another option available for performing VBR database queries.

The syntax is:

```
jdbc:sybase:Tds:<hostname>:port?ServiceName=<databasename>
```

For example:

```
jdbc:sybase:Tds:myhost:2994?ServiceName=vxcc
```

Index

U

V

X