Veritas Backup Reporter User's Guide

Veritas Backup Reporter User's Guide

Documentation version 6.0

PN: : (HRO7210)SKU 11132088

Legal Notice

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

Chapter 1

Introducing Veritas Backup Reporter console

This chapter includes the following topics:

Connecting to the VBR Management Server

The Veritas Backup Reporter (VBR) display information in a Web-based console from which you can perform all tasks associated with managing delivery of VBR Management Server services and quantifying the results of VBR Management Server expenditures.

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

If you have a supported Web browser and the other requirements are met, you can start the console and connect to a VBR Management Server host.

For more information about Web browser requirements and the requirements for installing Veritas Backup Reporter, see the *Veritas Backup Reporter Release Notes*.

To connect the console to a VBR Management Server host

1. On a client system that has a network connection to the VBR Management Server invoke a Web browser.

   Your browser must be configured to accept cookies, and JavaScript must be enabled. If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the VBR Management Server.

2. In the browser's address field, type the following URL and press **Enter**:

   https://<VBRServerHostName>:<portNumber>/vbr

   where `<VBRServerHostName>` is the hostname, IP address, or fully qualified domain name of the host on which the VBR Management Server is running, and `<portNumber>` is the Management Server host port through which you are connecting. The default `<portNumber>` is `8443`.

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

   You can connect to any VBR Management Server to which you have IP connectivity and for which the administrator has provided you with user credentials.

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

3. In the Login page, do the following:

   - Type your user name and password in the respective fields.
     Veritas Backup Reporter ships with default user name and password of admin ('admin' and 'password'). You may need to check with your administrator to see if these login credentials have been changed. (For security reasons, it is best to change them shortly after installation.)
   - On the Domain list, select the domain in which your user name is defined.
     If you are logging in as the administrator, use the `cc_users` domain.
     If the Domain list is empty, it is likely that the Management Server host is not configured correctly. Notify the administrator for the Management Server.
   - Click **Login**.
     Upon connection to the Management Server, your home page displays. From there you can access Veritas Backup Reporter views, reports, and other features.

To disconnect the console from the VBR Management Server

- Click **Logout** in the console navigation bar.

  The console disconnects from the VBR Management Server and refreshes the browser to return you to the Login page.

Understanding the VBR console

The VBR console displays in a Web browser and consists of a header, a set of tabs, a task pane, and the main content pane.

The following topics describe the use of these elements in Veritas Backup Reporter:

- See "About the header" on page 19.
- See "About the tabs" on page 19.
- See "About the task pane" on page 20.
- See "About the content pane" on page 20.

About the header

At the top of the console window, the header enables you to:

- Switch to another Veritas product
  See "Switching among Veritas products" on page 28.
- Access Veritas Backup Reporter product information (About link)
- Disconnect the console from the Management Server (Logout link)
- Access Veritas Backup Reporter help (Help link)

Note: The VBR console header does not display the name of the Management Server to which you are connected. To connect to another Management Server, log out and then connect.

See "Connecting to the VBR Management Server" on page 17.

About the tabs

Beneath the header, a series of tabs provide access to each major area of the VBR console.

Following is the default set of tabs:

Home	Display the home page
Reports	Create and view reports about backup resources and VBR Management Server usage
Monitors	Monitor the status of backup jobs, display and respond to alerts
Costs	Define chargeback rates and formulas to establish and monitor IT costs for different levels of the organization
Views	Display information about IT assets
Settings	Customize the VBR Management Server, configure exploration and automatic notification, define and manage user accounts

Under each tab is series of subtabs; the contents of the subtabs vary depending on the page currently displayed in the content pane. On the Reports tab, for example, there are subtabs for each of the major report types as well as a subtab for the My Reports pane.

To the right of the tabs, the console displays the user name with which you are logged in.

About the task pane

In most sections of the VBR console, a task pane on the left side of the console window serves as a navigation area, giving you quick access to specific views. The views are listed in a hierarchical (tree) structure. You can move among views by expanding the branches of the tree and then selecting the views you want to see.

See "Navigating object views" on page 30.

About the content pane

The main display area, or content pane, displays information in a variety of tabular and graphical formats. The information displayed in the content pane is context-sensitive to current selections in the tabs and the task pane.

One of the most common display formats is the object view.

See "Displaying object views" on page 29.

Using tables

Much of the information displayed in the content pane takes the form of tables. The Alerts Details is an example of such a table. You can manipulate the tables to display the information you want and how to preserve data to a printer or file.

Filtering the information displayed in tables

When a table displays a large amount of information, you can reduce the size of the display by selecting specific characteristics to filter. For example, if you filter the Alerts Details table by severity `CRITICAL` or `ERROR`, the table will refresh to display only alerts with those severity levels.

To filter the contents of a table

1 In the VBR console, select the Filter icon at the top of a table.

2 In the Filter Table dialog box, click **Enabled**.

The dialog box refreshes to display a list of the columns in the table. Each column represents a specific attribute of the object; for example ID or Severity.

The dialog box lists only those columns currently defined for the table.

See "Specifying rows and columns in tables" on page 23.

3 Check a column name.

The dialog box refreshes to display selection criteria for the column you selected.

4 Select one of the ollowing:

AND	If you checked two or more columns, the filtered table displays only the objects whose values satisfy all of the specified filters.
OR	The filtered table displays objects whose values match any of the filters.

5 For text attributes, select matching criteria from the drop-down list.

- Type text in the Value field.
  The Value text is not case-sensitive, and it can be any part of an object's name or attribute value. For example, if you typed the string `row`, all of

the following would display in the filtered table: `row`, `arrow`, `Rowland35`, and `brown`.

- On the drop-down list, select any of the following matching criteria:

ANY Words	Display objects for which the column contains any of the words typed in the Value field.
ALL Words	Display only objects for which the column contains all the words typed in the Value field, regardless of order.
Exact Phrase	Display only objects for which the column contains exactly what is typed in the Value field. Example: `not running` matches objects with a state of `NOT RUNNING`; however, `running` matches objects with a state of either `RUNNING` or `NOT RUNNING`.
Regular Exp.	Interpret the Value field as a Java regular expression, and display objects to which the expression applies. Example: `$(EMC|IBM)` matches any object whose attribute value begins with either `EMC` or `IBM`.

6 For numeric attributes, do one of the following:

- Click the top radio button to display objects whose numeric attributes satisfy a threshold, select a mathematical operator (<, <=, =, !=, =>,>) from the drop-down list, and then type a number in the text box.
  Examples: >=1, <2, !=900
- Click the bottom radio button to display objects whose numeric attributes fall within a certain range.
  Example: Between 10 and 20

7 For state attributes, click the radio button corresponding to the value you want to filter.

Example: Bound = `YES`

8 To filter on additional columns, repeat 3 through 7.

9 When you are finished, click **OK**.

The table redisplays, with filters applied. The table lists only those items that meet the filtering criteria. The word Filtered displays next to the table's name.

Your filters remain in effect only while you are displaying the table. When you display the table again, the default settings will be restored. (To remove filtering for the current display, reopen the Filter Table dialog window and delete the text from the text boxes for all attributes.)

Specifying rows and columns in tables

In many tables, you can choose the number of objects (rows) and which information (columns) to display. These tables have an Edit icon at the top.

Figure 1-1 Edit Icon

In all tables, you can also change column widths and sort columns in ascending or descending order.

For all of the following operations, your customized settings remain in effect until you disconnect from the VBR Management Server to which you are connected.

To specify what displays in tables using the Edit icon

1 Click the table's **Edit** icon.

2 In the Table Settings dialog window, specify table columns by doing one or both of the following:

- Select column names and then use the Add and Remove buttons to add them to, or remove them from, the Selected Columns list.
- Click column names in the Selected Columns list and then use the Move Up and Move Down buttons to change the order in which columns display.

3 To specify the number of table rows, select a value in the Rows Per Page list.

4 Click **OK**.

The table refreshes to reflect the specified settings.

To change the width of a table column

1 Click the edge of the column heading and hold the left mouse button down.

2 Drag the edge of the column heading to the right or left.

To sort the contents of a table column

1 In an object view table, click the column header.

The column is sorted in ascending order.

2 To sort in descending order, click the column header again.

Printing table contents

You can print the contents of a table using the Print icon.

To print a table's contents

1 In an object view, click the **Print** icon at the top of a table.

A new browser window opens, displaying the table in printer-friendly format.

2 In the Print dialog box, select a printer and adjust the printer settings as required.

3 Select one of the following:

- OK
- Print

The data in the table is queued to the printer you specify.

Saving table contents

You can preserve the contents of a table by exporting it to a comma-separated (CSV) file, using the Save icon. You can use a standard text editor or spreadsheet program to work with the data.

Figure 1-2 Save icon

To save a table's contents to a file

1 In an object view, click the **Save** icon at the top of a table.

2 If the File Download dialog box displays, click **Save**.

3 In the Save As dialog box, specify a path and name for the file, and then click **OK**.

The data in the table is saved in the location you specify.

Performing operations on objects

In some tables, you can select one or more objects and perform an operation on them. In the Alerts Details, for example, you can acknowledge several alerts at once.

To perform an operation on objects in a table

1 In a table, check each object on which you want to perform the operation.

To select all of the objects, check the checkbox in the upper left corner of the table.

2 On the drop-down list, select the operation (for example, Acknowledge), and then click **Go**.

3 Complete the dialog boxes for the indicated operation.

Accessing multiple pages of data in tables

When there is more data to display than a table has rows, the table will contain multiple pages. A Go to Page bar helps you navigate the pages.

Figure 1-3 Go to Page Bar

Note: You can control the number of rows displayed in many tables.

See "Specifying rows and columns in tables" on page 23.

To access pages in a table

1 In a table with multiple pages, locate the Go to Page bar just below the table.

2 Do any of the following:

- To go to a specific page, click the page number.
- To go to the previous page, click the left arrow.
- To go to the next page, click the right arrow.
- To go to the first page, click the double left arrow.
- To go to the last page, click the double right arrow.

Some tables, such as the Host Mapping Summary, have a Show control with which you can specify the number of rows on each page.

To change the number of rows on each table page

- In a table with multiple pages, in the Show drop-down list just below the table, select the number of rows to show on each page, and then click **Go**.

  The table is reconfigured; its pages contain the number of rows you selected.

  For example, if a table has 250 rows, you could select 50 to break the table into 5 pages of 50 rows each. Alternatively, you could select 20 to break the table into 12 pages of 20 rows each, plus one page of 10 rows.

  See the *Veritas Backup Reporter Administrator's Guide* for information about performing other, administrator-level tasks from the console's configuration window.

Updating your console settings

Use the My Profile section of the VBR console to update your user profile. The user profile contains information such as your name, email address, and the password you use to access Veritas Backup Reporter.

The settings you specify here affect only the user name with which you are logged in to this VBR Management Server. All settings persist across sessions.

Updating your personal information

Use the My Profile dialog box to update your personal information, including your email address, and to change your password.

Figure 1-4 My Profile dialog screen

To change your personal information

1. On the console Settings tab, click **Settings > My Profile and Settings**.
2. In the My Profile dialog box, type updated information in the First Name, Last Name, and Email Address text boxes.
3. Click **Save**.

   Your user profile is updated.

Changing your password

Your administrator assigns a password when setting up your user account. You should change the password the first time you access the VBR console and then change it at regular intervals thereafter.

To change the password with which you log on to Veritas Backup Reporter

1. On the console Settings tab, click **My Profile and Settings**.
2. In the My Profile dialog box, click **Change Password**.
3. In the Change Password dialog box, do the following:
   - Type your old password in the Old Password field.
   - Type your new password in the New Password field. Asterisks display in place of the password text.
     Passwords are case-sensitive and must be at least five-characters long.
   - Type your new password again in the Confirm New Password field.
4. Click **Save**.

   Your password is changed.

Accessing and using online help

Veritas Backup Reporter offers a cross-platform, browser-based online help system.

On UNIX computers, you can use manual pages to find reference and usage information about product-specific commands. When you install Veritas Backup Reporter, the `pkgadd` command installs the nroff-tagged manual pages in the appropriate directories under `/opt/VRTS/man`. However, the install does not update the windex database.

To ensure that new manual pages display correctly, update the following:

- `MANPATH` environment variable to point to `/opt/VRTS/man`
- `windex` database

Refer to the `catman(1M)` manual page for more information about updating windex.

To access help

- Click **Help** in the upper-right corner of the console.

Switching among Veritas products

You can switch to Veritas products on other hosts, provided that your administrator has configured links to those hosts.

The configuration steps are described in the *Veritas Backup Reporter Administrator's Guide*.

To access another Veritas product from the console

1. Select the product name (for example, VBR Management Server or Availability) in the header section of the console.

   The other product launches in the same browser window.

2. To return to Veritas Backup Reporter, click **Veritas Backup Reporter** in the console header.

Chapter 2

Viewing your IT assets

This chapter includes the following topics:

Displaying object views

Use the Views tab in the VBR console to view information about your information technology (IT) assets. These views, called object views, can be organized in a variety of ways to suit your needs.

Select the Views tab in the console to display the Views page, in which to display information about backup resources and groupings. An object view can contain detailed information about an object, such as a host or file system, or it can contain lists of data in table format for a class of objects.

The kinds of information displayed in a detail view depend on the object category.

See "Selecting object view categories" on page 30.

The task pane, on the left side of the console window, provides easy access to views by means of a hierarchical tree view.

The following topics provide detailed information for using the object views:

- See "Navigating object views" on page 30.
- See "Selecting object view categories" on page 30.
- See "Using object levels" on page 30.
- See "Searching for hosts" on page 32.
- See "Viewing details about hosts and file systems" on page 32.

- See "About viewing tabular information about a class of objects" on page 35.

Navigating object views

Familiarity with the structure of object views is helpful for navigating through the views and for performing other tasks in the console, such as generating reports.

Object views are organized into multiple hierarchical levels. The highest is the level of the entire view itself, referred to as the top level or view level. Discovered objects such as hosts and file systems occupy the lowest levels of the view. Typically, between the top and bottom levels there are several user-defined levels that serve to organize objects in the view into a useful structure.

When you are in the Views section of the console, the task pane displays the view hierarchy in the format of a tree view. A navigation path at the top of the content pane displays the hierarchy of views and allows you to retrace your steps easily.

Selecting object view categories

Your administrator defines object view categories for your installation. Following are some examples of object view categories:

- Geography
- Line of business
- Application
- Service provider
- Data classification
- Regulatory
- Server type
- Backup infrastructure

To select object view categories

- At the top of the task pane, select the category of object views you want to browse from the drop-down list, and then click **Go**.

  The view tree refreshes to display a list of object views organized by the specified category.

Using object levels

As you work in the console, it is helpful to understand object levels and the way they are represented in the tree view. The Report Wizard, for example, has controls

that use object levels to define the scope of your reports and how they display data.

All levels below the top level (the view level) are numbered, from Level 1 down to the lowest level defined for the view. The lowest levels consist of discovered objects: hosts and their associated file systems. The higher levels consist of nodes created by an administrator to organize the lower-level objects into logical groupings.

The following illustration shows a sample tree view called Geography, with level numbers shown for some of the objects in the tree.

Figure 2-1 console: Task Pane for Views Tab

In this example, the tree view displays three numbered levels: Level 1, which includes AsiaPac and North America; Level 2, which includes country names such as Australia and Canada; and Level 3, which includes city names such as Sydney and Toronto.

Lower levels representing hosts (Level 4) and file systems (Level 5) are not shown in the tree view for this example.

To view a list of hosts

- Do one of the following
  - Select an object at the next highest level (such as Toronto) to display a list of its hosts in the content pane.
  - Click **Show/Hide Hosts** to display hosts in the tree view.
    You can display additional levels by drilling down in the content pane. For example, when you display the object view for a host (Level 4) in the content pane, you can click from lists of file systems (Level 5).

Figure 2-2 Show/Hide Hosts Icon

Searching for hosts

You can search for specific hosts within the scope displayed in the content pane. For example, when Toronto is displayed in the content pane, you can quickly find and display details about host_01 in Toronto, or about all hosts whose names start with host_0.

To search for one or more hosts

1. Display a high-level view in the console content pane.
2. On the Search Hosts subtab, in the Search text box, type a text string.

   The string can be a host name or a partial host name. Use the percent sign (%) as a wildcard character.

   Examples:

   - `host_01` displays the host named host_01.
   - `host_0%` displays all hosts whose names begin with host_0.
   - `%row%` displays all of the following hosts: row, arrow, rowland35, and brown.
3. Click **Go**.

   The content pane is updated to display a table of all hosts whose names meet the search criteria.
4. Select a host name to view the host's object view.

Viewing details about hosts and file systems

The detail view for a host displays the host's attributes and lists of the file systems defined on the host.

To display the detail view

- Select the name of a host in a higher-level view or in the tree view.

Viewing and editing host attributes

VBR Agent modules discover a great deal of data about objects in your network. The terms information or details are used to describe these different kinds of data. Attributes refer to a specific kind of data: details pertain to a specific object

type. For example, the attributes for a host include its name, operating system, and whether it is a NetBackup master server or media server.

To display a list of attributes for a host or for an associated file system, database, or application

1 Click **Edit** in a table.

2 To edit some of the attributes, click **Edit Attributes** in the drop-down list, and then click **Go**.

See "About managing attributes" on page 39.

Viewing host file systems

In a host's detail view, the Defined File Systems list displays a list of the file systems defined on the host.

To display the attributes of a file system

- Select the name of a file system.

Viewing host backup jobs

If the host is a NetBackup master server or media server, you can view detailed information about current and completed backup jobs running on the host.

To view a snapshot of current backup activity

- Click **Backup Jobs**.

  The Backup Jobs table displays details about all backup jobs currently running.

To view a list of backup jobs that have completed

1 Click **Backup Jobs** in the drop-down list, and then click **Go**.

2 Select a backup job in the list to view details about it.

Updating host aliases

You can give each host alias names. The host's primary alias displays in tree views and in higher-level object views, and its other aliases are used when you are searching for hosts on the network. Alias names are also used by agent modules as they gather information from hosts in the network.

To view a list of the host alias names currently defined

- Click **Views > Host Aliases**.

Warning: It is essential that your alias names be compatible with your hosts' DNS names or with the names by which they are known to applications like NetBackup and Backup Exec. If, for example, you use an alias that is unknown to NetBackup, the explorer will stop collecting information from the NetBackup host and instead will attempt to collect data from a host with the alias name.

To give an alias to a host

1. In the task pane view, click a host name.
2. In a host's detail view, click **Host Aliases** from the drop-down list, and then click the green checkmark icon.
3. In the Manage Host Aliases dialog box, do the following:
   - In the Host Name drop-down list, select the name of the host.
   - Type a new alias in the New Name field, or change the primary alias in the Primary Name field.
   - Optionally, modify other alias names displayed in the dialog box.
   - Click **Save**.
     The dialog box refreshes to show the host's updated alias information. If you typed a value for New Alias, that value now displays as the primary alias.
4. If you are done, click **Cancel** to exit the dialog window.
5. To create additional alias names for the host, repeat 3.

   For information about changing aliases for higher-level entities in tree views and object views, see the *Veritas Backup Reporter Administrator's Guide*.

Viewing host IP addresses

You can view host IP addresses.

To view a list of host IP addresses

1. Click **Views > Host IPs**.
2. Click a column header to sort the list by IP address.

   The sort is a text sort. For example, IP addresses would be listed in this order: `nn.nn.nn.109`, `nn.nn.nn.11`, `nn.nn.nn.110`.

Displaying reports for individual hosts

You can view reports for an individual host or a collection of hosts by clicking the **Report Mode** icon in the task pane.

To view a report when report mode is turned on

- To view a report, check an item in the tree view (such as Toronto) or an individual host, and then click **Create Report**.

About viewing tabular information about a class of objects

Agent modules running on one or more hosts in your network, collect information about objects in the network. This information is presented in the form of tables in the Views section of the VBR console.

About displaying a table of objects

Whenever you select an object in the tree view (other than a host), the content pane displays a table listing the objects at the next level. For example, if you selected Sydney in the tree view, a table listing the hosts in the Sydney office would appear.

