

CA ARCserve® Backup for Windows

Dashboard User Guide

r12.5



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2009 CA. All rights reserved.

CA Product References

This document references the following CA products:

- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- CA Antivirus
- CA ARCserve® Backup Agent for Advantage™ Ingres®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Microsoft Windows Essential Business Server
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint
- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for Virtual Machines

- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Disk to Disk to Tape Option
- CA ARCserve® Backup for Windows Enterprise Module
- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA Dynam®/B Backup for z/VM
- CA VM: Tape for z/VM
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- CA 1® Tape Management
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM: Operator®

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At <http://ca.com/support>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA support website, found at <http://ca.com/support>.

Contents

Chapter 1: Understanding Dashboard	11
Introduction	11
Dashboard Features.....	13
Dashboard GUI	14
Display Options	15
Customize Dashboard Reports	18
Global Options	18
Configure Email Reports	20
Report-Specific Options.....	28
SRM Probe Settings	29
 Chapter 2: Using Dashboard	 31
Use CA ARCserve Backup Dashboard	31
Dashboard Groups	33
Add a Dashboard Group	35
Modify a Dashboard Group.....	36
Delete a Dashboard Group.....	37
Node Tiers	38
Node Information	39
Agent Upgrade Alert	40
 Chapter 3: Dashboard Reports	 41
CA ARCserve Backup Dashboard Report Types	41
Backup Environment Type Reports	42
SRM Type Reports	42
Drill Down Reports	43
Agent Distribution Report	44
Report Benefits	44
Report View	45
Drill Down Reports	46
Backup Data Location Report	48
Report Benefits	48
Report View	49
Drill Down Reports	50
Backup Server Load Distribution Report	51
Report Benefits	51

Report View	51
CPU Report	54
Report Benefits	54
Report View	55
Drill Down Reports	56
Data Distribution on Media Report	57
Report Benefits	57
Report View	58
Drill Down Reports	59
Deduplication Benefits Estimate Report	60
Report Benefits	60
Report View	61
Deduplication Status Report	62
Report Benefits	62
Report View	63
Drill Down Reports	64
Disk Report	65
Report Benefits	65
Report View	65
Drill Down Report	67
Job Backup Status Report	68
Report Benefits	68
Report View	69
Drill Down Reports	71
License Report	73
Report Benefits	73
Report View	74
Media Assurance Report	75
Report Benefits	75
Report View	76
Drill Down Reports	77
Memory Report	78
Report Benefits	78
Report View	79
Drill Down Reports	80
NIC Report	81
Report Benefits	81
Report View	82
Drill Down Reports	83
Node Backup Status Report	84
Report Benefits	84
Report View	84
Drill Down Reports	87

Node Disaster Recovery Status Report	89
Report Benefits	90
Report View	91
Drill Down Reports	92
Node Encryption Status Report	94
Report Benefits	94
Report View	95
Drill Down Reports	96
Node Recovery Points Report	98
Report Benefits	98
Report View	99
Drill Down Reports	100
Node Summary Report	101
Report Benefits	101
Report View	102
Node Tiers Report	103
Report Benefits	103
Report View	104
Drill Down Reports	105
Node Whose Most Recent Backup Failed Report	106
Report Benefits	106
Report View	106
Drill Down Reports	108
OS Report	109
Report Benefits	109
Report View	110
Recovery Point Objective Report	111
Report Benefits	112
Report View	113
Drill Down Reports	114
SCSI/Fiber Card Report	115
Report Benefits	115
Report View	116
Drill Down Reports	117
Tape Encryption Status Report	118
Report Benefits	118
Report View	119
Drill Down Reports	119
Top Nodes with Failed Backups Report	122
Report Benefits	122
Report View	123
Drill Down Reports	124
Top Nodes with Fastest/Slowest Backup Throughputs Report	125

Report Benefits	125
Report View	126
Virtual Machine Recovery Points Report	127
Report Benefits	127
Report View	128
Drill Down Reports	129
Virtualization Most Recent Backup Status Report	130
Report Benefits	130
Report View	131
Drill Down Report	132
Volume Report	133
Report Benefits	133
Report View	133
Drill Down Reports	135
 Chapter 4: Troubleshooting	 137
 Index	 145