Figure 2-3 Example of a Table in the VBR console

Details ▲	Object Name	Object Type
	ccsqawindp1	Host
	illusion.vxindia.veritas.com	Host
	blueberry.vxindia.veritas.com	Host
	ccsqawinsp1.vxindia.veritas.com	Host
	gompu.vxindia.veritas.com	Host
	pinacolada.vxindia.veritas.com	Host
	harishw.vxindia.veritas.com	Host
	harishw	Host
	adrenalize	Host
	ccsqawinsp1	Host
#	**Total Objects: 10**	

See "Using tables" on page 21.

About launching another object view

In many object views, you can select the display names for higher- and lower-level objects in the tables. Selecting the name of a lower-level object displays a view

for that object. For example, if you are displaying a list of all the hosts in Hong Kong, you can select the name of a host to display a detailed object view for that host.

See "Navigating object views" on page 30.

About customizing activity views

You can create custom views that fit the particular needs of your enterprise.

About creating custom views using the View Builder

An administrator can create custom views that display selected information for a particular class of objects or grouping of objects. This is done using the View Builder, an application for creating, modifying, and managing access to object views.

For more information and detailed instructions on using the View Builder, see the *Veritas Backup Reporter Administrator's Guide*.

About creating backup views that display data by file system

If most of your backup policies create backup jobs that include only one path, your views and reports will be able to show data at the file system level. If, for example, you have a machine where `D:\` is used by Division D and `E:\` is used by Division E, you will be able to create views and reports showing jobs that affect one division without showing other jobs being run for that machine.

For example, you could create a view like this:

Divisions

Division D

HostA

D:\

Division E

HostA

E:\

Enabling or disabling breakUpJobs

If you do not want to display backup job status at the file system level, disable the breakUpJobs option on the `bplist` command in NetBackup. With `breakUpJobs`

enabled, you would need to place a separate object for each file system when you construct a view using the View Builder. On the other hand, with `breakUpJobs` disabled, you need to place only one file system object (named `Other`) into your view.

To demonstrate the effect of breakUpJobs, a job for HostA and path C:\ will reference the following:

- With breakUpJobs enabled, host HostA and file system C:\
- With breakUpJobs disabled, host HostA and file system Other

About understanding the effects of your NetBackup policy configuration

Table 2-1 shows some NetBackup policy configurations and the resulting ways in which data is collected with `breakUpJobs` enabled. (With `breakUpJobs` disabled, every job references the file system object named `Other`.)

Note: Multistream policies will generally create backup jobs with only one path.

Table 2-1 Sample NetBackup policy configurations and the paths referenced as a result

Multi- stream?	File systems included	Number of NBU jobs	Paths shown in NetBackup jobs	Paths shown in Veritas Backup Reporter views
No	C:\ D:\	1	C:\ D:\	Other
No	C:\	1	C:\	C:\
No	C:\ NEW_STREAM D:\	2	C:\ D:\	C:\ D:\
No	ALL_LOCAL_DRIVES	1	ALL_LOCAL_DRIVES	ALL_LOCAL_DRIVES
Yes	C:\ D:\	2	C:\ D:\	C:\ D:\
Yes	C:\	1	C:\	C:\
Yes	C:\ NEW_STREAM D:\	2	C:\ D:\	C:\ D:\

Table 2-1 Sample NetBackup policy configurations and the paths referenced as a result *(continued)*

Multi- stream?	File systems included	Number of NBU jobs	Paths shown in NetBackup jobs	Paths shown in Veritas Backup Reporter views
Yes	ALL_LOCAL_DRIVES	2 The number of jobs—and paths shown for both NetBackup and Veritas Backup Reporter—depends on what local drives are defined for the computer. In this example, the machine has two drives: C:\ and D:\.	C:\ D:\	C:\ D:\

Verifying your customized host views

To verify that hosts are listed in your customized views as you expect, check the host mapping settings. You can access these displays by clicking their subtabs in the Views area of the console.

To view your customized hosts

- Click **Host Mapping Summary** to view, for each host, an icon indicating whether or not it is represented in each type of view.

  For example, a green icon in the Geography column for `db2host` indicates that `db2host` is represented in the Geography view. Click an icon to display the host's detail view.

To view the higher-level grouping for each host under which the host can be found in each type of view

- Click **Host Mapping Details** .

  For example, `samplehost` might be found in the Geography view under `Toronto` and in the Application view under `DB2 Servers`.

To display the detail view for a particular host

- In the Host Mapping Details table, click a hyperlinked cell.

  For example, on the row for `samplehost`, clicking `Toronto` in the Geography column will display the detail view for `samplehost` with the Geography tree visible in the task pane.

About managing attributes

Veritas Backup Reporter discovers a great deal of data about hosts and other objects. The terms information or details are used to describe these different kinds of data.

The term attributes refers to detailed data that pertains to a specific object type. For example, the attributes for a host include its vendor name, model, and operating system. VBR Agent modules query objects on the network and retrieve a standard set of attributes for each type of object.

Some attributes contain relevant details that cannot be discovered by Veritas Backup Reporter or any other software application. These user-created or custom attributes convey information that is meaningful to you but is not part of the object's physical or software makeup.

Some common examples include:

- Physical location of the object
- Warranty date for the object
- Date of purchase
- Date of most recent service
- Contact information for parties responsible for maintenance

You can add, change, or delete customized attributes for an object.

Note: Custom attributes are added on a per object basis. There is no way to create an attribute for a group of objects and set a default value for that attribute.

About viewing attributes

You can view attributes for a host by displaying the host's detail view.

See "Viewing details about hosts and file systems" on page 32.

Editing attributes

You can edit the value of several attributes, including the name by which a host object displays in the console. A `Misc Info` attribute is provided for specifying details such as the object's physical location.

To edit an object's user-defined attributes

1. Display the object's detail view.
2. On the drop-down list, click **Edit Attributes**, and then click **Go**.
3. In the Edit Attribute dialog box, do the following:
   - For each attribute you want to edit, type a new value in the Value column, or select a value from the drop-down list.
   - Click **Update**.
     The attribute's value is changed.

Chapter 3

Reporting on backup services

This chapter includes the following topics:

About reports

Veritas Backup Reporter (VBR) reports help you monitor and predict activity in several areas of business services. For example, you can monitor the success rate and predict future trends for backup jobs on the network. You can also display historical data on the volume of backup tasks being performed on behalf of service consumers.

Veritas Backup Reporter provides default reports for backup, recovery and cost. You can manipulate the scope and time frame for these default reports to create reports that are useful to you. Veritas Backup Reporter also gives you the option of creating custom reports for specific areas of network operations.

The default reports, along with the custom reports you create, are accessible using the subtabs in the Reports section of the console. For ease in viewing, you can

organize the reports you use most often into portal pages, such as My Reports and My Backup Reports. You can also archive reports and arrange for them to be sent by email to other people.

Additionally, for each report subject, Veritas Backup Reporter provides different types of reports including simple ranking and pie chart reports, trending and forecast reports, and reports correlating multiple data types, such as a comparison of the job success rate versus job size for data backups.

Veritas Backup Reporter reports gather data via VBR Agent modules.

The following topics describe basic information about using reports:

- See " About VBR report types" on page 42.
- See "About report formats" on page 44.

You can also use and manage the contents of reports portal pages, customize default reports and create your own reports, use reports for automatic notification, and run custom SQL queries.

About VBR report types

Veritas Backup Reporter provides the following report types:

- See "About backup reports" on page 42.
- See "About recovery reports" on page 43.
- See "About cost reports" on page 43.
- See "About special report types" on page 44.
- See "About report formats" on page 44.

About backup reports

Backup reports display historical data about backup operations performed on the network.

You can display the following kinds of information:

Historical activity	Show job size, file count, job count, and duration.
Tape & media	Show tape library capacity and related information.
Risk analysis	Show the highest recovery point exposures.
Asset	Show client and server jobs.
Forecasts	Show forecast of size, job count, and file count.

Service level	Show successful jobs, failed jobs, and success rate.
Windows	Show size, job count, and file count on Windows setup.
Custom	Show custom reports.

The dash boards in the Monitors section display a Backup Monitoring table summarizing the status of backup jobs for hosts (servers) and for host file systems. Data is arranged according to your selections and covers the time period you indicated.

To move the status display

1. In the Backup Monitoring display, use the Prev Day and Next Day controls to move the status display back or forward by one day.
2. Use the Prev Week and Next Week controls to move back or forward by one week.

   In the Backup Monitoring display, you can drill down to display more detailed status and history information. For example, clicking the name of a client displays a list of the file systems backed up for that client. From the file system list, you can display details about backup jobs and, by drilling down one more level, details about individual attempts.

About recovery reports

Recovery reports display both historical and forecast data about data recovery operations performed on the network.

You can display the following kinds of information:

- Historical activity, showing job size, file count, job count, and duration
- Recovered client assets
- Forecasts, showing size, job count, and file count
- Service level, showing successful jobs and failed jobs

About cost reports

Cost reports display historical cost data for backup and recovery jobs. You can configure these reports to display composite data or detailed information at the asset level.

Some preliminary steps are required before you can display cost reports. You must first create at least one cost variable and formula of the type corresponding to the type of report you want to run (backup/recovery). After defining those cost elements, you use them to generate and display cost reports.

About special report types

Some reports differ from the majority in the way they are created or in the form of their output. The following topics describe these “special case” reports.

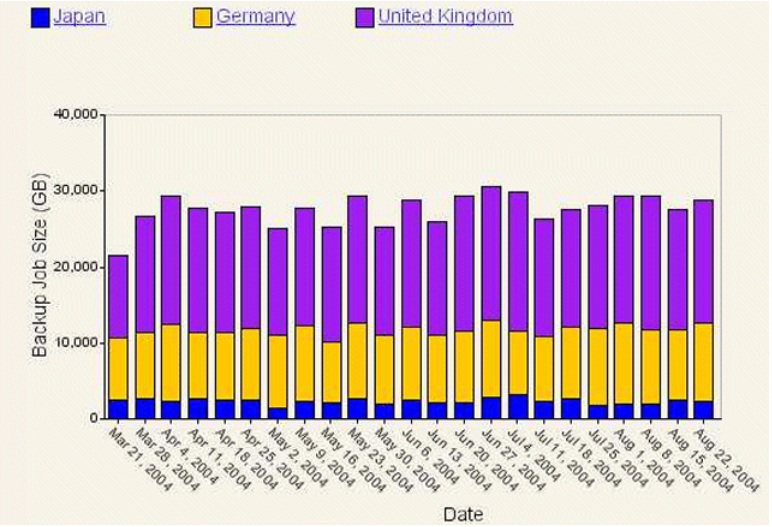
Recovery Point Exposure Report	In the event of catastrophic data loss, it is advantageous to have recently backed up all your important data. The longer the interval since your last backup, the greater the amount of lost data. The Recovery Point Exposure report displays all servers whose data has not been backed up within a recent period of time that you specify. This shows you which servers are most at risk.
Tabular Backup Report	This report is more highly customizable than most others. It lets you choose a set of table columns to display in the report, configure the order in which they display, and sort the table by column after generating the report. It is best to limit the scope of a tabular report to one or two view level objects and a short time frame, to keep from producing tables of an unwieldy length.
Job Status and Job Count By Level Reports	Many reports produce graphs with active hyperlinks that you can select to drill down and display report data aggregated at a lower view level. The Job Status and Job Count By Level reports produce graphs that do not permit drill-down to lower view levels, because the elements represented in the graph are not levels of the object view, but job success and failure rates. As a rule, if the graph legend for a report does not show view levels, you cannot select the active parts of the graph to drill down to a lower view level.

About report formats

Most types of reports available in Veritas Backup Reporter are fairly self-explanatory. For example: A Historical Activity report showing backup job duration for a group of hosts for the past six months. However, many reports fall into one of several broad, easily described format categories, and some report types are special cases that require explanation.

About graphical formats

Figure 3-1 Example of a Stacked Bar Chart



Veritas Backup Reporter reports have the following general graphical formats:

- Bar chart reports display stacked (segmented) bars showing subcategories within a category, for example the total size of each day's backup jobs broken out by geography. Some backup reports use a different bar-chart format, displaying clustered columns for easy comparison between two classes of objects or events.
- Rankings reports display a simple, horizontal bar graph showing all the data for each view level object, from greatest to least, within the selected time frame.
- Pie chart reports (or composition reports) display a simple pie graph showing all the data for each view level object within the selected time frame.
- Trending reports display a bar graph with a trend line superimposed over it, showing the average upward and downward trends of the data over time.
- Forecast reports display a line graph with a forecast line extending to future dates, using linear regression to predict values based on the trend of data within the report's time frame.

  Trending and forecast reports do not let you select the view level at which report data is aggregated. They always aggregate data at the top level of the view.

- Correlation reports compare two sets of data, such as backup job success rate and backup job count, to show how the number of jobs affects the success rate. The report displays a separate Y-axis for each data set.

Viewing numeric data in a graphical report

Graphical reports present data in a convenient, “at a glance” fashion. However, some precision may be lost when you use this format. When you are viewing a graphical report, ToolTips are available to provide the precise numerical data.

To view the numerical data on which a graphical report is based

- Move your mouse pointer over an area of the graph.

  The numerical data displays in a Tooltip.

About viewing data for a lower aggregate level

When you are viewing a backup report, you can easily view lower-level reports. When you click an area within a graph, the report refreshes to display data for the next lowest object level.

For example, in a Geography view, you could click a bar labeled Canada to display a bar chart showing data for Toronto and Vancouver. You could select the bar for a host to display data for the host’s file systems.

Saving the contents of a graphical report

You can save a copy of a graphical report to your workstation.

To save the contents of a graphical report

1. Right-click the report, and then click **Save Picture As**.
2. In the Save Picture dialog box, specify a directory path, file name, and format (such as .png).

   The report is saved as a graphic file.

Displaying tabular formats

When you are viewing a graphical report, you can view more detailed data in a table. This is helpful when you want to display precise numerical data for more than one object or event at the same time. It is also helpful when you want to capture the data in hard copy or in an email message.

To display the contents of a graphical report in a tabular format

1 Click **Show Table** at the top of the report display.

The report data displays in table format.

2 Select any column heading to sort the table by the data in that column: alphabetical order for text, chronological order for dates, and so forth.

Select the heading again to sort in reverse order.

3 To return to the graphical report, click **Show Chart**.

You might observe blank columns in tabular reports for non-NetBackup jobs. This happens when a column represents data that Veritas Backup Reporter obtains only from NetBackup hosts.

Using the reports portal pages

You use the My Reports page to run and display a personalized set of reports.

To display the My Reports page

1 Click the Reports tab.

This page functions as your personalized portal to Veritas Backup Reporter reports, running and displaying a personalized set of reports.

Similarly, each subtab under Reports has its own portal page (for example My Backup Reports), which you can also personalize. These subject-specific portal pages are sometimes referred to as My Reports pages.

When you load a portal page for the first time during a session, Veritas Backup Reporter runs that page's reports and displays data that is current. The reports are then cached so that, on subsequent page loads, they do not refresh.

2 To refresh the reports, click **Refresh all reports** at the top of the page.

Reports on portal pages are refreshed under three additional circumstances:

- When you schedule regular updates for cached reports
- When you modify a report in any way
- When the reports run for notification purposes

See "Refreshing cached reports" on page 51.

See "Refreshing cached reports" on page 51.

As your needs change, you can change the contents of your portal pages, adding new content and deleting content that you no longer need.

About selecting and displaying reports using the tree view

For each portal page, a tree view in the task pane provides access to your saved reports and to additional reports.

The first branch of the tree view is the My <Subject> Reports folder, for example My Backup Reports. This folder contains all of your saved reports for the indicated subject, and it helps you organize your reports into customizable sub-folders. Select a saved report to view it in the content pane.

Below My <Subject> Reports are additional folders representing other reports available for the indicated subject. Expand one of these branches to view the individual reports beneath it.

When you click a report in the tree view, the Custom Report Wizard displays in the content pane, giving you the chance to run the report with the specific characteristics you want, such as format, scope, and time frame.

See "Using and customizing default reports" on page 53.

Using quick links at the top of a displayed report, you can change the report, send the report data by email, and preserve the data in either online or printed format.

Creating sections on a reports portal page

The first step in displaying reports on a reports portal page is to create a section on the page to contain the reports.

Note: You must save a report prior to the following steps.

To create a new section on a reports portal page

1. Display a reports portal page.
2. In the My Tools list (in the task pane), click **Customize <Subject> Portal**
3. Click **Create** at the top of the list.
4. In the Create Section dialog box, type the name of the new section in the Name field.
5. In the Available Reports list box, select a report, and then click the right-arrow button to move the report to the Selected Reports list box.

   Repeat this step for each report you want to include.

6 In the Selected Reports list box, use the up and down arrow buttons to move reports up and down in the list.

7 Click **Save**.

The new section displays in the My <Section> Reports page.

Editing sections on a reports portal page

You can edit the sections on a reports portal page by renaming them and by adding and deleting reports.

To edit a section on a reports portal page

1 Display a reports portal page.

2 On the section's tab, click **Edit**.

3 Change the name of the section, if desired, by typing over data in the Section Name field.

4 Move reports into and out of the section by highlighting reports in the Available Reports the Selected Reports list boxes and using the left-arrow and right-arrow buttons.

In the Selected Reports list box, use the up and down arrow buttons to move reports up and down in the list.

5 Click **Save**.

The section is updated to display new contents on the My Reports page.

Deleting sections on a reports portal page

You can delete sections on a reports portal page. When you delete a section, the reports displayed in the section remain in the folders where you saved them.

To delete a section on a reports portal page

1 In a reports portal, on the section's tab, click **Delete**.

2 When a confirmation message displays, click **OK**.

The section is deleted from the page.

Managing the Reports folders

By default, all of your custom reports are saved in the top-level My <Subject> Reports folder for the indicated subject. To better organize your saved reports, you can create additional folders within either the My <Subject> Reports folders or the main My Reports folder.

To manage folders in the My Reports or My <Subject> Reports folders

1. Display a reports portal page.
2. In the My Tools list (in the task pane), select one of the following:
   - Manage “My Reports” Folders
   - Manage <Subject> Reports

   The content pane displays a list of the folders you have defined either in My Reports or in My <Subject> Reports, depending on what tab you have indicated. The list is alphabetical by folder name, but the names of subfolders (child folders) are concatenated to the names of their parent folders, for example: parent.child.
3. To create a new folder, do the following:
   - Click **Create** at the top of the list:
   - In the Create Folders dialog box, type a name for the new folder in the Name field.
   - From the drop-down list, select a parent folder for the new folder. (“My Reports” is the default, indicating the main My Reports or My <Subject> Reports folder.)
   - Click **Save**.
4. To rename a folder, do the following:
   - Click **Edit** to the right of the folder name.
   - In the Rename Folders dialog box, type a new name for the folder in the Name field.
   - From the drop-down list, select the name of the folder you are renaming.
   - Click **Save**.
     The folder is renamed. If the folder is a parent folder, its new name displays in the folders list for every subfolder (child folder).
5. To delete folders, do the following:
   - Check the names of one or more folders.
   - Click **Delete** at the top of the table.
   - Click **OK** to confirm the deletion.
     The folders are deleted; however, the reports they contained still exist within the My Reports folder. You can still access the reports in the task pane tree view.

You have completed and saved your updates to the My Reports folder. The subfolders display in the task pane for the My Reports page. They are also available for saving reports.

Refreshing cached reports

When you load a reports portal page for the first time during a session, Veritas Backup Reporter refreshes all reports on the page; that is, the data in each report display is updated. The reports are then cached so that, on subsequent page loads, they do not refresh.

You can arrange for some or all of your cached reports to be refreshed on a regular schedule.

To schedule regular updates for cached reports

1. On the console Settings tab, click **Report Cache Updates**.
2. In the Report Cache Updates window, click **Create**.
3. In the Create Report Cache Update dialog box, do the following:
   - In the Name field, type a descriptive name for the update.
   - Click **Enabled** to activate updates for the selected cached reports.
     The reports will be updated at the next scheduled interval. (Cancel the selection if you want to turn off updating for the time being.)
   - Select a time from the Schedule drop-down list. This is the schedule on which cached reports will be updated.
     To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
   - From the drop-down list, select one or more reports to update.
   - Click **Save**.
     The new cache update is saved. If the update is enabled, cached versions of the indicated reports are automatically updated according to the schedule you specified.

To change regularly scheduled updates for cached reports

1. On the console Settings tab, click **Report Cache Updates**.
2. In the Report Cache Updates window, click the **Edit** icon next to the name of the cache update.
3. In the Update Report Cache Updates dialog box, change one or more attributes, and then click **Save**.

   Your changes are saved.

Generating the library capacity forecast report

Veritas Backup Reporter 6.0 provides the Library Capacity Forecast report that shows the backup trend for future dates depending on maximum tape capacity.

To generate the Library Capacity Forecast report

1. Click **Reports > Backups** in the VBR console.
2. Click**Tape & Media Reports** on the Reports list.
3. Click **Library Capacity Forecast**.
4. On the Report Wizard, select the following:
   - Report Time Frame - Select period (for example, 1 month) or actual date range.
   - Report Time Frame Grouping - Select period (for example, 10 days or 2 weeks) by which the records are grouped.
   - Display Options - Select unit and total capacity operation.
     If you have selected User Defined as the total capacity operation, select the user defined values for the following parameters for each of the meadia type.
     - media type
     - maximum tape capacity
     - number of slots in a tape library
     - Alias x-axis
     - Alias y-axis
   - Forecast Parameters - Select filter parameters for forecasting, for example, Backup Media Type, Tape Library Manufacturer, and so on.
   - Exception Conditions - Select condition, either Total Backup Media Used Capacity or Average Backup Media Total Capacity.
5. Click **Run**.

The system generates the Library Capacity Forecast report showing backup trend for the dates selected.

Selecting total capacity operation

When you generate the Library Capacity Forecast report, the maximum tape library capacity is calculated depending on the following total capacity operations:

- Maximum

- Average
- Minimum
- User Defined

Using and customizing default reports

Veritas Backup Reporter provides a number of predefined (default) reports for backup and cost. Using the Report Wizard, you can manipulate the scope, time frame, and other attributes of these default reports to create reports that display the specific information you want.

As you work with different report types, the Report Wizard displays different parameters. Many of the parameters are used for multiple report types, and they appear in different combinations for each type.

Note: If you find that you need information presented differently than it is presented in the default reports, you can create custom reports. Use the Custom Wizard button in the Report Wizard to open the Custom Report Wizard.

See "Creating and using custom reports" on page 61.

The following topics describe basic information about using the default reports to display information that is specific to your enterprise:

- See "Using default reports" on page 53.
- See "Specifying the report scope and time frame " on page 54.
- See "Customizing an existing report" on page 55.
- See "Saving data in a report" on page 71.
- See "About Report Wizard parameters" on page 56.

Before you begin working with the default reports, you should become familiar with the following topics:

- See " About VBR report types" on page 42.
- See "About report formats" on page 44.

Using default reports

The first time you use Veritas Backup Reporter, after installation, you should load the default reports. After the reports have been loaded, they remain available to you indefinitely.

To load the default reports

1. Click **Reports > My Reports** in the VBR console.
2. Click **Generate Sample Reports** in the My Tools list (in the task pane).

   The default reports are loaded. The loading process may take a few minutes.

   After you load them, the following default reports are available for your use:

Backup reports	■ Backup history reports, including Week at a Glance and Rolling Eight Days ■ Backup risk analysis: recovery point exposure ■ Forecasts: job size, job count, and file count ■ Service levels ■ Time windows
Recovery reports	■ Historical activity: job size, job count, file count, and job duration ■ Forecasts: job size, job count, and file count ■ Service levels

Specifying the report scope and time frame

You can use the Report Wizard to create a report that is based on a default report.

See "About Report Wizard parameters" on page 56.

To specify the scope and time frame for a default report

1. Select a report subject from the menu bar on the My Reports page (for example, Backups).

   The My <Subject> Reports portal page displays, with a task pane on the left.
2. Expand a tree in the task pane, and then click the report subject (for example Asset - Client Count.).
3. If you are prompted to do so, select the report format (for example Stacked Bar), and then click **Continue**.

   See "About report formats" on page 44.
4. In the Report Wizard, define the report's scope by doing the following:
   - Select an object view category from the Within View drop-down list.
   - Select the view level you want the report to display from the Aggregate at drop-down list.

- If you want to filter the report to include only the data for a particular set of objects (instead of the data for all objects in the view), select the view level of the filtered objects from the Filter at drop-down list.
- If you selected a Filter at value, select one or more objects whose data you want to include in the report in the Select specific items list box.

See "About the Report On parameters" on page 56.

5 Define the report time frame by doing either one of the following:

- Click **Relative Date** to configure a relative time frame, and then click a number of hours, days, months or years using the Show Last drop-down lists.
  The report will display data collected within the specified time period, for example the last 3 months.
- Click **Absolute Date** to configure an absolute time frame, and then click a start time (month, day, year, and time of day) using the From drop-down lists, and a end time using the drop-down lists.
  The report will display data from the time period between the start and end dates.

See "About Report Time Frame parameters" on page 57.

6 Select values for one or more report parameters, depending on the category and type you have clicked for your report.

See "About Report Wizard parameters" on page 56.

7 Click **Run**.

The report displays. Click a hypertext link in the report (such as North America) to view the same report for the next lowest level (such as Canada).

8 To return to the Report Wizard and make changes to the report, click **Edit**.

See "Saving data in a report" on page 71.

Customizing an existing report

To create a report with a scope and time frame similar to a report you have already displayed, you do not need to run the Report Wizard from beginning to end.

To customize the scope and time frame for an existing report

1 Display a report in the console.

2 Click **Edit** at the top of the report display.

The Report Wizard displays, with parameters for the current report.

3 Change parameters as needed to configure the new report.

4 To access additional features for report data, click **Custom Wizard** to launch the Custom Report Wizard.

See "Creating and using custom reports" on page 61.

5 Click **Run**.

The new report displays.

6 To return to the Report Wizard and make more changes, click **Edit**.

See "Saving data in a report" on page 71.

About Report Wizard parameters

The Report Wizard displays a set of parameters that varies depending on the report type and the report format. The following reference sections describe each parameter that you may encounter:

- See "About the Report On parameters" on page 56.
- See "About Report Time Frame parameters" on page 57.
- See "About Report Time Frame grouping parameters" on page 58.
- See "About the Report Time Frame Trendline parameter" on page 58.
- See "About Filter options" on page 58.
- See "About Forecast parameters" on page 58.
- See "About the Retries Restriction parameter" on page 59.
- See "About the Target Performance parameter" on page 59.
- See "About the Cost Formula parameter" on page 59.
- See "About Display Option parameters" on page 59.
- See "About the Define Viewable Columns parameter" on page 59.
- See "About the Condition parameters" on page 60.

About the Report On parameters

Use the Report On parameters to define the report scope.

You can select up to four different values:

Within view	The report will display data for objects in the selected view.

Aggregate at	Select the level at which to group data in the report. This setting determines the way data will be grouped and labeled in the report. For example, when reporting on the Client Count view, you could aggregate data at the Top level—in which case the report would display data for all servers as a single unit—or at the Client level, in which case the report would display data for each client individually. **Note:** The Aggregate at field is not available for some report types which only display data at the Top level of the object view.
Filter at	Select one or more objects within the specified view to limit the amount of data that is collected for the report. Data is collected only for the specified object type.
Select specific item(s)	You can further limit the amount of data collected by selecting individual objects within the filtered scope, such as file systems on a host. Objects in this list may be "real" objects such as hosts and file systems, or they may be user-created nodes in the view, depending on the view level at which you set the filter. For example, when reporting on the Client Count view, you can filter the report at the Client level and select individual clients to include in the report. This does not mean that the clients will appear individually in the report (your selection in the Aggregate at field determines that); it means that only data from those clients will be included in the report. **Note:** After you select a Report On parameter, wait for the console screen to refresh before clicking additional parameters.

About Report Time Frame parameters

Use the Report Time Frame parameters to define the beginning and end of the time interval to be covered by the report. You can choose either absolute dates, for example March 1 to April 1, or relative dates, for example the last 3 months.

If you plan to save reports for later viewing or for scheduled distribution by email, it is best to choose a relative time frame, so that the report always represents the most recent data relative to the time the report is accessed or emailed.

It is best to configure trending and forecast reports with absolute time frames. If you chose a relative time frame, such as "the last 6 months," the database would probably contain incomplete data for the present month, and the last bar in the graph would be shorter as a result. This would skew trend lines and forecast lines downward, giving a false result. If you decide to use a relative time frame, choose a granular time period such as hours or days to minimize the skew.

About Report Time Frame grouping parameters

You use the Report Time Frame Grouping parameters to display and filter report data.

To use the drop-down lists in Report Time Frame Grouping to display data

- Use the drop-down lists in Report Time Frame Grouping to select the unit of time (hours, days, weeks, months or years) in which the report should display its data.

  For example, if you want your report to show long-range usage statistics for all NetBackup clients, you might select 1 Month or 3 Months. The report data will be grouped by 1-month or 3-month intervals.

  As another example, to display statistics for a single client over the most recent week, you could select 1 Day to see day-by-day information for the client.

About the Report Time Frame Trendline parameter

Use the Report Time Frame Trendline parameter to specify whether the report should include a trendline, and the length of the interval between points on the trend line (in days).

See "About Trendline and Forecast parameters (Trending reports)" on page 66.

About Filter options

Filter options enable you to narrow the scope of your report beyond the selections you made in using the Report On parameters. For example, you can filter a backup report to include data for full backup jobs, incremental jobs, or all jobs.

For some report types, you can use drop-downs in the Report Wizard window to click filter options. For example, the Backup Level Filter option specifies the type of backup job level (full backup, incremental backup, or both) that the report should include in its data. Attempt Status specifies whether to display data for backup jobs or attempts.

Expand Show Advanced Filters at the bottom of the window to click additional filtering criteria for the report display. The list of available criteria depends on the report format and type.

See "About Filter parameters" on page 70.

About Forecast parameters

Use Forecast Parameters to select the length of a report's forecast line, in periods. The length of a period is determined by the Report Time Frame Grouping

parameter. If that parameter is set to group data by month, for example, you can specify 6 forecast periods to generate a 6-month forecast line.

About the Retries Restriction parameter

Use the Retries Restriction parameter to specify whether the jobs counted for the report should include only the last tried job or all tries for a given backup host.

About the Target Performance parameter

Use the Target Performance parameter to click where a report draws the target line, to which you compare the actual performance shown.

About the Cost Formula parameter

Use the Cost Formula parameter - applicable only for Cost reports - to click the cost formula you want to use to calculate chargeback costs for the report.

About Display Option parameters

Use the following Display Options parameters to control the way data will be labeled in the report display:

- Use the Display Unit parameter to select the size units for reports that display quantities of storage capacity. You can choose from KB, MB, GB, and TB.
- For rankings reports, use the Display Top Rankings parameters to click the number of items to display in the ranking, and the order in which to display them.

  Examples: `5 Descending`, `10 Ascending`
- Use the Alias X-Axis Name and Alias Y-Axis Name parameters to provide labels for the axes in a bar chart, distribution, or trending report. If you leave these fields blank, default labels are provided.
- Use the Report Description field to provide an optional text description. This is useful when you plan to distribute the report by email. A default description is provided for almost all reports.
- Use the Table Rows Per Page drop-down list to specify how many rows display in each page of a tabular report.

About the Define Viewable Columns parameter

Use the Define Viewable Columns parameter to click the columns that display in a tabular report. In the Available Columns list box, click a column you want to include in the tabular report and then click the right single-arrow button to move

the column to the Selected Columns list box. You can also move all columns from one box to the other simultaneously using the double-arrow buttons.

To configure the order in which columns display in the report

- Click a column in the Selected Columns list box and then click the up or down arrow to move it higher or lower in the list.

  The first column in the list displays on the left end of the report while the last column displays on the right end.

About the Condition parameters

In the Exception Conditions section of the Report Wizard window, specify exception conditions for notification. Exception conditions represent potential problems, for example an unusually high percentage of backup job failures or an unusually low quantity of data being backed up.

Each exception condition is defined by assigning threshold values for a particular metric, such as Success Rate or Total Backup Job Size. You can set a low threshold, a high threshold, or both.

After you specify your conditions, you can configure Veritas Backup Reporter so that when a condition is true, an alert is triggered and/or an email notification is sent.

To define report conditions

1. Select a metric in the Add Condition To field, and then click **Go**.
2. Set threshold values for the metric using the following fields:

Scale	If applicable, select the scale in which to measure, for example a storage size (like GB) or a time period (like days). The label on this field corresponds to the metric you selected in 1.
Low Threshold	Specify the low threshold. When a measurement falls below this value, the condition is met.
High Threshold	Specify the high threshold. When a measurement exceeds this value, the condition is met. **Warning:** Avoid setting ranges (in other words, both low and high threshold values) for measurements that might return non-numeric data.
Invert	Switch the Low Threshold and High Threshold values.

3 Repeat 1-2 to create additional conditions.

4 To delete a condition you no longer need, check **Delete**.

As an example, you could define a backup report with the following conditions:

- Success Rate: Low threshold 80%
  The condition is met whenever the success rate falls below 80 percent.
- Total Backup Job Size: Low threshold 500 GB, high threshold 1000 GB
  The condition is met whenever the total quantity of backed-up data falls outside the range of 500-1000 GB.

Creating and using custom reports

In addition to using the reports that come by default with Veritas Backup Reporter, you can use the Custom Report Wizard to create custom reports that are unique to your installation.

See "Creating and using custom reports" on page 61.

After creating a custom report, you can modify the report, print, save, and email it to the concerned persons.

As you work with different report types, the Report Wizard displays different parameters. Many of the parameters are used for multiple report types, and they appear in different combinations for each type.

Before you begin creating custom reports, you should become familiar with the following topics:

- See " About VBR report types" on page 42.
- See "About report formats" on page 44.

The following topics describe how to create and use custom reports:

- See "Creating a custom report" on page 61.
- See "About Custom Report Wizard parameters" on page 63.
- See "Modifying a custom report" on page 71.
- See "Saving data in a report" on page 71.

Creating a custom report

You can create a custom report with various parameters that may appear in the wizard.

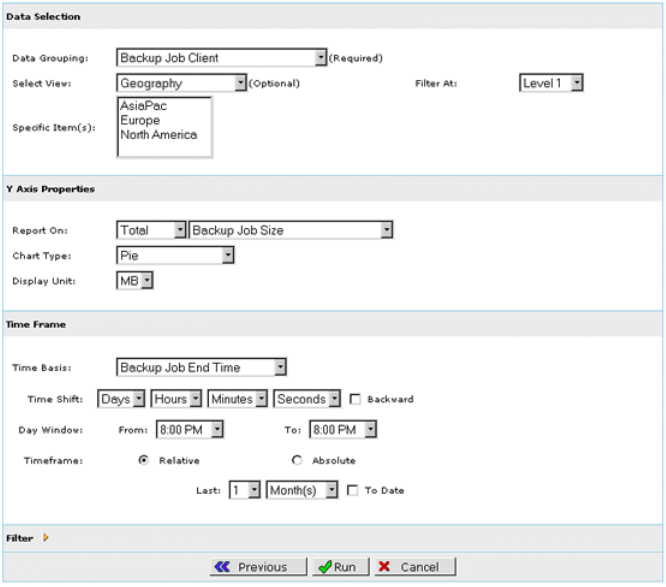
See "About Custom Report Wizard parameters" on page 63.

To create a custom report

1. Click **Reports > Custom** in the console.
2. Click **Custom Report** in the task pane.
3. In the Custom Report Wizard, in the Select Report Category and Type panel, do the following:
   - Select a category from the Category drop-down list.
     You can select from several types of backup/recovery and cost reports.
   - Select one of the following from the Report Type drop-down list:

Top ranking	Display data for the leading objects in the specified metric, for example the hosts with the greatest number of successful backup jobs.
Trending	Display data as a graph that shows fluctuations over time and, optionally, projects trends into the future.
Distribution	Display groupings or objects or resources in a pie-chart, a graphical format.
Tabular	Display data in the form of a table.

4. Click **Next**.



5 In the second panel of the Custom Report Wizard, select values for one or more report parameters, depending on the report category and type you have selected.

See "About Custom Report Wizard parameters" on page 63.

As you select parameters, the content pane may refresh to display additional selections. For example, when you select a view filter, you are then given a choice of items on which to filter the report display.

6 Click **Run**.

The custom report displays.

7 If you want to return to the Custom Report Wizard and make changes to the report, click **Edit**.

See "Saving data in a report" on page 71.

About Custom Report Wizard parameters

The Custom Report Wizard displays a set of parameters that varies depending on the report type. The following reference sections describe each parameter that you may encounter:

- See "About Data Selection parameters" on page 63.
- See "About Data parameters" on page 64.
- See "About the Viewable Columns parameters (Tabular reports)" on page 65.
- See "About Trendline and Forecast parameters (Trending reports)" on page 66.
- See "About time frame parameters" on page 67.
- See "Defining report conditions" on page 69.
- See "About Filter parameters" on page 70.

About Data Selection parameters

Use the Data Selection parameters to define the report scope.

You can select up to four different values:

Data Grouping	The way in which report data will be grouped, or aggregated. Example: Status groups backup jobs according to their status. Example: Host: OS Type groups hosts according to host platforms such as Solaris and Windows. To use a different grouping from the ones listed, click **View Aggregation Level Node**, and then select a level from the Aggregate at drop-down list. For example, when reporting data in the Geography category, you could aggregate data at the Top level, in which case data would display for all servers as a single unit, or a lower level, in which case data would display according to countries, cities, or even individual servers.
Within View	Select an object view category. Object view categories are defined by your system administrator and are the same ones used in the Views area of the console. Examples: Geography, Application
Filter at	Specify the hierarchical level, if any, for filtering the object view category. Examples: Level 1, Level 3
Specific items	When you select a filter, you are given a choice of items on which to filter the report display. Examples (with Geography and Level 2 selected): Japan, Canada Examples (with Line of Business and Level 1 selected): Finance, HR

About Data parameters

Use the data parameters to define the measurements to be collected for trending, ranking, and distribution reports.

Note: For ranking reports, the wizard displays data parameters under the heading Rank By. For trending reports, the wizard displays data parameters under the heading Y Axis Properties and enables you to pick two different sets of data to plot.

You can select from the following values:

Report On	Define the report's scope using the drop-down lists: ■ The mathematical category Examples: Total, Minimum, Maximum, Average, Percent ■ The type of data Example: Backup Job Total Size ■ The backup job group ID (if multistream jobs are grouped together) Example: BackupGroup1
Top	The number of items to display in the ranking, and the order in which to display them. Available only for Top Ranking type Examples: Top 5 Descending, Top 10 Ascending
Display Unit	For numeric data types, such as Backup Job Total Size, the units in which to display the data. Examples: MB, GB.
Chart Type	The report format. Additional formats may be available depending on the values specified in Report Data. See "Using and customizing default reports" on page 53.
Target	For trending reports, select the radio button and type a value in the text box to include a target level or threshold in the report display. The target value will display as a horizontal line, useful for making quick visual comparisons between the target value and the actual values being reported.
Alias X-Axis Name or Alias Y-Axis Name	A label for the graph axis that reflects quantity (as opposed to time). For trending reports, this is the vertical (Y) axis. For other reports it is the horizontal (X) axis. If you leave this field blank, a default label is provided.
Report Description	Description to display along with the report. If you leave this field blank, no description is provided by default.

About the Viewable Columns parameters (Tabular reports)

Use the Viewable Columns parameters to establish the column titles for a tabular report.