Chapter 1: Understanding Dashboard

This section contains the following topics:

[Introduction](#) (see page 11)

[Dashboard Features](#) (see page 13)

[Dashboard GUI](#) (see page 14)

[Display Options](#) (see page 15)

[Customize Dashboard Reports](#) (see page 18)

Introduction

The CA ARCserve Backup Dashboard is a user interface tool that provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment. This dashboard view lets you quickly and easily monitor relevant information to help you manage the performance and operation of your backup and SRM environment. The CA ARCserve Backup Dashboard provides snapshot displays that provide an overall status of the specified CA ARCserve Backup domain, servers, nodes, and/or jobs.

In addition, some of the reports have an enhanced capability to drill down into the report to display more detailed information. For these reports, you can click on any of the status categories to drill down from a display of summary information to a more focused and detailed report about that particular category.

You can access the CA ARCserve Backup Dashboard from the Monitor & Reports Menu on the Navigation Bar of the CA ARCserve Backup Manager Console or from the Quick Start menu.

Note: Dashboard can only be accessed by users having CA ARCserve Backup Administrator, Monitor Operator, and Report Operator assigned user profile roles. For more information about User Profiles, see the *Administration Guide* or online help.

The reports displayed on the CA ARCserve Backup Dashboard are:

Note: An asterisk symbol * indicates an SRM-type report.

- Agent Distribution Report
- Backup Data Location Report
- Backup Server Load Distribution Report
- CPU Report *
- Data Distribution on Media Report
- Deduplication Benefits Estimate Report
- Deduplication Status Report
- Disk Report *
- Job Backup Status Report
- License Report
- Media Assurance Report
- Memory Report *
- NIC Report *
- Node Backup Status Report
- Node Disaster Recovery Status Report
- Node Encryption Status Report
- Node Recovery Points Report
- Node Summary Report *
- Node Tiers Report
- Node Whose Most Recent Backup Failed Report
- Operating System Report *
- Recovery Point Objective Report
- SCSI/Fiber Card Report *
- Tape Encryption Status Report
- Top Nodes with Failed Backups Report
- Top Nodes with Fastest/Slowest Backup Throughput Report
- Virtual Machine Recovery Points Report
- Virtualization Most Recent Backup Status Report
- Volume Report *

Dashboard Features

Dashboard contains the following features:

- Provides a central snapshot overview of your backup infrastructure and your storage resource management (SRM) environment.
- Provides 29 individual reports, focusing on such items as jobs, nodes, tapes, encryption, resources of agent machines etc.
- Provides the capability to customize the look of CA ARCserve Backup Dashboard to meet your specific needs and preferences.
- Some reports provide an enhanced capability to drill down into the report to display more detailed and focused information.
- Provides filtering capabilities to limit the data being displayed in the report based upon specified parameters.
- Provides the capability to create customized collections (groups) of reports that when selected displays the specified reports as a pre-configured grouping based upon your specific needs or preferences.
- Provides the capability to manually or automatically refresh the data displayed on the reports.
- Provides the capability to export the collected data for the reports in various formats (print, save as a CSV for use in a spreadsheet, or email).
- Provides the capability to create a customized schedule for sending reports via email to specified recipient(s).
- Provides the capability to perform a probe to collect SRM-related data for the SRM-type reports.

Dashboard GUI

The Dashboard GUI consists of two report content panes on the left side and a report display window on the right.