To populate the table columns

1. In Available Columns, select one or more values for table columns, and then click **Add**.

   Examples: Host Name, Status, Backup Job Group ID

2. In Size Display Unit, select the scale in which to display storage values in the table:

   - KB
   - MB
   - GB
   - TB

3. In Duration Display Unit, select the units in which to display time intervals in the table:

   - Seconds
   - Minutes
   - Hours
   - Days

4. In Selected Columns, after selecting table columns, use the controls in Selected Columns to define the way in which data is displayed in each column.

   Examples: Selected Column: Job Duration, Host OS Type

   Sort order: Ascending, Descending

   Operation: Average, Maximum, Total

   In the list of selected columns, use the Up, Down, and Remove controls to specify the order in which the columns appear, or to delete columns you no longer need.

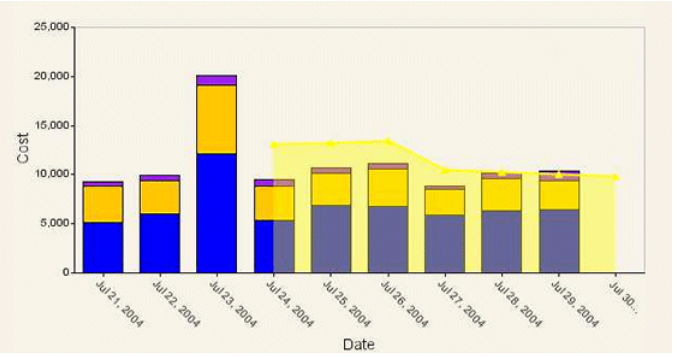
5. Top: The number of items or objects to display in the table.

   Example: If the first column is Job Duration, the value 10 displays data for the 10 longest backup jobs in terms of duration

About Trendline and Forecast parameters (Trending reports)

Use the Trendline and Forecast parameters to establish characteristics that are unique to trending reports. Using these parameters, your report can project future trends by averaging actual data from the recent past.

Figure 3-2 Example of a Report with a Trendline (Shown in Yellow)



To specify trendlines

1 In Show trendline with moving average, check the checkbox and use the drop-down list to specify the number of data points to factor into the average.

   At each interval on the graph, the trendline shows a moving average of the most recent data points.

   Example: 3 displays a trendline that, at each interval, shows the average of the current data point and the two previous data points.

2 In Show forecast with forecast periods, check the checkbox and use the drop-down list to specify a number of forecast periods (intervals).

   Example: 12 shows forecast data for the next 12 months (if the Group By is 1 month).

About time frame parameters

You use the Time Frame parameters to define the report's overall time frame and the intervals for which data is reported.

Note: For trending reports, the wizard displays time frame parameters under the heading X Axis Properties.

You can select from the following values:

X Axis Type	For trending reports, the metric used to define the graph's horizontal (X) axis. Examples: `Backup End Time`, `Host Name`

Alias X-Axis Name	For trending reports, a label for the horizontal (X) axis. If you leave this field blank, a default label is provided.
Group By	For trending reports, the unit of time into which measurements in X Axis Type are grouped. Example: 1 Day groups all measurements by one-day intervals. The default one-day interval runs from midnight to midnight.
Time Basis	The metric used for assigning a time to each item in the report, if not specified by the X Axis Type parameter. Example: The start time or the end time for each backup job.
Time Shift	Move the starting point for a defined interval (such as minute, hour, day, or month) to one that more closely matches your own operations. Click a value from each of the drop-down lists: days, hours, minutes, and seconds. Example: 30 seconds shifts the minute interval so that it begins at 30 seconds after the minute rather than exactly on the minute. Example: 14 days shifts the monthly interval so that it begins on the 15th day of the month rather than on the first day. Check **Backward** to move the starting point backward in time. Example: 6 hours Backward shifts the daily interval to 18:00 - 18:00 from midnight-midnight. (18:00 is equivalent to 6:00 PM.). Use the Day Window value together with Time Shift to shorten the length of the daily interval from 24 hours.
Day Window	Specify the time interval that constitutes one day. Select values from the From and To drop-down lists. Example: 6:00 PM to 6:00 AM Example: 12:00 AM (midnight) to 12:00 PM (noon)
Timeframe	Define the beginning and end of the time interval to be covered by the report. You can choose either absolute dates, meaning that the report's contents will remain static whenever you display it, or relative dates, meaning that the report will always display data collected over the most recent time interval. **Note:** The Relative Date setting is especially useful for reports that you plan to generate on a regular basis. Such reports will always show data collected over the most recent time interval.

To configure an absolute or relative time frame

- Do one of the following:

Configure an absolute time frame.	■ Click **Absolute Date** ■ Select a start time (month, day, year, and time of day) using the From drop-down lists, and a end time using the To drop-down lists. Alternatively, use the Unbounded checkboxes to indicate an open-ended time interval. The report will display data from the time period between the start and end dates. Example: `From MAR 1 2004 12:00 AM to APR 30 2004 12:00 AM` Example: `Unbounded to APR 30 2004 12:00 AM`
Configure a relative time frame.	■ Click **Relative Date**. ■ Select a time interval using the Last drop-down lists. The report displays data collected within the specified time period, up to the current time Examples: `Last 21 Days`, `Last 2 Quarters`

Defining report conditions

Expand **Exception Conditions** in the Custom Report Wizard window to specify exception conditions for notification. Exception conditions represent potential problems, for example an unusually high percentage of backup job failures or an unusually low quantity of data being backed up.

Each exception condition is defined by assigning threshold values for a particular metric, such as Success Rate or Total Backup Job Size. You can set a low threshold, a high threshold, or both.

After you specify your conditions, you can configure Veritas Backup Reporter so that when a condition is true, an alert is triggered and/or an email notification is sent.

See "Using reports for notification" on page 123.

As an example, you could define a backup report with the following conditions:

- Success Rate: Low threshold 80%
  The condition is met whenever the success rate falls below 80 percent.
- Total Backup Job Size: Low threshold 500 GB, high threshold 1000 GB
  The condition is met whenever the total quantity of backed-up data falls outside the range of 500-1000 GB.

To define report conditions

1. Select a metric in the Add Condition To field, and then click **Go**.
2. Set threshold values for the metric in the following fields:

Scale	If applicable, select the scale in which to measure, either a storage size (like GB) or a time period (like days). The label on this field corresponds to the metric you selected in 1.
Low Threshold	Specify the low threshold. When a measurement falls below this value, the condition is met.
High Threshold	Specify the high threshold. When a measurement exceeds this value, the condition is met. **Warning:** Avoid setting ranges (in other words, both low and high threshold values) for measurements that might return non-numeric data.
Invert	Switch the Low Threshold and High Threshold values.

3. Repeat 1-2 to create additional conditions.
4. To delete a condition you no longer need, check **Delete**.

About Filter parameters

You can use Filter parameters to obtain additional filtering capability for the report you want to display.

Following are some examples of the ways in which you can filter the model:

- Host Discovered Backup Client
- Host Operating System

To specify additional filtering criteria

1. Expand **Filter** at the bottom of the Custom Report Wizard window.

   The list of criteria depends on the report category and type you have selected.
2. For each filtering criterion you want to use, check the criterion name, and then specify one or more values using the fields provided.

Modifying a custom report

If you want to create a new custom report that is similar to one you already have, you do not need to start the Custom Report Wizard from scratch.

To customize an existing report

1. Display a custom report in the console.
2. Click **Edit**.

   The second panel of the Custom Report Wizard displays, with parameters for the current report selected.
3. Change parameters as needed to create the new custom report.
4. Click **Run**.

   The new report displays. Otherwise, save the report.

   See "Saving data in a report" on page 71.
5. To return to the Custom Report Wizard and make more changes, click **Edit**.

Saving and preserving report data

You can save the contents of reports you have customized or new reports you have created. You can also preserve report data in files or print the data.

The following topics contain more information about saving and preserving report data:

- Saving data in a report
- Exporting report data to a file
- Printing reports

Saving data in a report

After you create or customize a report, you can save it for later viewing or for use in sending notifications to users.

After you create and save reports, you can use them in any of the following ways:

- View saved reports by selecting them from the task pane in the My <Subject> Reports page.
- Add saved reports to a portal page.
  See "Editing sections on a reports portal page" on page 49.
- Email saved reports to interested people on a regular basis.

- Trigger alerts to notify staff members of potential problems.

To save data in a report

1. Create and display a report.
   - See "Specifying the report scope and time frame " on page 54.
   - See "Customizing an existing report" on page 55.
   - See "Creating a custom report" on page 61.
2. Click **Save As**.
3. In the Save Report dialog box, type a name for the report in the Report Name field.
4. Select a folder in which to save the report in the Save Under field.
5. To add the report to one of you're my <Subject> Reports portal pages, select the page in the Add to main portal section drop-down list.

   See "Using the reports portal pages" on page 47.
6. Check the checkbox to add a line break before the report.

   The report displays on a separate line on the portal page.
7. Check the checkbox to overwrite any existing report that has the same name.
8. To schedule reports to be added to emails, select a scheduled email in the Schedule report for email drop-down list.
9. Click **Save**.

   The My <Subject> Reports portal page displays, and the report is saved in the folder you specified.

Exporting report data to a file

Veritas Backup Reporter provides two ways of preserving report data in files:

- Export the report you are currently viewing in the console window, using the procedure in this section.
- Arrange for a report to be archived at regularly scheduled intervals.

In both instances, the report data is exported to a file in either comma-separated (CSV) or tab-separated (TSV), XML, or HTML format. You can then open the file using other applications, like a spreadsheet program or a text editor.

To preserve the report you are currently viewing

1. Display a report in the console.
2. Click **Export to File**.

3 In the Export Report Options dialog box, in the Name field, type a name for the export operation:

The name should be descriptive enough that you can click it from a list.

4 Click **Enabled** to activate the export operation.

Report data will be exported at the next scheduled interval. (Cancel the selection if you want to defer the export operation until later.)

5 From the Schedule drop-down list, select a schedule.

The schedule determines the time and days on which report data is exported.

6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

7 Select one of the following export file formats:

HTML	Display on an internal Web site. Unlike the other formats, HTML preserves the original format of the data as well as any graphics in the original report.
XML	Can be imported (using user-written scripts) by other programs like databases or billing applications.
CSV (comma-separated)	Use with spreadsheet programs.
TSV (tab-separated)	Compatible with word-processing applications and text editors.

The format you choose depends on how you want the data to be displayed and manipulated.

8 Click **Export**.

9 If you are prompted, specify whether you want to open the file or save it on your computer's file system.

The report data is saved to a file in the specified format.

Printing reports

You can print the report you are currently viewing in the console window.

To print a report

1. Display a report in the console.
2. Click **Print**.
3. In the Print dialog box, select a printer and adjust printer settings as required, and then select one of the following:
   - OK
   - Print

   The report is queued to the printer you specify.

Running custom database queries

You can use the Saved Query Tool (or SQL Tool) to create and run custom queries of VBR database of logged events, backup jobs, media usage, and change requests. In this way, an administrator can get information that is tailored to your enterprise's operating environment.

Using the Saved Query Tool, you can create and save the SQL database queries you plan to run frequently.

The following topics describe basic information about using and managing custom database queries:

- See "Creating and saving new database queries" on page 74.
- See "Running database queries" on page 75.
- See "Modifying and copying saved database queries " on page 76.
- See "Viewing the list of saved database queries" on page 77.
- See "Deleting saved database queries " on page 77.

Note: You can also run SQL queries using a command-line interface.

For more information, see the *Veritas Backup Reporter Administrator's Guide*.

Creating and saving new database queries

Use the Saved Query Tool to create a new SQL database query and save it for future use.

To create a new query

1. On the console Report > Customs tab, in the task pane tree view, expand **Custom Queries**, and then click **Create New Query**.
2. In the Add Query dialog box, type the following:

Title	The title of the query. It should be descriptive, yet short enough to display in a table.
Category	The Query category. If the category you specify does not exist, Veritas Backup Reporter will create a new category with that name. To add a new entry to an existing category, you must type the category name exactly as it appears in the table of saved database queries.
Out File (optional)	The directory path and name of the file to which query results will be written.
SQL Statement	The SQL code that defines the query, for example: `LOCATION = 'TORONTO'AND STATE != 'CLOSED' AND DATE_OPENED > '2004-04-15'`
Description	A detailed description of the query, for example `Events for Toronto hosts, opened after 15 April 2004 and not yet closed.`

3. Click **Add** to save the new query.

   The new query displays in the table of saved database queries.

Running database queries

You can run saved SQL database queries or create instant queries for one-time use.

You can also create a new SQL database query and run it without saving it.

To run a saved database query

1. On the console Reports > Custom tab, in the task pane tree view, expand **Custom Queries**, and then click **All Saved Queries**.

   The Saved Query Tool displays a table of saved database queries.
2. Select the query you want to run.

   The query runs, and the results display in the content pane.

To run an instant database query

1. On the console Reports > Custom tab, in the task pane tree view, expand **Custom Queries**, and then click **Run Query**.
2. In the Run Query dialog box, type (or paste from your system clipboard) SQL code in the SQL Statement text box, and then click **Run It!**.

   The query runs, and the results display in the content pane.
3. To modify the query and run it again, click **Back**.

Modifying and copying saved database queries

As your needs change, you can modify existing SQL database queries. You can also create new queries by copying existing queries and changing some of their characteristics.

To modify or copy a saved query

1. On the console Reports > Custom tab, in the task pane tree view, expand **Custom Queries**, and then click **All Saved Queries**.

   The Queries Tool displays a table of saved database queries.
2. On the line for the query you want to modify, click **Modify**.
3. In the Modify SQL Query dialog box, replace text in the fields as desired.

   See "Creating and saving new database queries" on page 74.

   The new or modified query is saved and can be viewed in the table of saved database queries.
4. To have the query prompt for user input when it runs, check one or more checkboxes in the Prompt For area.
5. Do one of the following:

   - To create a new query and preserve the original query without modifications, click **Clone**.
   - To modify the original query, click **Modify**.
     If you click Clone without having modified the query name, the new copy is saved as Copy of <QueryName>, where <QueryName> is the name of the original query.
     You can change this name by invoking the Modify Query dialog box for the new copy.

Viewing the list of saved database queries

You can view all saved database queries from the Operations page of the VBR console.

To view saved database queries

1. On the console Reports > Custom tab, in the task pane tree view, expand **Custom Queries**, and then click **All Saved Queries**.

   The Queries Tool displays a table of saved database queries.

2. Select a query in the table to view a details page for that query.

Deleting saved database queries

Use the Saved Query Tool to delete saved SQL database queries that you no longer need. Deleting a saved query removes it permanently from the database.

To restore a deleted query, you must recreate the query manually.

To delete a saved query

1. On the console Reports > Custom tab, in the task pane tree view, expand **Custom Queries**, and then click **All Saved Queries**.

   The Queries Tool displays a table of saved database queries.

2. On the line for the query you want to delete, click **Delete**.

3. Click **OK** to confirm deletion.

Chapter 4

Managing cost analysis and chargeback for services

This chapter includes the following topics:

Generating cost reports

The Veritas Backup Reporter chargeback feature is a tool you use to evaluate IT services costs for your organization. You can create cost rates and formulas that enable you to run reports that show costs for different levels of your organization.

Veritas Backup Reporter provides organizations with a tool to evaluate the cost of the IT services they consume. A financial officer, for example, can run cost reports to:

- Determine which divisions of the organization are the largest consumers of data recovery services
- Do a cost-benefit analysis of providing data backup every day versus three times per week
- Project future IT costs for budget planning

Using the cost chargeback feature in Veritas Backup Reporter, you can define chargeback costs for several aspects of basic IT services, for example:

- Cost per backup job
- Cost per backed-up GB of data
- Cost per restore job
- Cost per restored GB of data

You can run the Formula Modeling Tool to estimate baseline rates for the IT services in which you are interested.

See "Modeling chargeback costs" on page 80.

To generate cost reports

1. Create variables for assigning costs to the service types.

   See "Creating and managing cost variables" on page 84.

   To reflect changes in the rates for specific services, Veritas Backup Reporter offers the flexibility of creating more than one variable for a service type or of including more than one rate in a single variable.

2. Create formulas that apply one or more of these variables to determine the cost of a service.

   See "Creating and managing cost formulas" on page 86.

   For example, you can create a Backup Service formula that uses two variables: cost per backup job and cost per backed-up GB. When you run a report using the formula, the report calculates both costs and represents the total in its graphical display.

3. Generate the cost report.

   See "Generating the cost report" on page 88.

Modeling chargeback costs

The Formula Modeling Tool offers an easy way for you to estimate baseline rates for the IT services you provide. Using historical data, it provides you with an estimate of how much it costs your organization to provide a specific kind of service.

For example, suppose you anticipate spending $500,000 over the next year to provide backup services throughout your enterprise. How much should you plan to charge for each kilobyte of data that is backed up? By inserting the metric `Daily Occupancy`into the modeler, along with the amount `$500000`, you can obtain a per-kilobyte estimate that is based on the backup activity you performed last year.

To estimate chargeback costs using the Formula Modeling Tool

1 On the console Costs tab, click **Formula Modeling Tool**.

The tool launches, displaying a dialog window.

2 Use the following Report Grouping parameters to define the model's scope:

Within View	Optionally, select a view category. Examples: `Geography`, `Application`
Filter at	If you selected a view category, specify the hierarchical level, if any, for filtering the category. Examples: `Level 1`, `Country`
Specific items	If you selected a level for filtering, select one or more individual items on which to filter the report display. Examples (with `Geography` category selected): `Asia`, `Europe`, `North America`

3 Use the following Metric Selection parameters to specify the metric whose rate you want to estimate:

Select Metric	Select a metric, or category of service. Example: `Daily Occupancy`
Enter amount	Specify the total amount of money, in dollars, you expect to charge for service within that category in a given time frame. Examples: `$50000`, `$10,000`, `$10000.00`

4 Use the following Time Frame parameters to define the time intervals for which data is modeled:

Group By	The unit of time to be covered by your estimate. Example: `1 Day` provides a per-day cost estimate. The default one-day interval runs from midnight to midnight.

Time Shift	Move the starting point for a defined interval (such as minute, hour, day, or month) to one that more closely matches your own operations. Select a value from each of the drop-down lists: days, hours, minutes, and seconds. Example: `30 seconds` shifts the minute interval so that it begins at 30 seconds after the minute rather than exactly on the minute. Example: `14 days` shifts the monthly interval so that it begins on the 15th day of the month rather than on the first day. Check **Backward** to move the starting point backward in time. Example: `6 hours Backward` shifts the daily interval to 18:00 - 18:00 from midnight-midnight. (18:00 is equivalent to 6:00 P.M.). Use the **Day Window** value together with **Time Shift** to shorten the length of the daily interval from 24 hours.
Day Window	Specify the time interval that constitutes one day. Select values from the From and To drop-down lists. Example: `6:00 P.M. to 6:00 A.M.` Example: `12:00 A.M.` (midnight) `to 12:00 P.M.` (noon)

Timeframe

Define the beginning and end of the time interval to be covered by the estimate. You can choose either absolute dates, meaning that the estimate's contents will remain static whenever you display it, or relative dates, meaning that the estimate will always reflect data collected over the most recent time interval.

Do one of the following:

- Click **Absolute** to configure an absolute time frame. Then select a start time (month, day, year, and time of day) using the From drop-down lists, and a stop time using the To drop-down lists. (Alternatively, use the Unbounded checkboxes to indicate an open-ended time interval.) The estimate will reflect data from the time period between the start and end dates.

  Example: `From MAR 1 2004 12:00 A.M. to APR 30 2004 12:00 A.M.`

  Example: `Unbounded to APR 30 2004 12:00 A.M.`
- Click **Relative** to configure a relative time frame. Then select a time interval using the Last drop-down lists. The estimate will reflect data collected within the specified time period, up to the current time.

  Examples: `Last 21 Days`, `Last 2 Quarters`

  The Relative setting is especially useful for estimates that you plan to generate on a regular basis. Such estimates will always reflect data collected over the most recent time interval.

5 Expand the Filter section at the bottom of the Formula Modeling Tool window to select additional filtering criteria for the model.

  The list of criteria depends on the metric you have selected.

  Following are some examples of the ways in which you can filter the model:

  - Host Discovered Backup Client
  - Host Operating System

6 Click **Next**.

  Veritas Backup Reporter displays the results.

7 Click **Back to Formula Modeling Tool** to try the model with different values, or to run a new model.

Creating and managing cost variables

Cost reports in Veritas Backup Reporter are based on user-defined variables that define the cost of various services.

Typically, each service will be represented by one variable that reflects the cost of the service, for example $1.00 per backup job. However, you can account for rate changes in one of two ways: by creating two variables for the same service (which you will later include in a single cost formula) or by incorporating both rates into a single variable. For example, a single variable can incorporate the rate of $1.00 per backup job until 31 December 2004 and the rate of $1.25 per backup job starting on 1 January 2005.

Creating cost variables

The first step in setting up Veritas Backup Reporter to run cost reports is to create the variables that define the cost of various services.

To create a new cost variable

1. On the console Costs tab, click **Step 1 - Create Cost Variables**.
2. In the content pane, click **Create** at the top of the list.
3. In the Create Cost Variables dialog box, type a name for the variable in the Variable Name field.
4. Select a metric from the drop-down list in the Variable Metric field.

   Examples: `Job Count`, `Job Size (GB)`

5 If necessary, select additional parameters to refine the metric you selected.

For Backup Job Count and Backup Job Size:

Job Type	Measure costs for a specific type of job, for example `Backup` or `Restore`. The default is `Archive`.
Job Policy Type	Measure costs for jobs that use a specific policy type. In NetBackup, the policy type determines the type of clients that can be part of the policy and, in some cases, the types of backups that can be performed on the clients. Examples include `DB2`, `Sybase`, and `MS-Exchange-Server`. The default is `Standard`.
Storage Vendor	Limit the search to storage devices from a specific manufacturer, for example `EMC` or `Hitachi`. The default is `All`.
RAID Level	Limit the search to LUNs having a certain RAID level, for example `RAID 5` or `RAID 1+0`. The default is `All`.
	(Other metrics do not require additional parameters.)

6 Add one or more date ranges and associated rates using the drop-down lists for Month, Day, Year, and Time and by typing a cost per service unit (such as backup jobs or backed-up GB) in the Rate field.

You only need one date range.

7 Optionally, to add more date ranges, click **Add New Range**.

This can be useful for defining multiple date ranges to represent historical—or future—changes in service costs. You can also modify the variable later to add or delete date ranges as costs change.

8 Click **Save Variable**.

You have now finished creating a new cost variable. You can now use that variable to build formulas that form the basis for cost reports.

See "Creating cost formulas" on page 86.

Modifying and deleting cost variables

You can update cost variables and formulas without having to recreate the reports that rely on them. For example, you could modify the name, date ranges and rates of a variable to reflect changing conditions in your enterprise.

You can also delete variables you no longer need. Deleting a cost variable removes it permanently from the database, and you must update any formulas that use the variable. To restore a deleted variable, you must recreate the variable manually.

To modify a cost variable

1. On the console Costs tab, click **Step 1 - Create Cost Variables**.

   The content pane displays a list of cost variables defined on the Server. The variables are listed in alphabetical order.
2. Click **Edit** to the right of the variable name.
3. In the Edit Cost Variable dialog box, do any of the following:
   - Change the variable's name by typing over text in the Variable Name field.
   - Change the variable's metric by selecting a different value in Variable Metric drop-down list.
   - Change date ranges and rates by replacing values in the various fields, or by using the Add New Range and Delete Selected buttons to add and delete date ranges.
4. Click **Save Variable**.

Creating and managing cost formulas

Using the variables you created, you can create and update formulas that Veritas Backup Reporter will use to generate cost reports.

See "Creating cost variables" on page 84.

Creating cost formulas

After you create cost variables, the second step in setting up Veritas Backup Reporter to run cost reports is to create formulas that define the cost of various services.

To create a new cost formula

1. On the console Costs tab, click **Step 2 - Create Cost Formula**.
2. In the content pane, click **Create** at the top of the list.
3. In the Create Cost Formulae dialog box, type a name for the formula in the Formula Name field.
4. Add one or more cost variables to the formula.

   You only need to specify one variable to create the formula.

5 Optionally, to define formulas containing more than one variable, click **Add New Variable**.

You can also modify the formula later to add or delete variables and date ranges as the cost of the service changes.

6 Click **Save Formula**.

You have now finished creating a new cost formula. You can now use the formula to create cost reports with which you can evaluate the cost of services and make decisions about what to charge for performing those services.

See "Generating the cost report" on page 88.

Modifying and deleting cost formulas

You can modify the name and variables of a cost formula that you have created.

You can update chargeback formulas without having to recreate the reports that rely on them. For example, you might want to update a formula called `RecoveryRate` to reflect a change in the hourly rate charged for recovery operations.

You can also delete formulas you no longer need. Deleting a cost formula removes it permanently from the database. To restore a deleted formula, you must recreate the formula manually.

To modify a cost formula

1 On the console Costs tab, click **Step 2- Create Cost Formulas**.

2 The content pane displays a list of cost formulas defined on the Server. The formulas are listed in alphabetical order.

3 In the content pane, click **Edit** to the right of the formula name.

4 In the Edit Cost Formula dialog box, do one or more of the following:

- Change the formula's name by typing over text in the Formula Name field.
- Change variables and the factors associated with them by replacing values in the various fields, or by using the Add New Range and Delete Selected buttons to add and delete variables.

5 Click **Save Formula**.

To delete a cost formula

1. On the console Costs tab, click **Create Cost Formulas**.

   The content pane displays a list of cost formulas defined on the Server. The formulas are listed in alphabetical order.
2. In the content pane, check the checkbox next to the name of the formula you want to delete.
3. Click **Delete** at the top of the list.
4. In the confirmation message, click **OK**.

   The formula is deleted.

Generating the cost report

Using cost variables and formulas you have defined, you can generate reports about backup/recovery operations. The Report Wizard guides you through the process of generating reports.

To generate a new cost report

1. On the console Costs tab, click **Step 3 - Generate Cost Reports**.
2. In the My Cost Reports page, select a report type and format in the task pane (for example Costs - Rankings).

   See "Displaying object views" on page 29.
3. In the Report Wizard, select an object view category from the drop-down list in the Within View field.

   See "Displaying object views" on page 29.
4. Select the view level you want the report to display from the drop-down list in the Aggregate at field.

   For example, when reporting on the Client Count view, you could aggregate data at the Top level (in which case the report would display data for all servers as a single unit) or at the Client level, in which case the report would display data for each client individually.
5. To filter the report to include only the data for a particular set of objects (instead of the data for all objects in the view), do the following:

   - Select the view level of the filtered objects from the drop-down list in the Filter at field.
   - Select one or more objects whose data you want to include in the report in the Select specific items list box.

The objects in the list box may be “real” objects such as hosts and file systems, or user-created nodes in the view, depending on the view level at which you set the filter.

6 Set the report time frame by doing one of the following:

- Click **Relative Date** to configure a relative time frame. Then select a number of hours, days, weeks, months, or years using the drop-down lists in the Show Last field.
  The report will display the most recent data within the specified amount of time.
- Click **Absolute Date** to configure an absolute time frame. Then select a start date using the drop-down lists in the From field, and a end date using the drop-down lists in the To field.
  The report will display data from the time period between the start and end dates.
  If you plan to save reports for later viewing or for scheduled distribution by email, it is best to choose a relative time frame, so that the report always represents the most recent data relative to the time the report is accessed or emailed.

7 Select Display Options parameters, which govern the way the report display will look.

The parameters depend on the report format you selected in 2.

For example, for a rankings report, you specify the number of objects to rank, the ranking order (ascending or descending), and a label for the x-axis.

See “About Custom Report Wizard parameters” on page 63.

8 Select a cost formula from the Choose Cost Formula drop-down list.

9 Click **Run**.

The report displays, showing the cost for the specified service, as defined by the formula you selected, over the specified time frame.

10 To make changes to the report (for example, adjusting the time frame or the filtering level), click **Edit**.

You are returned to the Report Wizard.

You can save the cost report for later use.

See “Saving and preserving report data” on page 71.

Chapter 5

Monitoring backup job status and other network events

This chapter includes the following topics:

Monitoring and troubleshooting backup jobs

The VBR console provides several different ways for you to monitor the status of backup jobs and to view, search, and manage events on the network. There are also tools for creating policies that automate notification and other actions in response to specified conditions.

To monitor and troubleshoot backup jobs and track network changes

1 Click **Monitors** in the console header.

You can view, search, and manage logs of backup jobs, media usage, and change requests.

2 On the Monitors tab in the console, view, search, and manage alerts that correspond to events on the network.

You can create policies to automate response to events, and you can compile a Knowledge Base with information that is tailored specifically to your enterprise.

The features described in this section are useful for administrators who use Veritas Backup Reporter to evaluate the effectiveness of their data backup system and for troubleshooting problems.

Veritas Backup Reporter collects log data from your backup servers and compiles it into a history of backup jobs. Use the Backup explorer to view detailed information about any backup job in the database. This tool helps the administrator evaluate backup success rates and troubleshoot problems.

In the Monitors section of the console, you can expand items in the task pane tree view to view backup jobs sorted in a variety of ways, for example by jobs, by hosts, or by tape backups.

The descriptions of backup monitoring features use terms and examples specific to the Veritas NetBackup product. However, Veritas Backup Reporter also supports backup monitoring for additional products as shown in Table 5-1.

Table 5-1 Backup monitoring features supported by Veritas Backup Reporter

Items Monitored	Veritas NetBackup	Veritas Backup Exec	Tivoli Storage Manager	EMC Legato Networker
Total backup jobs	Supported	Supported	Supported	Supported
Policies	Supported	Supported	Supported	Supported
Skipped files	Supported	Not Supported	Supported	Supported
Error log data	Supported	Supported	Supported	Supported
Media usage	Supported	Not Supported	Not Supported	Supported

Table 5-1 Backup monitoring features supported by Veritas Backup Reporter *(continued)*

Items Monitored	Veritas NetBackup	Veritas Backup Exec	Tivoli Storage Manager	EMC Legato Networker
Tape drive usage	Supported	Supported	Not Supported	Supported
Tape library	Supported	Not Supported	Not Supported	Not Supported
Image Backup	Supported	Not Supported	Not Supported	Not Supported

The following topics describe the displays available for monitoring your backup job history in the Veritas Backup Reporterconsole:

- See "Monitoring backup jobs by object view category" on page 93.
- See "Monitoring backup jobs by host" on page 94.
- See "Monitoring backup jobs over a period of time" on page 95.
- See "Monitoring tape drive usage" on page 101.
- See "Monitoring backup tape media" on page 101.

Monitoring backup jobs by object view category

You can monitor backup jobs organized by object view category, for example Geography or Application. (Categories are installation-specific.)

To view backup jobs for hosts in an object view category

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, expand **Backup Job Monitor**, and then click **By View**.

3. On the drop-down list, select an object view category, such as Geography or Application.

   Categories are installation-specific.

4 Click **Next**.

The Backup Monitor Job table displays, showing a detailed list of the backup jobs for the selected category.

5 Do one of the following:

- Select a backup job ID to view additional details for that job, including skipped files and job log entries.
- Select a backup job's status (indicated in the Status column by an icon and a numeric code) to view information about the status. For example, a status code of 0 means the job completed without errors.

Monitoring backup jobs by host

You can monitor the backup jobs for hosts on a specific master server or media server, or within a specific object view category.

To view backup jobs for hosts on a master server or media server

1 Click **Monitors** in the console header.

The console displays a menu of tools for monitoring and tracking backup jobs.

2 In the task pane tree view, expand **Backup Explorer**.

3 Select one of the following:

- By Master Server
- By Media Server

A table of master servers or media servers displays, showing the number of backup jobs, last backup, and oldest backup for each one.

4 Select the server whose backup jobs you want to view.

The Backup Summary table displays, showing backup jobs for each host in the indicated server. Each host's backup jobs display in a single row sorted by date, the most recent jobs appearing in the leftmost columns. Mouse over an individual job to see a ToolTip that includes details like the job ID, the exact time the job completed, and the job's status.

5 Click a host name to view the Host Backup Jobs table, which contains a more detailed list of that host's backup jobs.

6 Do one of the following:

- Select a backup job ID to view additional details for that job, including skipped files and job log entries.

- Select a backup job's status (indicated in the Status column by an icon and a numeric code) to view information about the status. For example, a status code of 0 means the job completed without errors.
  This status information comes from the Knowledge Base.
  See "Using the Knowledge Base" on page 118.

To view backup jobs for hosts within an object view category

1. Click **Backup** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, expand **Backup Job Monitor**, and then click **By View**.

3. From the drop-down list, select an object view category, such as Geography or Application.

   Categories are installation-specific.

4. Click **Next**.

   A table displays, showing backup jobs within the selected category. You can filter the table contents using the Status, Job Type, and Range drop-down lists at the top of the table.

5. Do one of the following:

   - Click a backup job ID to view additional details for that job, including skipped files and job log entries.
   - Click a backup job's status (indicated in the Status column by an icon and a numeric code) to view information about the status. For example, a status code of 0 means the job completed without errors.
     This status information comes from the Knowledge Base.
     See "Using the Knowledge Base" on page 118.

Monitoring backup jobs over a period of time

The Monitors section of the console provides several different ways to display data over specific intervals of time: by week, by rolling eight-day period, or by a customized interval (cycle).

Note: Using the Custom Report Wizard, you can also generate weekly and rolling eight-day reports for backup jobs in the Service section of the console. Those reports can be archived and used for notification.

Monitoring by week

You can monitor the backup jobs for hosts on a master server or media server, or within an object view category, for a specific week.

In the Backup Monitoring display, you can drill down to display more detailed status and history information. For example, selecting the name of a client displays a list of the file systems backed up for that client. From the file system list, you can display details about backup jobs and—by drilling down one more level—details about individual attempts.

To view backup jobs for a specific week

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, expand **Week at a Glance**.
3. Click one of the following:
   - By Master Server
   - By Media Server
   - ByView
4. In the Report Wizard dialog window, click an object or view type by which to filter data:
   - If you selected By Master Server in 3, select a master server.
   - If you selected By Media Server in 3, select a media server.
   - If you selected By View in 3, select a view type (for example Geography).
5. On the Week Setting drop-down list, select one of the following weekly cycles for which you want to display data:
   - This Week
   - Last Week

- A specific week such as 3 Weeks Ago

6 Click **Next**.

The VBR console displays a Backup Monitors table summarizing the status of backup jobs for hosts (servers) and for host file systems. Data is arranged according to your selections and covers the week you indicated.

Monitoring by the most recent eight days

You can monitor the backup jobs for hosts on a master server or media server, or within an object view category, for the most recent eight-day period. For example, if today is Monday, the display shows data about backup jobs ranging from last Monday through today.

To view backup jobs for the most recent eight days

1 Click **Monitors** in the console header.

The console displays a menu of tools for monitoring and tracking backup jobs.

2 In the task pane tree view, expand **Rolling 8 Day**.

3 Click one of the following:

- By Master Server
- By Media Server
- By View

4 In the Report Wizard dialog window, click an object or view by which to filter data:

- If you selected By Master Server in 3, select a master server.
- If you selected By Media Server in 3, select a media server.
- If you selected By View in 3, select a view type (for example Geography).

5 If you want the display to include an extended list of attributes for each backup host, click **Display Extended Host Attributes**.

You can drill down to display more detailed status and history information. For example, clicking the name of a client displays a list of the file systems backed up for that client. From the file system list, you can display details about backup jobs and, by drilling down one more level, details about individual attempts.

6 Click **Next**.

The VBR console displays a Backup Monitors table summarizing the status of backup jobs, arranged according to your selections and covering the rolling eight-day period.

In the Backup Monitoring display, use the Ending controls to define the end of the time frame you want to monitor. (Time is specified in 24-hour format; for example, 22:00 means 10:00 P.M.) Use the Status and Job Type controls to further filter the contents of the list.

Monitoring by customized time intervals (cycles)

You can use cycles to define separate time boundaries for displaying the status of backup jobs. You can, for example, set the boundaries of a day to begin and end at some time other than midnight. By defining cycles that match the schedule on which your enterprise operates, you can generate precise and meaningful displays of backup job status.

For example, your normal weekly cycle for backup jobs might be as follows:

- Monday 5:30 P.M. to Tuesday 8:30 A.M.
- Tuesday 5:30 P.M. to Wednesday 8:30 A.M.
- Wednesday 5:30 P.M. to Thursday 8:30 A.M.
- Thursday 5:30 P.M. to Friday 8:30 A.M.
- Friday 6:00 P.M. to Monday 8:30 A.M.

Each of these time intervals constitutes a cycle period. Taken together to form a complete calendar week, they represent the cycle for one week. You can define multiple cycles, to reflect, for example, weeks that contain holidays.

Rather than displaying backup job status based on calendar days and weeks, the VBR console can display status based on cycle periods and cycles that you have defined. The Cycle Dashboard is a tool for displaying backup job status based on user-defined settings for cycle, master server name, and week of the year.

To define a cycle for displaying backup job status

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, expand **Cycle Settings**, and then click **Add a New Cycle**.

3. In the Add Cycle dialog window, type the name of the cycle in the Cycle Name field, and then click **Add**.

   The cycle is added to the Cycles list.

4. To define a cycle period, click **Create cycle period** next to the cycle name in the Cycles list.

   Using the drop-down lists in the Modify Cycle Period dialog window, specify a cycle period's start time and end time.

   Example: Start: Tuesday 5:30 PM End: Wednesday 8:30 AM

5. Click **Modify**

6. To define more cycle periods, repeat 4-5.

   The Cycles list displays the cycle along with the cycle periods you have defined for it.

To display backup job status using the Cycle Dashboard

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, expand **Cycle Dashboard**, and then select one of the following displays:

   - By Cycle
   - By Master Server
   - By Media Server
   - By View
   - Job Types

3. In the Custom Report Wizard dialog box, do the following:

   - If applicable, click an object or view type by which to filter data displayed in the Cycle Dashboard:
   - If you selected By Cycle in 2, skip to step 4.

- If you selected By Master Server in 2, select a master server.
- If you selected By Media Server in 2, select a media server.
- If you selected By View in 2, select a view type, for example `Geography`.
- If you chose Job Types in 2, select a master server.

4 On the Week Setting drop-down list, select the weekly cycle for which you want to display data. You can choose from among `This Week`, `Last Week`, or a specific week such as `3 Weeks Ago`.

5 On the Select Cycle drop-down list, select a cycle.

Example: Master Server: nbuhost1.example.com Week Setting: Last Week Click Cycle: NormalWeek

6 Click **Next**.

The VBR console displays a Backup Monitors table summarizing the status of backup jobs, arranged according to your selections.

In the Backup Monitoring display, you can drill down in the list to display more detailed status information. You can also use the Week control to display status information for a different week, and you can use the Status and Job Type controls to further filter the contents of the list.

Monitoring active versus queued jobs

You can monitor the backup jobs for hosts on a master server according to their status: ACTIVE or QUEUED.

To view backup jobs by active or queued status

1 Click **Monitors** in the console header.

The console displays a menu of tools for monitoring and tracking backup jobs.

2 In the task pane tree view, expand **Running vs. Queued**.

3 Click **By Master Server**.

The VBR console displays a Backup Monitors table summarizing the status of active and queued backup jobs, arranged by master server.

4 At the top of the table, do any of the following:

- On the Start drop-down lists, define the beginning of the time frame you want to monitor. (Time is specified in 24-hour format; for example, 22:00 means 10:00 P.M.)
  Example: May 20 2005 22:00

- On the Format drop-down list, select a time frame and intervals.
  Examples: 4 Hours at 15 minute intervals
- To include statistics on tape drive usages associated with backup jobs, check **Include Tape Drive Use**, and then click **Go**.
  Using this option will probably increase the time it takes to populate the table with data.
  The table refreshes to display data based on your selections. Select the name of a master server to display more detailed information about backup jobs for that server.