The screenshot shows the Dashboard GUI interface. Red arrows point to the following components:

- Global Options:** Located at the top left, showing 'Date Range for All: Last 7 Days' and 'Node name:'.
- Dashboard Groups Selection Pane:** A pane on the left titled 'Dashboard Groups' with a list of groups like 'Backup Status', 'Encryption', etc.
- Agent Upgrade Alert Pane:** A yellow alert box at the top right titled 'Agent Upgrade Required' with buttons for 'Upgrade Now', 'Remind Me Later', and 'Remind me after 1 Day'.
- All Reports Selection Pane:** A pane on the left titled 'All Reports' with a list of reports like 'Agent Distribution Report', 'Backup Date Location Report', etc.
- Report Display Window:** The main area on the right displaying various reports:
 - Node Backup Status Report:** Shows a pie chart and a table of backup status (Failed, Cancelled, Incomplete, Not Attempted).
 - Job Backup Status Report:** Shows a pie chart and a table of job status (Failed, Cancelled, Incomplete, Successful).
 - Top Nodes with Failed Backups Report:** Shows a table of nodes with failed backup counts.
 - Node Whose Most Recent Backup Failed Report:** Shows a table of nodes with their most recent backup failure times.

Dashboard Groups

This pane displays a list of Dashboard Groups. A Dashboard Group is a collection of one or more Dashboard reports. (The maximum number of reports that can be included in a group is four). By default, several pre-configured groups are automatically included. You can create, modify, or delete groups based on your requirements. For more information, see [Dashboard Groups](#) (see page 33).

All Reports

This pane displays a complete list of all available reports (in alphabetical order).

Report Display Window

This window displays the selected report(s). You can choose to display one or more of the individual reports (which are listed in the All Reports pane) or display one of the pre-defined Dashboard Groups (which are listed in the Dashboard Groups pane).

Global options toolbar

This toolbar lets you to apply specified actions to all reports. For more information, see [Global Options](#) (see page 18).

Agent Upgrade Alert

This is a warning message which pops up when you launch Dashboard and it is detected that your backup environment contains some CA ARCserve Backup agents that are at a version older than r12.5. For more information, see [Agent Upgrade Alert](#) (see page 40).

Display Options

Dashboard lets you select how you want the graphical information to be displayed. These graphical controls let you select such options as whether you want your information displayed as a pie chart or as a bar chart, whether you want to expand or collapse the viewed report, whether you want to refresh the data being displayed, and what to do with the collected data.

Pie Chart Display

A pie chart is a circular chart divided into a series of sectors, with each sector representing a relative percent of the total categories being monitored. Together, the sectors represent a full 100% of the monitored information. The advantage of pie charts is that they are simple. Pie charts provide you with an aggregate view over a period of time. However, a disadvantage is that it can be very difficult to see the difference in slice sizes when their values are similar.

Bar Chart Display

Bar charts are used to highlight separate quantities. The greater the length of the bars, the greater the value. Bar charts are useful for comparing quantities within or among categories. For some reports, bar charts provide you with a daily view over a period of time, which can help in identifying trends/patterns. You might find it difficult to compare segments from a pie chart; however, in a bar chart, these segments become bars which are much easier to make comparisons.

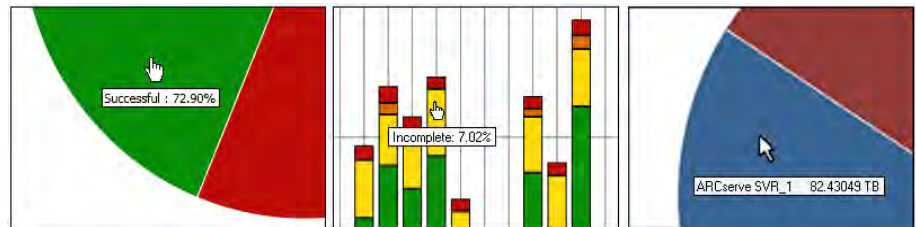
Tabular View

Tabular charts are used to display report information in a table format. The column headings may vary between different reports and also may vary within a specific report between selected report categories. Table views allow you to sort the report information based upon a specific column heading.

Cursor Actions

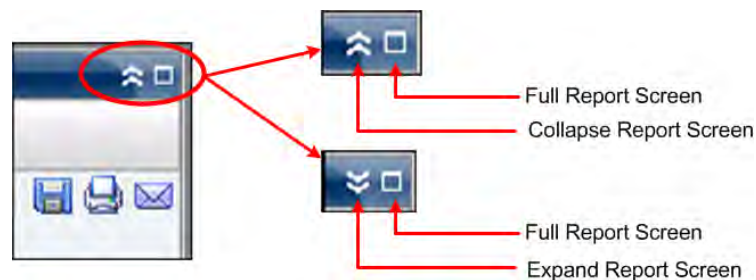
For either graphical display (pie chart or bar chart), when you hover the mouse cursor over a particular category of a report, a small box appears under the cursor displaying the category and its corresponding value.