Monitoring tape drive usage

Veritas Backup Reporter collects log data from your backup media servers and compiles it into a history of tape drive utilization. Use the Tape Drive Usage tool to view detailed information about a drive's history of writes and percent utilization. This tool helps the administrator evaluate whether tape drives are being used efficiently and whether there is a need to add more drives.

To view tape drive utilization history

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, click **Tape Drive Usage**.

   The Tape Drive Usage table displays a list of master servers and media servers, showing the most recent sample, number of samples, and utilization percentage for each server.

3. In the Tape Drive Usage table, click the server whose tape drive usage history you want to view.

   A table displays the utilization history of the server's individual tape drives. Each column in the table represents a snapshot of the drive utilization, with 15 minute intervals between each sample. Mouse over a table field to see the exact time the snapshot was taken, and which media server was writing to the drive at that time.

Monitoring backup tape media

Veritas Backup Reporter collects log data from Veritas NetBackup and Backup Exec and compiles status information for the backup media into its database. You can view recent writes, availability, and status for your backup media.

To view backup media

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. In the task pane tree view, click **Media Explorer**.

   A table of master servers and media servers displays, showing the number of media (usually tapes) and the images they contain, along with the date and time they were last updated, and the total amount of data on media (in GB) for each server.

3. Click the server host whose backup media you want to view.

   A table displays data about all of the server's backup media, organized by status. Each row displays the number of media devices, the total number of images they contain, and the total amount of data (in GB).

4. In the Master Media Explorer table, select a status, such as Active or Full.

   A table displays summary information for each backup medium reporting the selected status. For each medium, the table displays its volume pool, number of images, when it was last updated, the oldest expiration date, its density, and the total amount of data (in GB).

5. Click an individual media ID to view detailed information for that medium.

Monitoring job attempt data

Job attempt data is included with job data. Backup modules may not return any attempt information, either because the backup product does not keep track of attempts, or as a design decision when job information is collected. You can retrieve job attempt data for any report where you include a "Backup Attempt" field, or if you enable a "Backup Attempt" filter.

Note: If there is no attempt data, and you attempt to report on the attempt data, you will receive a "No Data Found" for a Chart report and an empty table for a Tabular report.

Table 5-2 Backup reports that can be run for finding attempt data

How to access reports	Description
Reports > Backups > Historical Activity	All reports when an Attempt field is selected from the Report On dropdown list.

Table 5-2 Backup reports that can be run for finding attempt data *(continued)*

How to access reports	Description
Reports > Backups > Asset	All reports when an Attempt field is selected from the Report On dropdown list.
Reports > Backups > Future Forecast	All reports when an Attempt field is selected from the Report On dropdown list.
Reports > Backups > Service Level > Success Rate	**Note:** Attempt columns are set implicitly for these reports.
Reports > Backups > Service Level > Sucessful Job Count	
Reports > Backups > Service Level > Partially Sucessful Job Count	
Reports > Backups > Service Level > Failed Job Count	
Reports > Backups > Window Reports	All reports when an Attempt field is selected from the Report On dropdown list.
Reports > Recovery	All reports when an Attempt field is selected from the Report On dropdown list, except for reports under Service Level > Job Status.

Monitoring and tracking network changes

The Change Manager is a simple system for tracking user requests of all types. The Change Manager is an open-ended system that enables any user to modify, approve, deny, or reply to a change request.

The Change Manager contains a record of all change requests that have been logged in the database. In the VBR console, it displays as a table of change requests, sorted by date. You can view detailed information about a request and perform operations on the request.

Viewing the Change Manager

You can view all logged change requests from the Operations page of the VBR console.

To view the Change Manager

1. Click **Monitors** in the console header.

   The console displays a menu of tools for monitoring and tracking backup jobs.

2. On the Operations tab, click **Change Manager** in the task pane.

   The content pane displays the Change Manager, which is a log of change requests from users.

   From a change request's detail page, or from any dialog window within the Change Manager section of the console, you can display the Change Manager log by selecting the View All icon.

3. Click a change request to view detailed information for that request.

Creating change requests

Any user can create a change request and add it to the log.

To create a new change request

1. Display the Change Manager.
2. Click **Add A New Entry** from the task pane tree view.

   You can also create a new request using the Add icon on the detail page for any other request.

3. In the Add Change Request dialog box, in the Title field, type a short title for the request.
4. On the Severity drop-down list, select one of the following:
   - Low
   - Medium
   - High
   - Critical

- Emergency

5 In the Description field, type a detailed description.

6 Click **Add.**

Modifying change requests

Any user can modify a change request in the log.

To modify a change request

1 From the Change Manager, select a change request to display its detail page.

2 Click the **Modify** icon.

3 In the Modify Change Request dialog box, edit the dialog field values.

4 Click **Modify** to save your changes to the change request.

Authorizing change requests

Use the Change Manager to authorize, or OK, change requests. Typically, this indicates some level of approval. The precise meaning will depend on the internal procedures in place for your organization.

You can use the OK feature independently from, or in conjunction with, the Approve feature.

See "Approving change requests " on page 106.

For example, an operator might OK a request to indicate preliminary approval, and a system administrator might then approve the request to provide formal authorization.

Any user can OK a change request in the log. However, you should consider establishing internal procedures that define which individuals can OK requests and under what circumstances.

To OK a change request

1 From the Change Manager, select a change request to display its detail page.

2 Click the **OK** icon.

Approving change requests

Any user can approve a change request in the log. However, you should consider establishing internal procedures that define which individuals can approve requests and under what circumstances.

You can use this feature independently of, or in conjunction with, the OK feature.

See "Authorizing change requests " on page 105.

To approve a change request

1. From the Change Manager, click a change request to display its detail page.
2. Click the **Approve** icon.

Denying change requests

Any user can deny a change request in the log.

Note: Consider establishing internal procedures that define which individuals have the authority to deny requests.

To deny a change request

1. From the Change Manager, click a change request to display its detail page.
2. Click the **Deny** icon.

Holding change requests

Any user can place a change request on hold. The HOLD status indicates that a final decision on whether to approve or deny the request is being deferred.

Note: Consider establishing internal procedures that define which individuals have the authority to hold requests.

To hold a change request

1. From the Change Manager, click a change request to display its detail page.
2. Click the **Hold** icon.

The request is placed on hold. In the Change Manager, its status displays as ON HOLD.

Replying to change requests

Any user can reply to a change request in the log. A reply is a comment, for example, a note from an administrator to an operator explaining why a request was approved or denied. Each reply displays in the request's detail view.

To reply to a change request

1. From the Change Manager, click a change request to display its detail page.
2. Click the **Reply** icon.

3. In the Add a Reply dialog box, type your reply in the text field.
4. Click **Add** to add the reply to the change request.

Deleting change requests

Deleting a change request removes it permanently from the database. To restore a deleted change request, you must recreate the request manually.

To delete a change request

1. From the Change Manager, click a change request to display its detail page.
2. Click the **Delete** icon.

3. In the Confirm Deletion dialog box, click **OK** to delete the change request.

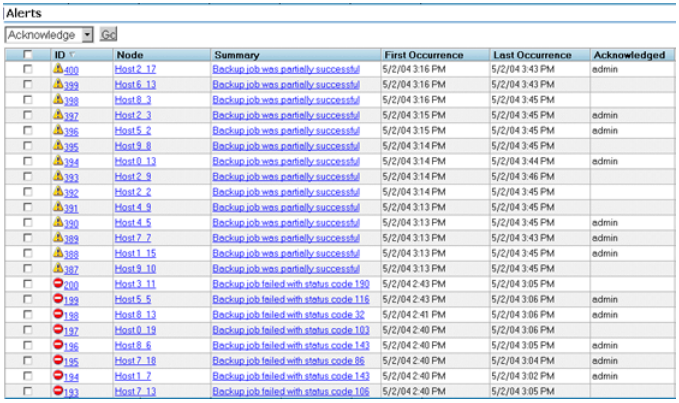
About monitoring and managing alerts

The Alerts Details lists active alerts for all VBR Management Server hosts to which you are connected. You can think of the Alerts Details as an event log showing the status of backup jobs.

The Alerts Details also provides a simple way to track user responses to alerts, including acknowledging an alert, adding comments to it, closing it, or deleting it from the log.

Note: When the Server receives multiple alerts having the same alert key or error code from the same source, they display in the console as a single alert.

Figure 5-1 The Alerts Details



	ID	Node	Summary	First Occurrence	Last Occurrence	Acknowledged
	400	Host 2_17	Backup job was partially successful	5/2/04 3:16 PM	5/2/04 3:43 PM	admin
	399	Host 6_13	Backup job was partially successful	5/2/04 3:16 PM	5/2/04 3:43 PM	
	398	Host 8_3	Backup job was partially successful	5/2/04 3:16 PM	5/2/04 3:45 PM	
	397	Host 2_3	Backup job was partially successful	5/2/04 3:15 PM	5/2/04 3:45 PM	admin
	396	Host 5_2	Backup job was partially successful	5/2/04 3:15 PM	5/2/04 3:45 PM	admin
	395	Host 9_8	Backup job was partially successful	5/2/04 3:14 PM	5/2/04 3:45 PM	
	394	Host 0_13	Backup job was partially successful	5/2/04 3:14 PM	5/2/04 3:44 PM	admin
	393	Host 2_9	Backup job was partially successful	5/2/04 3:14 PM	5/2/04 3:46 PM	
	392	Host 2_2	Backup job was partially successful	5/2/04 3:14 PM	5/2/04 3:45 PM	
	391	Host 4_9	Backup job was partially successful	5/2/04 3:13 PM	5/2/04 3:45 PM	
	390	Host 4_5	Backup job was partially successful	5/2/04 3:13 PM	5/2/04 3:45 PM	admin
	389	Host 7_7	Backup job was partially successful	5/2/04 3:13 PM	5/2/04 3:43 PM	admin
	388	Host 1_15	Backup job was partially successful	5/2/04 3:13 PM	5/2/04 3:45 PM	admin
	387	Host 9_10	Backup job was partially successful	5/2/04 3:13 PM	5/2/04 3:45 PM	
	200	Host 3_11	Backup job failed with status code 190	5/2/04 2:43 PM	5/2/04 3:05 PM	
	199	Host 5_5	Backup job failed with status code 116	5/2/04 2:43 PM	5/2/04 3:06 PM	admin
	198	Host 8_13	Backup job failed with status code 32	5/2/04 2:41 PM	5/2/04 3:06 PM	admin
	197	Host 0_19	Backup job failed with status code 103	5/2/04 2:40 PM	5/2/04 3:06 PM	
	196	Host 8_6	Backup job failed with status code 143	5/2/04 2:40 PM	5/2/04 3:05 PM	admin
	195	Host 7_18	Backup job failed with status code 86	5/2/04 2:40 PM	5/2/04 3:04 PM	admin
	194	Host 1_7	Backup job failed with status code 143	5/2/04 2:40 PM	5/2/04 3:02 PM	admin
	193	Host 7_13	Backup job failed with status code 106	5/2/04 2:40 PM	5/2/04 3:05 PM	

Viewing alerts in the Alerts Details

You can view all logged alerts in the console Alerts Details.

To view the Alerts Details

1. Click **Monitors > Alerts**.
2. To reach the Alerts Details from anywhere in the Monitoring area of the console, click **Alert List** from the Tools box in the task pane.
3. In the Alerts Details, select one of the following:
   - The ID number or summary text for an individual alert: Display detailed information about the alert.
   - A host name: Display the host's object view.

Filtering the Alerts Details display

You can easily sort and filter the Alerts Details to focus on the specific data you want to see. For example, you can apply a filter that either displays or hides acknowledged alerts.

To filter data in the Alerts Details

1 Click **Monitors > Alerts**.

The Alerts Details displays a list of all alerts for the VBR Management Server host to which you are connected.

2 On the drop-down list, click **Filter**, and then click **Go**.

3 In the Filter Alerts dialog box, specify one or more of the following filtering criteria:

Filter by number of alerts	Check the checkbox, type a positive integer, and select a sort order. The Alerts Details display will be limited to the specified number of alerts. Unchecking the checkbox means there is no limit on the number of alerts displayed.
Filter by severity	Check the checkbox and then select one or more severity levels. The Alerts Details will display only the alerts with the specified severity level.
Filter by age	Check the checkbox and specify a time interval (hours or days). For example, if you specify 2 day(s), the Alerts Details will display only the alerts that were created or modified within the last two days.
Filter by acknowledgment state	Check to hide acknowledged alerts. The Alerts Details will display only the alerts that have not been acknowledged.
Filter by status	Check to hide alerts with a status of `UNKNOWN`. The Alerts Details will display only the alerts with a status other than `UNKNOWN`.
Filter by server	Check to show only alerts from the active Service Server (the Server to which you are logged on).
Filter by column value	Use the controls to display alerts based on one or more attribute values. Check NOT to hide alerts with a specific attribute value. Use the drop-down lists to display alerts based on partial or blank character strings in attribute values, for example all alerts whose summary text begins with `Traffic`

4 Click **OK**.

The list of alerts displayed in the Alerts Details is filtered according to the criteria you specified. The filtering criteria remain in effect until you reset them using the same procedure.

5 To remove filtering, open the Filter Alerts dialog window and uncheck all of the checkboxes.

When you use filtering to display data in the Alerts Details, the filtered alerts remain in the database until they are aged out. As long as they remain in the database, you can change your filtering options to display them again if desired.

About managing alerts

The following topics describe using the Alerts Details to update alerts, close alerts, and check the Knowledge Base for related information:

- See "Acknowledging alerts" on page 110.
- See "Replying to alert " on page 111.
- See "Changing alert severity " on page 111.
- See "Closing alerts " on page 112.
- See "Referencing alert keys in the Knowledge Base" on page 112.
- See "Viewing the backup job history for hosts originating alerts " on page 113.

An administrator can use the Monitors > Alerts area of the VBR console to set attributes, such as sampling intervals and retention periods, for the collectors on which policies and alerts are based.

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

Acknowledging alerts

Alerts sent to the VBR console remain in the database for a preconfigured period of time. If an alert is not self-clearing, it will continue to display in the Alerts Details as long as it remains in the database. However, you can hide an alert by flagging it as "Acknowledged" and filtering the Alerts Details to hide acknowledged alerts. This removes the alert from the Alerts Details but does not remove it from the database.

Acknowledging an alert changes the alert's status to ACKNOWLEDGED and appends a comment to the event history.

To acknowledge alerts

1. Click **Monitors > Alerts**.
2. In the Alerts Details, check one or more alerts.
3. On the drop-down list, click **Acknowledge**, and then click **Go**.

   The status for the alerts changes to ACKNOWLEDGED, and the action is added to the event history.

Replying to alert

A reply is a comment, for example, a note from an operator describing the diagnostic steps the user took in response to an alert. Replying to an alert updates the event history and appends the user comment to the alert's detail page.

To reply to one or more alerts

1. Click **Monitors > Alerts**.
2. In the Alerts Details, check one or more alerts.
3. On the drop-down list, click **Add Comment**, and then click **Go**.
4. In the Add Comment to Alert dialog box, type the comment text, and then click **OK**.

   The comment is added to each selected alert and is recorded in the event history.

Changing alert severity

You can change the severity of an alert in the database. For example, an alert that originally reflected a CRITICAL problem could be downgraded to a severity of ERROR.

This action appends a comment to the event history.

Note: You should establish internal procedures defining the criteria for each severity level and specifying which individuals have the authority to change alert severity.

To change an alert's severity

1. Click **Monitors > Alerts**.
2. In the Alerts Details, click the ID number or summary text for an alert to open its detail view.
3. On the drop-down list, click **Change Severity**, and then click **checkmark**.

4 In the Change Severity of Alert dialog box, select one of the following severity levels:

- CRITICAL
- ERROR
- WARNING
- INFORMATION

5 Type a comment in the Comment field.

6 Click **OK**.

The alert's severity is updated, and the action (along with any comment you entered) is added to the event history.

Closing alerts

When an alert condition is resolved, you can close the alert. Closing an alert changes the alert's status to CLOSED and appends a comment to the event history, but it does not remove the alert from the database.

To close an alert

1 Click **Monitors > Alerts**.

2 In the Alerts Details, check the alert that you want to close.

3 On the drop-down list, click **Reset**, and then click **Go**.

The alert's status becomes CLOSED, and the action is added to the event history.

Referencing alert keys in the Knowledge Base

Veritas Backup Reporter has a Knowledge Base: a database of reference information in which users store and retrieve installation-specific information about system events, individual resources, processes, and procedures.

See "Using the Knowledge Base" on page 118.

From the Alerts Details, you can check the Knowledge Base for information about the alert key, or error code, associated with any alert.

To look up information for an alert key in the Knowledge Base

1. Click **Monitors > Alerts**.
2. In the Alerts Details, click the value in the Alert Key column for an alert.

   The Knowledge Base entry for that alert key displays.

   See "Using the Knowledge Base" on page 118.

Viewing the backup job history for hosts originating alerts

When an alert shows a backup job failure for a particular host, you may want to view all the recent backup jobs for that host to determine whether there is a recurring problem.

To view a history of backup jobs for an alert's originating host

1. Click **Monitors > Alerts**.
2. In the Alerts Details, select the host name, or node, for an alert.
3. In the host's object view, on the drop-down list, click **Backup Jobs**, and then click **Go**.

   A table displays the backup job history for the host where the alert originated.

About monitoring the network using policies

Veritas Backup Reporter policy management comprises two major functions: alerts and notifications.

Veritas Backup Reporter provides tools for creating and managing policy notifications (actions that disseminate and log important information about objects and jobs, such as backup operations, managed by Veritas Backup Reporter). For a variety of alert types, you can generate an email, write a system log entry, execute a command, and even generate an SNMP trap.

You can view and manage policies using Veritas Backup Reporter.

Viewing and managing policies

You can use the Veritas Backup Reporter Policies Summary to get a quick view of a policy's status and the conditions and actions defined in it. You can also display detailed information about customizing, enabling, or disabling policies.

To view and manage policies

1. Click **Monitors > Alerts > Policies**.
2. In the Policies Summary, do one of the following:

Create a new policy.	Click **Create Global Policy** from the drop-down list, and then click **checkmark** . The Edit Policy dialog window launches, with instructions for defining the characteristics of the new policy.
Modify an existing policy.	Select the name of the policy. The policy's detail view displays. From there, you can customize the policy, copy it for use in another policy, enable or disable it, and export it for distribution among multiple systems.

Configuring policy notification

When you define or update a policy, one of your most important tasks is deciding what will be notified when the policy generates an alert. Your policy can send notification to any of three types of recipients:

Email recipient	A person who receives notifications by email. See "Defining email recipients" on page 115.
Trap recipient	A host computer that receives traps, or interrupts. See "Defining trap recipients" on page 116.
Group	A combination of persons, hosts, or other groups. See "Defining recipient groups" on page 117.

The Recipients Summary displays lists of all recipients defined on the Veritas Backup Reporter Management Server and provides a launching point from which you can add, delete, and modify recipients.

To view the Recipients Summary

- Click **Monitors > Alerts > Recipients**.

Defining email recipients

An email recipient is a person who receives notifications by email when a policy condition is met. For example, you could set up a policy so that a network operator receives an email message whenever a server goes offline.

Note: Before you define email recipients, make sure that your SMTP email server has been configured.

For details, see the *Veritas Backup Reporter Administrator's Guide*.

To add an email recipient

1. Click **Monitoring > Alerts > Recipients**.
2. In the Recipients Summary, on the drop-down list for the Email Recipients table, click **Create Recipient**, and then click **checkmark**.
3. In the Email Recipient dialog box, in the Name field, type the person's name.
4. In the Address field, type the person's email address.
5. For confirmation purposes, click **Test Recipient** to send email to the newly defined recipient.
6. Check **Active** to enable notification for this recipient.
7. If you want the circuit breaker to limit the number of notifications sent within a specified time interval, check **Enable Delivery Limit** and fill in the following fields:

Delivery Limit	Type the maximum number of notifications and the time interval (minutes, hours, or days). When the number of notifications reaches this threshold within the specified time period, the circuit breaker stops additional notifications from being sent. Example: 20 messages within 10 minute(s)
Reset the message count after	Type a time interval (minutes, hours, or days). When the circuit breaker is invoked, it will reset after this much time has elapsed, allowing notifications to be sent again. Example: 1 hour(s)

8. Click **OK**.

   The person is now available as a recipient for SMTP mail. This person can be added to any of your defined person groups.

Defining trap recipients

Traps, also known as interrupts, are signals sent to inform programs that an event has occurred. In Veritas Backup Reporter, traps are notification signals sent to a specified SNMP host or group of hosts when the policy condition is met.

A trap recipient is a host that receives notifications in the form of traps when a policy condition is met. For example, you could set up a policy so that a trap is sent, and an alert generated, whenever a server goes offline.

To add a trap recipient

1. Click **Monitoring > Alerts > Recipients**.
2. In the Recipients Summary, on the drop-down list for the Trap Recipients table, click **Create Recipient**, and then click **checkmark**.
3. In the Trap Recipient dialog box, in the Name field, type a descriptive name for the host you are defining.
4. In the Host field, type the network name for the host (for example testhost.example.com).
5. If the target host receives traps on a port other than the default port of 162, type the port number in the Port field.
6. To send a test trap to the specified host, click **Test Recipient**.
7. Check **Active** to enable notification for this trap recipient.
8. If you want the circuit breaker to limit the number of notifications sent within a specified time interval, check **Enable Delivery Limit**, and then fill in the following fields:

Delivery Limit	Type the maximum number of notifications and the time interval (minutes, hours, or days). When the number of notifications reaches this threshold within the specified time period, the circuit breaker stops additional notifications from being sent. Example: 20 messages within 10 minute(s)
Reset the message count after	Type a time interval (minutes, hours, or days). When the circuit breaker is invoked, it will reset after this much time has elapsed, allowing notifications to be sent again. Example: 1 hour(s)

9. Click **OK**.

   The host is now available as a recipient for traps. This host can be added to any of your defined host groups.

Defining recipient groups

When you define groups of recipients, Veritas Backup Reporter is able to send policy notifications to multiple people or multiple hosts. Groups can consist of email recipients, trap recipients, or other groups.

To set up a recipient group, you specify a list of group members. A group contains one or more members, and each member of the group receives notifications for the associated policies.

To create a recipient group

1. Click **Monitoring > Alerts > Recipients**.
2. In the Recipients Summary, in the Email Recipients table or the Trap Recipients table, check the names of every recipient that will be a member of the group.

   To specify all of the recipients and groups in the table, check the checkbox in the upper left corner of the table.
3. On the drop-down list, click **Create Recipient Group**, and then click **checkmark**.
4. In the Recipient Group dialog box, in the Name field, type a descriptive name for the group you are defining.
5. Check **Active** to enable notification for this recipient group.
6. Verify the list of group members in the Recipients table.

   To make changes, check or uncheck the checkboxes.
7. Click **OK**.

   The group is now available for notification. It can be added to any other groups of the same type (email or trap).

Modifying recipients and recipient groups

You can modify the definition for a recipient or group. For example, you might want to update a person's email address, change a recipient's active status, or update the membership of a group.

To modify a recipient or group

1. Click **Monitoring > Alerts > Recipients**.
2. In the Recipients Summary, select the name of the recipient or group you want to modify.
3. Change any fields in the Email Recipients, Trap Recipients, or Recipient Group dialog box, and then click **OK**.

Deleting recipients and recipient groups

You can delete a recipient or group.

To delete a recipient or group

1. Click **Monitoring > Alerts > Recipients**.
2. In the Recipients Summary, in the Email Recipients table or the Trap Recipients table, check the names of every recipient or group you want to delete.

   To select all of the recipients and groups in the table, check the checkbox in the upper left corner of the table.
3. On the drop-down list, click **Delete Recipient**, and then click **checkmark**.
4. Click **OK** to confirm deletion.

   Deleted recipients are no longer available for notification. If they were members of groups, they are automatically removed from the groups.

   Deleted groups are no longer available for notification. The group members, however, are still defined.

Using the Knowledge Base

The Veritas Backup Reporter Knowledge Base is a database of reference information for error codes and commands. It is a good way for users to store and retrieve installation-specific information about system events, individual resources, processes, and procedures.

When viewing other parts of the database, such as the backup job history, an administrator can click an error code for a failed job to view the Knowledge Base entry for that error code.

In addition to viewing the Knowledge Base entries that ship with Veritas Backup Reporter, you can create and modify your own entries.

Browsing Knowledge Base entries

You can browse all the entries in the Knowledge Base from the Operations page of the VBR console.

To browse entries in the Knowledge Base

1. Click **Monitors > Knowledge Base**.
2. In the table of Knowledge Base categories, click the category whose entries you want to view.
3. In the table of Knowledge Base entries, click the entry you want to view.

   The detail page for the Knowledge Base entry displays.

Creating Knowledge Base entries

You can add your own entries to the Knowledge Base. This may be helpful for making notes about the administration or operation of Veritas Backup Reporter available for others or for your own future reference.

To create a new entry in the Knowledge Base

1. Click **Monitors > Knowledge Base**.
2. In the table of Knowledge Base categories, in the Tools box in the task pane, click **Add Knowledge Base Entry**.

3 In the Add Knowledge Base Entry dialog box, complete the dialog fields:

Title	The title of the entry. It should be descriptive, yet short enough to display in a table.
Category	The Knowledge Base category. If the category you specify does not exist, Veritas Backup Reporter will create a new category with that name. To add a new entry to an existing category, you must type the category name exactly as it appears in the Knowledge Base table.
Error Code (optional)	A code associated with the event or condition you are describing. Use this field if your organization has a list of error codes for identifying various types of events or conditions.
Email (optional)	An email address to be notified whenever this entry is updated.
Group (optional)	A group to be notified whenever this entry is updated.
Description	The text of the entry. It can describe a problem and its recommended solution, list configuration details about a resource in the network, or provide any other information of value to users at your installation.

Knowledge Base descriptions can contain standard HTML coding.

4 Click **Add** to add the new entry to the Knowledge Base.

Copying Knowledge Base entries

Starting with an existing Knowledge Base entry, you can modify the entry and then save the modified version as a new entry. The original entry is not affected by this operation.

To copy an entry in the Knowledge Base

1 Click **Monitors > Knowledge Base**.

2 In the table of Knowledge Base categories, click the category for the entry you want to copy.

3 In the table of Knowledge Base entries, on the line for the entry you want to copy, click the icon in the Edit column.

4 In the Add Knowledge Base Entry dialog box, type a new title in the Title field.

5 Edit some or all of the other dialog field values.

See "Creating Knowledge Base entries " on page 119.

6 Click **Clone**.

A new Knowledge Base entry is created, and the original entry remains unchanged.

Modifying Knowledge Base entries

To ensure that your Knowledge Base entries contain current information, you can edit them.

To modify an entry in the Knowledge Base

1 Click **Monitors > Knowledge Base**.

2 In the table of Knowledge Base categories, select the category for the entry you want to modify.

3 In the table of Knowledge Base entries, on the line for the entry you want to modify, click the icon in the Edit column.

4 In the Add Knowledge Base Entry dialog box, edit the dialog field values.

See "Creating Knowledge Base entries " on page 119.

5 Click **Modify** to save your changes to the Knowledge Base entry.

The entry is updated in the Knowledge Base.

Deleting Knowledge Base entries

You can delete entries in the Knowledge Base when they are no longer useful.

To delete an entry in the Knowledge Base

1 Click **Monitors > Knowledge Base**.

2 In the table of Knowledge Base categories, select the category for the entry you want to modify.

3 In the table of Knowledge Base entries, on the line for the entry you want to delete, click the icon in the Delete column.

4 Click **OK** to confirm deletion.

The entry is deleted from the Knowledge Base.

Chapter 6

Managing notification and archiving

This chapter includes the following topics:

Using reports for notification

You can plan for and generate automatic, report-based notifications tailored to the needs of the people in your enterprise. You can also archive data in reports.

Veritas Backup Reporter reports provide several ways to either notify staff members when problems occur or generate routine status updates:

- See "Using report data to notify staff when problems occur" on page 123.
- See "Using report data to trigger alerts" on page 124.
- See "Sending routine status updates" on page 125.

Using report data to notify staff when problems occur

By setting threshold conditions in a report's definition, you can cause Veritas Backup Reporter to notify staff members by email whenever those conditions are not being met.

For example, you can set up a report so that backup admins receive an email message when the backup success rate falls below a certain level.

To notify people by email when a report condition is met

1. In the VBR console, open a predefined (default) report or launch the Custom Report Wizard.

   See "Using and customizing default reports" on page 53.

   See "Creating and using custom reports" on page 61.

2. Using the controls in the Exception Conditions section of the wizard, define thresholds to represent potential problem conditions.

   These are the conditions under which Veritas Backup Reporter will send notifications.

   See "Defining report conditions" on page 69.

3. Click **Run** to run the report.

   The report output displays in the console.

4. Save the report.

   See "Saving data in a report" on page 71.

5. Create or edit an email report.

   See "Managing the mailing of email notifications" on page 130.

6. In the Create Email Report or Edit Email Report dialog window, select the report you just saved and then update the conditions list so that the report is included in the email report when the conditions are met.

   Veritas Backup Reporter runs the report at regular intervals and sends email notifications whenever the report conditions are met—in other words, whenever a potential problem is detected.

Using report data to trigger alerts

By setting threshold conditions in a report's definition, you can cause Veritas Backup Reporter to trigger when those conditions are met. An alert is a form of notification designed to call attention to a potential problem. Alerts display in the VBR console. You can also use them to initiate automated responses, called policies.

For example, you can set up a report so that an alert is generated when the percentage of failed backup jobs reaches a certain level, or when the total size of all backup jobs exceeds a certain threshold.

To define a report to trigger alerts

1. In the VBR console, open a predefined (default) report or launch the Custom Report Wizard.

   See "Using and customizing default reports" on page 53.

   See "Creating and using custom reports" on page 61.

2. Using the controls in the Exception Conditions section of the wizard, define thresholds to represent potential problem conditions.

   These are the conditions under which Veritas Backup Reporter triggers an alert.

   See "Defining report conditions" on page 69.

3. Click **Run** to run the report.

   The report output displays in the console.

4. Save the report.

   See "Saving data in a report" on page 71.

5. Create or edit an email report.

   See "Configuring reports to trigger alerts" on page 134.

6. In the Create Email Report or Edit Email Report dialog box, select the report you just saved and then update the conditions list so that the report is not attached when the conditions are met.

   Veritas Backup Reporter runs the report at regular intervals and triggers an alert whenever the report conditions are met (whenever a potential problem is detected).

Sending routine status updates

You can send an individual report or the contents of a portal page by email to other personnel in your organization. This topic describes how to send the report or portal page you are currently viewing in the VBR console.

You can also schedule routine email deliveries of report data on a regular basis.

See "About configuring and managing report-based notification" on page 127.

To send the report you are currently viewing by email

1. Display a report in the console.
2. Click **Email**.
3. In the Email Report dialog box, type a subject line in the Subject field.

4 Specify one or more recipients by doing one of the following:

- Type (or paste from your system clipboard) a list of email addresses in the Send To field. Use commas to separate each address in the list, for example `reggie@example.com,mark@example.com,sammy@example.com`.
- Select a distribution list from the drop-down list.

5 Type (or paste from your system clipboard) an optional list of carbon-copy (cc) recipients in the CC to field.

Use commas to separate each address in the list.

6 Type an optional message in the Message field, for example:

```
This report shows backup job status as of Thursday morning.
```

7 Click **Send**.

The report is emailed to the specified recipients.

To send the contents of a report portal page by email

1 Select a report subject from the menu bar on the My Reports page, for example Backups.

2 In the My <Subject> Reports portal page, in the My Tools list (in the task pane), click **Email <Subject> Portal Page**.

3 In the Email Report dialog box, type a subject line in the Subject field.

4 Specify one or more recipients by doing one of the following:

- Type (or paste from your system clipboard) a list of email addresses in the Send To field. Use commas to separate each address in the list, for example reggie@example.com,mark@example.com,sammy@example.com.
- Select a distribution list from the drop-down list.

5 Type (or paste from your system clipboard) an optional list of carbon-copy (cc) recipients in the CC to field.

Use commas to separate each address in the list.

6 Type an optional message in the Message field, for example:

```
These reports show key backup data as of Thursday morning.
```

7 Click **Send**.

The portal page contents are emailed to the specified recipients.

About configuring and managing report-based notification

After you customize Veritas Backup Reporter reports or define new ones, you can arrange to use them for automatic notification. There are two primary forms of notification: email and alerts.

Email notifications are email messages, containing data from reports, that are sent on a regular schedule to interested parties. They are useful for notifying key IT staff when problems or potential problems arise as well as for providing status updates at regular intervals.

The following topics describe the steps you take to arrange for report-based notification using email:

- See "Managing report schedules" on page 127.
- See "Managing email distribution lists " on page 129.
- See "Managing the mailing of email notifications" on page 130.

Note: Before setting up email features, make sure that the SMTP Mail server is configured properly.

See the *Veritas Backup Reporter Administrator's Guide* for details about configuring the SMTP Mail server.

Report-triggered alerts are generated when Veritas Backup Reporter reports, running on a predefined schedule, identify a problem or potential problem involving backup or restore.

An alert is a form of notification designed to call attention to a potential problem. Alerts display in the VBR console. You can also use them to initiate automated responses, called policies.

The following topics describe the steps you take to arrange for report-based notification using alerts:

- See "Managing report schedules" on page 127.
- See "Configuring reports to trigger alerts" on page 134.

Managing report schedules

The report schedule specifies the days and the time of day for running the reports on which both email notifications and alerts are based. Each schedule you define

can be assigned to one or more email notifications, report-triggered alerts, or both.

Following are some examples of how you can use report schedules for notification:

- You can arrange to send an email notification—containing data from several different reports—at 6:00 A.M. every day so that operators can view the status of the network when they arrive for work each morning. Alternatively, you can send a different email notification at 12:00 noon on the first day of each month, so that executives have up-to-date data for their monthly status meeting.
- You can schedule reports to run each day or each week so that backup admins are notified whenever potential problems exist in the network. Because the email notifications are based on reports that contain conditions, they are sent only when a potential problem is detected.

You can use the same scheduling process for the following additional purposes:

- Regular updating of cached reports.
  See "Refreshing cached reports" on page 51.
- Regular archiving, or exporting, of reports.
  See "About archiving reports" on page 138.

To schedule reports to run for notification

1. On the console Settings tab, click **Schedules**.
2. In the Schedules window, click **Create**.
3. In the Create Schedule dialog window, in the Name field, type a name for the schedule.
4. Select a time on the At Time drop-down list.

   This is the time at which reports will be sent on the specified days.
5. Select a recurrence pattern for running the reports, and then do one of the following:
   - If you selected Daily, check one or more days each week.
   - If you selected Monthly, select a day of the month from the drop-down list.
6. Click **Save**.

   The new schedule is saved. It appears in the Schedules window.

To edit a notification schedule

1. On the console Settings tab, click **Schedules**.
2. In the Schedules window, click the **Edit** icon next to the name of the schedule.

3 In the Modify Schedule dialog window, do any of the following:

- In the Name field, type a name for the schedule.
- Change the time by indicating a new time from the At Time drop-down list.
  This is the time at which reports will be sent on the specified days.
- Change the recurrence pattern to either Daily or Monthly, and then do one of the following:
  - If you selected Daily, check one or more days for reports to be sent each week.
  - If you selected Monthly, select a day of the month from the drop-down list.

4 Click **Save**.

To delete a report schedule

1 On the console Settings tab, click **Schedules**.

2 In the Schedules window, check the names of the schedules you want to delete.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.

To set font style and font size of e-mail messages

1 Open the `application.properties` file.

2 Modify the following parameters:

- schedule.email.font.face - Type the font name / style.
- schedule.email.font.size - Type the font size.

3 Save the file.

The system will use the new font style and size for e-mails text.

Managing email distribution lists

You can set up email distribution lists for distributing reports to interested parties and for notifying key IT staff when problems or potential problems arise.

To create a distribution list for email notifications

1 On the console Settings tab, click **Distribution Lists**.

2 In the Distribution Lists window, click **Create**.

3 In the Create Distribution List dialog window, type the name of the distribution list in the Name field.

4 Type (or paste from your system clipboard) a list of email addresses in the Send To field.

Use commas to separate each address in the list, for example
`reggie@example.com,mark@example.com,sammy@example.com`

5 Click **Save**.

The new distribution list appears in the Distribution Lists window.

To edit a distribution list for email notifications

1 On the console Settings tab, click **Distribution Lists**.

2 In the Distribution Lists window, click the **Edit** icon next to the name of the distribution list you want to edit.

3 In the Edit Distribution List dialog window, do one or both of the following:

- Change the name of the list by typing over the value in the Name field.
- Update the list of email addresses in the Send To field.
  Use commas to separate each address in the list, for example
  `reggie@example.com,mark@example.com,sammy@example.com`

4 Click **Save**.

To delete a distribution list for email notifications

1 On the console Settings tab, click **Distribution Lists**.

2 In the Distribution Lists window, check the names of the distribution lists you want to delete.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.

Managing the mailing of email notifications

After you have created schedules and distribution lists for email notifications, you configure the email notifications themselves. You do this by specifying which reports to include in the email notification, the schedule on which it is sent, the people to whom it is sent, and the contents of the email message.

If the email notification contains reports with conditions, you can set it up so that the reports are included only when the conditions are met. Note that, if no conditions are met and no reports are included, then no email notification is sent. (In other words, users will not receive an empty email notification.)

To configure the distribution of an email notification

1 On the console Settings tab, click **Email/Export Reports**.

2 In the Email Reports list, click **Create**.

3 In the Create Email Report dialog window, in the Name field, type a name for the email notification.

The name should be descriptive enough that you can click it from a list of email notifications.

4 Click **Enabled** to activate email distribution for the indicated report.

The report will be sent at the next scheduled interval. (Deselect if you want to defer email distribution for this report until later.)

5 On the Schedule drop-down list, select a schedule.

The schedule determines the time and days on which the email is sent.

6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

See "Managing report schedules" on page 127.

7 From the Select Report list box, click the names of one or more reports to send within the email notification.

8 To specify who will receive the email, do one of the following:

- Click a list of recipients from the Distribution List drop-down list.
  To define a distribution list that does not appear in the drop-down list, click the **Edit** icon next to the list.
  See "Managing email distribution lists " on page 129.
- Type email addresses for individual recipients, separated by commas, in the Send to, CC to, and BCC to fields.
  Example: `operator1@example.com,joe@example.com`

9 Type text in the Subject field.

This text will appear as the subject for each email message that is sent. Use substitution tokens to include variable data, such as the name of an alert.

See "About using variable data in notifications" on page 137.

Example: `$Alert.Alert Key$ in Backup Report`

10 Click one of the following formats:

HTML	Display in a Web browser. Unlike the other formats, HTML preserves the original format of the data as well as any graphics in the original report.
CSV	For use with spreadsheet programs.
TSV	Compatible with word-processing applications and text editors.
XML	Can be imported (using user-written scripts) by other programs like databases or billing applications.

11 Type an optional message in the Message field.

This text appears within each email message along with the contents of the indicated reports.

12 If you have clicked reports in which exception conditions are defined, do the following in the Exception Conditions area of the dialog window:

- Check the reports to run.
- Check the conditions within reports that, when met, will cause the corresponding report to be included in an email notification.
  The exception conditions defined for these reports represent problems or potential problems. When you click conditions in this dialog window, Veritas Backup Reporter includes the report data in an email message whenever a potential problem is detected.
  See "Using report data to notify staff when problems occur" on page 123.
- To send the email notification only when one or more of the selected exception conditions are met, click **Send email only if reports are attached**.
  If you uncheck this box, an email notification is always sent at the scheduled interval, regardless of whether any reports are included.
- Click **Update Conditions List** to confirm the Exception Conditions settings.