If the cursor is a pointing hand symbol, it is an indication that the corresponding area is "clickable" and can display additional information about that category when clicked. If the cursor is an arrow symbol, it is an indication that the corresponding area is not "clickable" and no additional information is available.



Report Displaying

All reports let you select how they are displayed. From the overall display, you can collapse an individual report if you do not want to view the report details, and then expand it back to its original size. (When a report is collapsed it only displays the title bar and description bar). In addition, you can also select to fully expand the report to a full screen view. You can also double click on the title bar of a report to maximize it or bring it back to default view.



Report Refresh

All reports let you refresh or reload the data to be displayed on the corresponding report. Each report has a refresh button that updates the display for the corresponding report to let you view up-to-date information about your backup/SRM environment. A refresh indicator provides a visual indication that the displayed data is being refreshed. Although Dashboard does not provide an option to automatically refresh reports after every few seconds, you can click Refresh All in global toolbar to refresh all the Dashboard reports at once. In addition, when you switch from one report (report A) to another (report B), report B is automatically refreshed.



Data Exporting

All reports let you export collected data for the corresponding report. For each report you can specify if you want to print the collected data, save it as a Comma-Separated Values (CSV) file to store the tabular data (to be used in a spreadsheet), or email the report through a SMTP server.

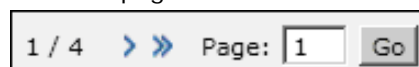
- If you select to print the report, you can avoid printing an "about blank" string at the end of the report by accessing the Page Setting dialog from the print preview screen and deleting the information from the Footer field (or enter your custom text in the footer field).
- If you select to email the report, the content is the same as the printed content and all graphical charts are sent as embedded images.

Note: Before any email can be sent out (either from the GUI or scheduled), you must first configure the SMTP setting using the Alert Manager. For more information, see the *Administration Guide* or online help.



Next Page Button

For any drill-down report that contains more than 100 message entries, Dashboard automatically paginates the display and includes a next page button. Each subsequent page is then limited to 100 entries before creating another page. The next page button lets you jump to view a different page.



Customize Dashboard Reports

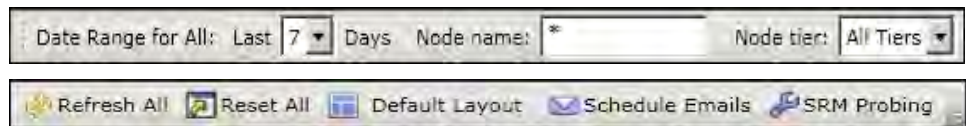
Each report contains various configuration options that let you customize the look and performance of CA ARCserve Backup Dashboard to meet your specific needs and preferences. For many of the reports, you can select such features as how the graphical information is displayed, the time period for the report, the servers or node tiers being monitored, the backup methods being monitored, what to do with the collected information, and many other report-specific options.

Any parameter or configuration settings that you make to the individual reports remain with the same settings when you close and re-open Dashboard. It does not automatically return to the default settings. In addition, to further enable customized reports, the configuration settings that you make to one of the reports does not get applied automatically to all the remaining reports. Each individual report can have its own specific settings.

However, Dashboard also lets you make some configuration settings that would be globally applied to all reports. These global settings let you specify the time period (number of days) for all reports, specify the node tiers being monitored, refresh the displayed data for all reports, reset all reports to the default values, and reset the overall layout of the reports to the default look.

Global Options

CA ARCserve Backup Dashboard provides a global options toolbar to let you apply specified actions to all reports. These specified actions have a global effect, and are applied to all reports as applicable. For example, if a global option is applicable to a report, then the action is applied to that report. However, if a global option is not applicable to a report, then the action is considered not relevant and has no effect on that report.



Last Number of Days

You can specify to filter the displayed data that is included in all reports based upon the last number of days. The Last Days field contains a drop-down menu with a preset listing of the most commonly used data collection time periods (1, 3, 7, and 30 days) to select from. You can also manually enter a value in this field.

Default: 7 days

Node name

You can specify to filter the displayed data that is included in all reports based upon the name of the node you want to monitor.

The wildcard characters asterisk and question mark are supported in the Node name field. If you do not know the complete node name, you can simplify the results of the filter by specifying a wildcard character in the Node name field.

- "*" - Use the asterisk to substitute zero or more characters in the node name.
- "?" - Use the question mark to substitute a single character in the node name.

The following Dashboard limitations apply to the Node name:

- Dashboard will only distinguish node names by the first 15 characters. If multiple node names are identical for the first 15 characters, Dashboard will not distinguish between them.
- The Node name must be DNS resolvable. If your node cannot be found using DNS, Dashboard will not be able to resolve it or display any related information.
- The Node name cannot contain a parenthesis "(" character. If your node name has this character, Dashboard will not be able to correctly identify the backup information for that node.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Node tier

Specifies the tier category for the nodes you want to monitor. This will be filter all reports based upon the selected node tier that you want to monitor.

The node tiers are configured into three categories, with Tier 1 representing high-priority nodes, Tier 2 representing middle-priority nodes, and Tier 3 representing low-priority tiers. The Node tier field contains a drop-down menu listing each tier category to select from.

For more information, see [Node Tiers](#) (see page 38).

Default: All Tiers

Refresh All

Refreshes all reports to display the most current data.

Reset All

Resets all reports to the applicable parameter default values:

- Last Days field is set to 7 days
- Node name field is set to *
- Node tiers is set to All Tiers

For all applicable reports, the default view is set to the Pie Chart view. If any reports have other parameters, they are set to default values.

Default Layout

Resets the overall layout of the reports to the default look. This option is useful when you are viewing multiple reports inside a Dashboard Group.

Schedule Emails

Specifies the email configuration settings for exporting Dashboard reports.

The email scheduling option lets you create a schedule to send reports via email to specified recipient(s). These report emails are automatically updated, generated, and sent as scheduled. You can customize the schedule of these report emails to be sent at specified days and times, as a recurring task. You can also specify which report(s) is included in the email and who these reports are sent to. The selected reports are embedded within the email.

For more information, see [Configure Email Reports](#) (see page 20).

SRM Probing

Lets you initiate an immediate probe or configure the settings for scheduled probes to collect SRM-related data for the SRM-type reports. The SRM prober is a data-collection utility that when invoked, probes or communicates with all machines in your storage environment. These machines send back an updated response containing all related information to be included in the SRM-type reports.

For more information, see [SRM Prober Settings](#) (see page 29).