13 Click **Save**.

The new email notification appears in the Email Reports list.

To edit an email notification

1 On the console Settings tab, click **Email/Export Reports**.

2 In the Email Reports window, click the **Edit** icon next to the name of the email notification.

3 In the Edit Email Report dialog box, do any or all of the following:

- In the Name field, change the name of the email notification.
- Check **Enabled** to activate email distribution for the selected report.
  The report will be sent at the next scheduled interval. (Uncheck if you want to defer email distribution for this report until later.)
- From the Schedule drop-down list, select a schedule.
  The schedule determines the time and days on which the email is sent.
  To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
  See "Managing report schedules" on page 127.
- In the Select Report drop-down list, select one or more reports to send.
  Cancel the selected reports you no longer want to send.
- Specify who will receive the email by doing one of the following:
  - Select a list of recipients from the Distribution List drop-down list.
    To define a distribution list that does not appear in the drop-down list, click the **Edit** icon next to the list.
    See "Managing email distribution lists " on page 129.
  - Add or remove email addresses for individual recipients in the Send to, CC to, and BCC to fields.
    Use commas to separate addresses. Example:
    `operator1@example.com,joe@example.com`
- Change the text in the Subject field.
  This text will appear as the subject for each email message that is sent.
  Use substitution tokens to include variable data, such as the name of an alert. Example: `$Alert.Alert Key$ in Backup Report`
  See "About using variable data in notifications" on page 137.
- Select one of the following formats:
  - HTML
  - XML
  - CSV
  - TSV
- Change the text in the Message field.
  This text will appear within each email message along with the contents of the selected reports.

- Update the list of reports and conditions to determine which exception conditions, when met, will cause the corresponding report to be included in the email notification, and then click **Update Conditions List**.

4 Click **Save**.

To delete email notifications

1 On the console Settings tab, click **Email/Export Reports**.

2 In the Email Reports window, check the names of the email notifications you want to delete.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.

Configuring reports to trigger alerts

After setting threshold conditions in a report's definition, you can cause Veritas Backup Reporter to generate alerts when those conditions are met. For example, you can set up report-triggered alerts to indicate that the percentage of failed backup jobs has reached a certain level, or that the total size of all backup jobs has exceeded a certain threshold.

Following is the process with which Veritas Backup Reporter generates a report-triggered alert:

- A report containing one or more conditions runs according to a predefined schedule.
  See "Managing report schedules" on page 127.
- The report shows that at least one of its conditions has been met, that is, a threshold has been exceeded.
- Based on this result, Veritas Backup Reporter generates an alert.

To define a report-triggered alert

1 On the console Settings tab, click **Alert Trigger Reports**.

2 In the Alert Trigger Reports list, click **Create**.

3 In the Create Alert Trigger Report dialog window, in the Name field, type a name for the alert definition.

The name should be descriptive enough that you can click it from a list of alert definitions.

4 Click **Enabled** to activate the alert definition.

Veritas Backup Reporter will begin generating alerts whenever any of the clicked reports are run and their conditions met. (Cancel the selection if you want to avoid generating alerts for now.)

5 On the Schedule drop-down list, select a schedule.

The schedule determines the time and days on which the reports are run to test their conditions.

6 To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

See "Managing report schedules" on page 127.

7 On the Select Report drop-down list, select the names of one or more reports to run.

8 On the Alert Severity drop-down list, select one of the following:

- CRITICAL
- ERROR
- WARNING
- INFORMATION

9 Type **Alert_Trigger** in the Alert Type field to specify the alert type.

10 Type summary text in the Alert Summary field.

This text displays in alert listings in the VBR console.

11 To associate the alert with a specific report condition, use the following substitution strings in the text:

`$Condition$`	The metric used for the report condition, for example `Total Backup Job Size`
`$ReportName$`	The name of the report containing the condition.
`Condition $Condition$ on $ReportName$ has matched`	Default

12 Type optional descriptive text in the Alert Description field.

This text displays when a console user views details about the alert.

Default: `Condition $Condition$ on $ReportName$ has matched`

13 If you have clicked reports in which exception conditions are defined, do the following in the Exception Conditions area of the dialog window:

- Check the reports to run.
- Check the conditions within reports that, when met, will trigger an alert. (A separate alert is triggered for each condition met.)
  The exception conditions defined for these reports represent problems or potential problems. When you click conditions in this dialog window, Veritas Backup Reporter triggers an alert whenever a potential problem is detected.
  See "Using report data to notify staff when problems occur" on page 123.
- Click **Update Conditions List** to confirm the Exception Conditions settings.

14 Click **Save**.

The new report-triggered alert appears in the Alert Trigger Reports list.

To edit a report-triggered alert

1 On the console Settings tab, click **Alert Trigger Reports**.

2 In the Alert Trigger Reports list, click the **Edit** icon next to the name of the report-triggered alert.

3 In the Edit Alert Trigger Report dialog box, do any of the following:

- In the Name field, change the name of the alert definition.
- Click **Enabled** to activate the alert definition.
  Veritas Backup Reporter will begin generating alerts whenever any of the selected reports are run and their conditions met. (Cancel the selection if you want to avoid generating alerts for now.)
- On the Schedule drop-down list, click a schedule.
  The schedule determines the time and days on which the reports are run to test their conditions.
- To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
  See "Managing report schedules" on page 127.
- On the Select Report drop-down list, select the names of one or more reports to run.
  Cancel the clicked reports you no longer want to run.
- On the Alert Severity drop-down list, select one of the following:
  - CRITICAL
  - ERROR

- WARNING
- INFORMATION

- Change the summary text in the Alert Summary field.
- Change the descriptive text in the Alert Description field.
- Update the list of conditions which, when met, will cause an alert to be generated, and then click **Update Conditions List**.

4 Click **Save**.

About using variable data in notifications

You can use substitution tokens to provide variable data in notifications. For example, you can insert the name and severity of an alert into the subject line of a notification email.

Table 6-1 includes an alphabetical list of the substitution tokens available for including variable data in notifications.

Table 6-1 Substitution tokens for variable data in notifications

Token	Description
$Alert.Agent$	Name of the VBR Agent host that issued the alert.
$Alert.Alert Group$	Category to which the alert belongs, for example `Partial Success`.
$Alert.Alert Key$	Numeric identifier optionally be associated with the alert. In the case of Backup Job failure alert, it refers to the error code returned from the backup software. (Same as $Alert.JobStatus$.)
$Alert.Count$	Number of times this alert was issued by the host since the last time it was cleared manually.
$Alert.EventType$	Alert class. For example, all backup failures—even if reported by different products—display an alert class of `BackupJob`.
$Alert.First Occurrence$	Date and time of origin for the event that created the alert. When there is a delay between the event and the creation of the alert, this token preserves the original event time.
$Alert.IP$	IP address of the host issuing the alert.
$Alert.Initial Severity$	Numeric designation of the alert's severity: 5 = `CRITICAL` 4 = `ERROR` 3 = `WARNING` 2 = `INFORMATION`

Table 6-1 Substitution tokens for variable data in notifications *(continued)*

Token	Description
$Alert.Job ID$	Job ID for the job associated with the alert.
$Alert.JobStatus$	Numeric identifier optionally be associated with the alert. In the case of Backup Job failure alert, it refers to the error code returned from the backup software. (Same as $Alert.Alert Key$.)
$Alert.Last Occurrence$	Time when the last deduplicated event was generated. Example: A backup job on `HostA` fails with error code 3, and an alert already exists from `HostA` with error code 3. $Alert.Last Occurrence$ contains the time the backup job was performed.
$Alert.Leveln$	The name of the object level within a view (specified in $Alert.View Name$) associated with the alert. n can be any integer between 1 and 12. Examples (within the `Geography` view): `Canada`, `Vancouver`
$Alert.Node$	Node of the VBR Agent host that issued the alert.
$Alert.Other Info n$	Optional additional information about the alert, such as the name of the schedule on which it was generated (where n is 1 or 2).
$Alert.View Name$	The primary view (specified in Settings > Global Settings > Monitoring Settings) used to identify attributes of the machine where the alert originated, such as its location or contact person. Examples: `Geography`, `Business Unit`

About archiving reports

After you define custom reports, you can archive them by arranging to store them on the VBR Management Server at regular intervals. This process is called exporting. You can set up the exporting of reports on a regular schedule.

Data from exported reports is stored in a default directory. A user with administrator-level privileges can designate this directory.

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

About managing export schedules

The report schedule specifies the days and the time of day at which reports are exported. Each schedule you define can be assigned to one or more export activities.

The process for defining schedules for exports is the same as that for email notifications and report-triggered alerts. In fact, you can use the same schedule to export reports and generate notifications.

See "Managing report schedules" on page 127.

Setting up exporting of reports

After you have created schedules for exporting reports, you configure the export activities. You do this by specifying which reports are exported, the format of the exported file, and the export schedule.

To configure an export operation for reports

1. On the console Settings tab, click **Email/Export Reports**.
2. In the Export Reports list, click **Create**.
3. In the Create Export Report dialog box, in the Name field, type the file name to be used for the export operations.

   The name should be descriptive enough that you can select it from a list of export operations.
4. Click **Enabled** to activate exporting.

   At the next scheduled interval, the indicated reports will be exported to the directory location displayed at the bottom of the dialog window. (Deselect if you want to defer exporting until later.)
5. On the Schedule drop-down list, select a schedule.

   The schedule determines the time and days on which the export operation occurs.
6. To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.

   See "Managing report schedules" on page 127.
7. On the Select Report drop-down list, select the names of one or more reports to export.
8. Select one of the following file formats:

   - CSV (comma-separated)
   - TSV (tab-separated)

   The format you choose depends on how the data will be displayed and manipulated. For example, many spreadsheet programs import data in CSV

format, while TSV-formatted files are compatible with word-processing applications and text editors.

9 Click **Save**.

The new export operation appears in the Export Reports list. The export operation will include data from all of the selected reports in a file that has the name and format you specified.

To configure an export operation for reports

1 On the console Settings tab, click **Email/Export Reports**.

2 In the Export Reports list, click **Edit**.

3 In the Edit Export Report dialog box, do any of following:

- In the Name field, change the file name to be used for the export operation.
- Click **Enabled** to activate exporting.
  At the next scheduled interval, the selected reports will be exported to the directory location displayed at the bottom of the dialog window. (Deselect if you want to defer exporting until later.)
- On the Schedule drop-down list, select a schedule.
  The schedule determines the time and days on which the export operation occurs.
- To define a schedule that does not appear in the drop-down list, click the **Edit** icon next to the list.
  See "Managing report schedules" on page 127.
- On the Select Report drop-down list, select one or more reports to export.
  Cancel the selected reports you no longer want to export.
- Change the file format to **CSV** (comma-separated) or **TSV** (tab-separated).

4 Click **Save**.

To delete export operations for reports

1 On the console Settings tab, click **Email/Export Reports**.

2 In the Export Reports window, check the names of the export operations you want to delete.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.

Glossary

Administrator console	See *Veritas Backup Reporter View Builder*.
Agent	See *VBR Agent*.
alert	One of several types of configurable notifications produced when a Veritas Alert Manager alarm is triggered. An alert is dynamic, resetting itself automatically when a condition monitored by a policy returns to its specified `CLEAR` state.
Alert Manager	See *Veritas Alert Manager*.
application	A program or group of programs designed to perform a specific task. Oracle Database and Veritas NetBackup are examples of applications.
Audit Log	A text file that contains a list of all changes made to the SAN Access Layer (SAL)—such as devices added and removed—and to the Veritas Alert Manager—such as modifications to policy and alert notification and changes to configuration settings.
Authentication Service	See *Symantec Product Authentication Service* .
circuit breaker	A function in the Veritas Alert Manager that automatically limits the number of notifications sent to a recipient within a specified time.
Veritas Alert Manager	A server component that manages policies associated with objects on the storage network. A policy associates certain sets of conditions with storage resources and defines actions to be taken when these conditions are detected. The Alert Manager is seamlessly integrated with the Veritas products so that console users can monitor, define, and modify policies.
VBR console	A graphical user interface that displays reports and other information for users of Veritas Backup Reporter through a standard Web browser. The console provides a central point to manage cost analysis and chargeback for services, managing workflow, displaying and managing reports, and other tasks.
VBR database	A database, residing on the Server, that gathers data related to performance and monitoring, reports, alarms, service requests, and the SAN Access Layer (SAL). A Sybase ASA (Adaptive Server Anywhere) database management system, the Server database is installed silently when you install Veritas Backup Reporter.
Veritas Backup Reporter	A product offering that tracks IT effectiveness by providing complete business-level reporting of resource utilization, costs, and service level delivery. Veritas Backup Reporter also helps enable business customers ensure that their application performance and availability requirements are met at the lowest cost.

VBR Agent	The part of Veritas Backup Reporter that collects information from discoverable applications residing on remote host systems, such as Veritas NetBackup, Veritas Backup Exec, and EMC Legato Networker. Veritas Backup Reporter formats the information collected from these applications and displays it through the VBR console.
VBR Management Server	The portion of the Veritas Backup Reporter product offering that resides on the primary host.
VBR View Builder	A Flash-based application in which an administrator creates, modifies, and manages access to the object views that users see in the VBR console. (An earlier, Java-based version of this application was known as the Administrator console in earlier releases of Veritas Backup Reporter.) See also *object view*.
CommandCentral Storage	A product designed to maximize the return on an enterprise's storage technology investment by providing tools with which a storage administrator can make the storage network or SAN operate as effectively as possible.
console	See *VBR console*.
device	A collective term for disks, tapes, disk arrays, tape arrays, and any other objects that store data.
event	A notification that indicates when an action, such as an alert or a change in state, has occurred for one or more objects on the storage network.
failover	A backup operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing.
file system	A means of organizing the addressable storage of one or more physical or virtual disks to give users and applications a convenient way of organizing files. File systems appear to users and applications as directories arranged in a hierarchy.
firmware	A set of software instructions set permanently in a device's memory.
folder	In the VBR console, one of several logical containers in which users can display and monitor reports and Active Practices. Examples of folders are My Reports, My Active Practices, and the public Catalog folder.
host	A computer system to which storage devices and file servers are attached. Synonymous with system in Veritas Cluster Server.
IP address	An identifier for a computer or other device on a TCP/IP network, written as four eight-bit numbers separated by periods. Messages and other data are routed on the network according to their destination IP addresses. See also *virtual IP address*.
master server	The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. NetBackup BusinesServer supports only a single server, and it is the master. See also *Veritas NetBackup*. See also *media server*.

media server A NetBackup server that provides storage within a master and media server cluster. The master can also be a media server. A media server that is not the master is called a remote media server. NetBackup BusinesServer does not support remote media servers. See also *master server*.

My Reports In Veritas Backup Reporter, a console area in which to display and run custom reports saved by the user.

NetBackup See *Veritas NetBackup*.

node An object in a network. In Veritas Cluster Server, refers specifically to one of any number of hosts in a cluster. See also *object*.

object view A graphical display showing storage resources and information about them. In Veritas Backup Reporter, an administrator can use the View Builder to create, modify, and manage access to object views. See also *Veritas Backup Reporter View Builder*.

policy A set of rules, or configuration settings, that are applied across a number of objects in the storage network. You establish policies to help you monitor and manage the network. Each policy associates certain sets of conditions with storage resources and defines actions to be taken when these conditions are detected. See also *collector*.

Policy Service See *Veritas Alert Manager*.

primary server See *server*.

resource Any of the individual components that work together to provide services on a network. A resource may be a physical component such as a storage array or a switch, a software component such as Oracle8 or a Web server, or a configuration component such as an IP address or mounted file system.

robotic library A collection of tapes controlled and managed through firmware.

router A device that connects two segments of a storage network and determines the optimal path along which traffic should be forwarded. See also *bridge*.

SAN Acronym for “storage area network.” A network linking servers or workstations to devices, typically over Fibre Channel, a versatile, high-speed transport. The storage area network (SAN) model places storage on its own dedicated network, removing data storage from both the server-to-disk SCSI bus and the main user network. The SAN includes one or more hosts that provide a point of interface with LAN users, as well as (in the case of large SANs) one or more fabric switches and SAN hubs to accommodate a large number of storage devices.

SCSI Small Computer Systems Interface. A hardware interface that allows for the connection of multiple peripheral devices to a single expansion board that plugs into the computer. The interface is widely used to connect personal computers to peripheral devices such as disk and media drives.

SCSI bus	The communication pathway between a SCSI host adapter card and target SCSI devices. Physically, the bus begins at one end of a SCSI cable at the host adapter card and ends at the other end of the cable at the target device.
SCSI disk	A storage device (fixed disk) attached to a SCSI bus.
server	The machine on which the VBR database resides. A typical configuration consists of one server (for example, the VBR Management Server) and several Agent hosts.
slot	An opening in a computer or other network device into which a printed circuit board can be inserted, adding capability to the device. See also *expansion slot*.
SMTP	Simple Mail Transfer Protocol, a commonly used protocol for sending email messages between servers.
snapshot	A point-in-time image of a volume or file system that can be used as a backup. See also *SAN snapshot*.
SNMP	The Simple Network Management Protocol for Internet network management and communications used to promote interoperability. SNMP depends on cooperating systems that must adhere to a common framework and a common language or protocol.
storage area network (SAN)	See *SAN*.
subnet	A portion of a storage network typically consisting of all machines in one locale, in one building, or on the same local area network (LAN). Internet Request for Comments 950 provides the standard procedure for creating and identifying subnets.
subnet mask	A 32-bit mask that identifies the portions of an IP address to be used for locating addresses in a subnetwork.
switch	A network device to which nodes attach and which provides high-speed switching of node connections via link-level addressing.
system	The physical hardware on which data and applications reside, and the connections between them. In Veritas Backup Reporter Availability, the physical components on which applications and VCS cluster service groups reside. See also *host*.
tape device	A storage device that writes data to tape. Veritas Backup Reporter identifies a tape drive, tape transport, and tape arrays as a tape device.
tape mark	A mark that is recorded between backup images on a tape.
topology	The physical or logical arrangement of resources on the storage network and the connections between them.

Symantec Product Authentication Service A component of the Veritas Security Services (VxSS) that is used by the Veritas products to provide user authentication. Symantec Product Authentication Service is a set of processes and runtime libraries that enables users to log on to multiple Veritas products with one logon.

Veritas NetBackup A Veritas product family designed to provide a fast, reliable backup and recovery solution for environments ranging from terabytes to petabytes in size. The term is used to refer to either of two products that interact with Veritas Backup Reporter: Veritas NetBackup DataCenter and Veritas NetBackup BusinesServer.

Symantec Private Branch Exchange A common Veritas component that uses socket passing to reduce the number of ports required to be open across a firewall. Symantec Private Branch Exchange uses a paradigm similar to that of a telephone switchboard in which calls placed to a switchboard are redirected to a known extension. In the PBX exchange, client connections sent to the exchange's port are redirected to an extension associated with the VBR Management Server.

Veritas Volume Manager A Veritas software product installed on storage clients that enables management of physical disks as logical devices. Volume Manager enhances data storage management by controlling space allocation, performance, data availability, device installation, and system monitoring of private and shared systems.

View Builder See *Veritas Backup Reporter View Builder*.

virtual fabric A storage area network (SAN) technology in which a group of switches and other objects constitute a hardware-based, isolated environment within a physical fabric. Virtual fabrics create multiple, isolated SAN environments within a physical SAN fabric in order to enable more efficient use of the SAN, especially in terms of availability and scalability.

volume In storage media managed by Veritas Volume Manager, a virtual disk made up of a portion or portions of one or more physical disks and representing an addressable range of disk blocks. It is used by applications such as file systems or databases.

A file system on a NetApp unified storage device, such as a filer. Each device has a root volume containing its configuration files, and one or more data volumes containing user data.

Volume Manager See *Veritas Volume Manager*.

XML import/export utility A tool with which an administrator or service provider can preserve report data in XML format. The user can import the formatted data into the VBR console for later use.

Index

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W