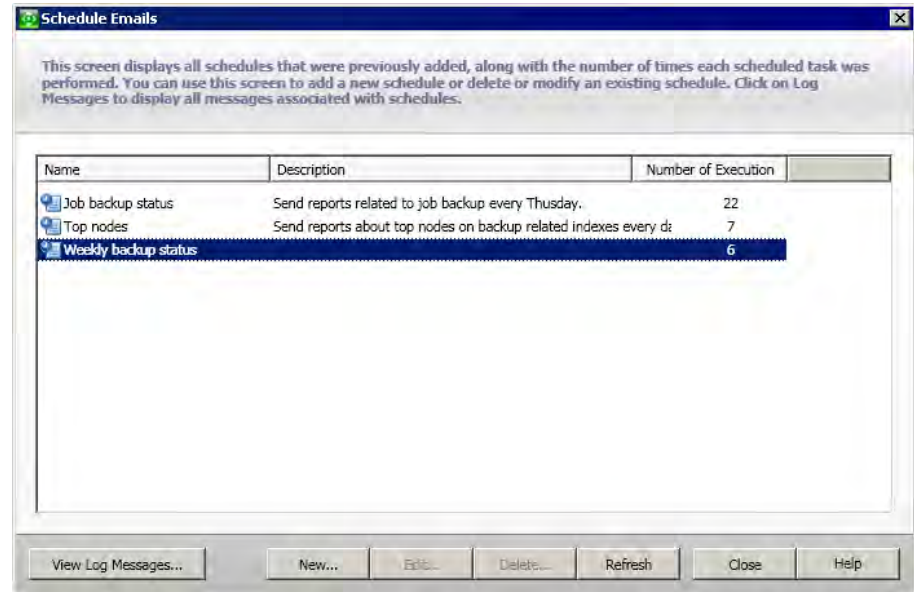
Configure Email Reports

From the global options toolbar, you can select to schedule email settings for all Dashboard reports. The email scheduling option lets you create a schedule to send reports via email to specified recipient(s). These report emails are automatically updated, generated, and sent as scheduled. You can customize the schedule of these report emails to be sent at specified days and times, as a recurring task. You can also specify which report(s) is included in the email and who these reports are sent to. The selected reports are embedded within the email.

Configure an Email Report

1. From the global options toolbar, click the Schedule Email icon.

The Schedule Emails dialog opens.



2. From this dialog, you can either select an existing email schedule name to edit or delete, or add a new email schedule.
 - **New** - Allows you to add a new schedule
 - **Edit** - Allows you to edit an existing schedule
 - **Delete** - Deletes an existing schedule
 - **Refresh** - Displays up-to-date information on the status of each schedule
3. You can also click the Log Messages button to display the Log Message window and check for any log messages of the schedule runs. For more information, see [Tracking Status of Email Schedules](#) (see page 27).

Add a New Email Schedule

The email scheduling option lets you create a new customized schedule to send reports via email to specified recipient(s).

Note: Before any email can be sent out (either from the GUI or scheduled), you must first configure the SMTP setting using the Alert Manager. For more information, see the *Administration Guide* or online help.

Add a new Email Report

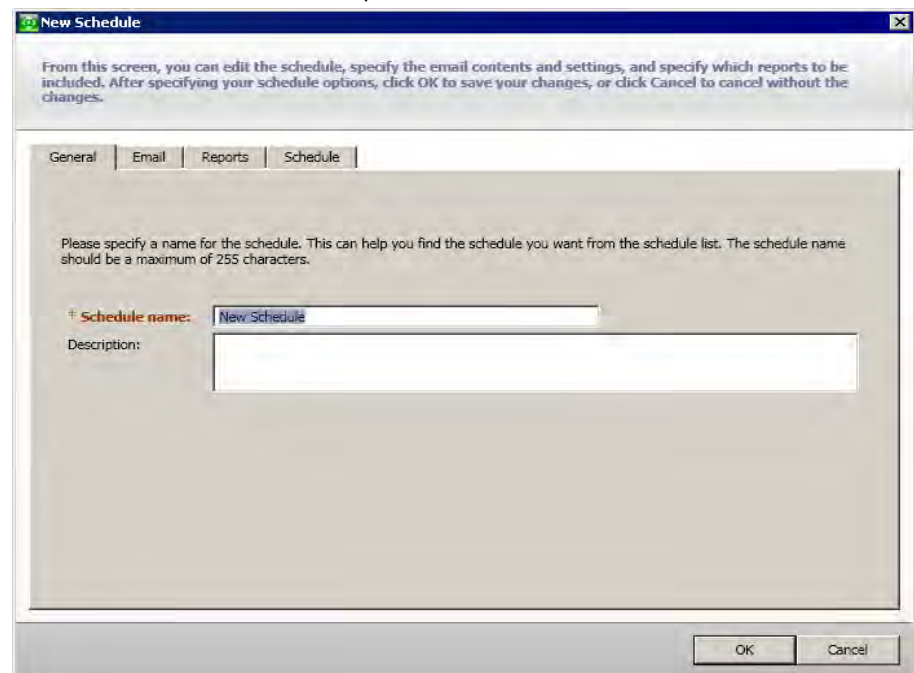
1. From the global options toolbar, click the Schedule Email icon.

The Schedule Emails dialog opens.

2. Click the New button.

The New Schedule dialog opens with the General tab selected.

Note: All fields in red are required fields.

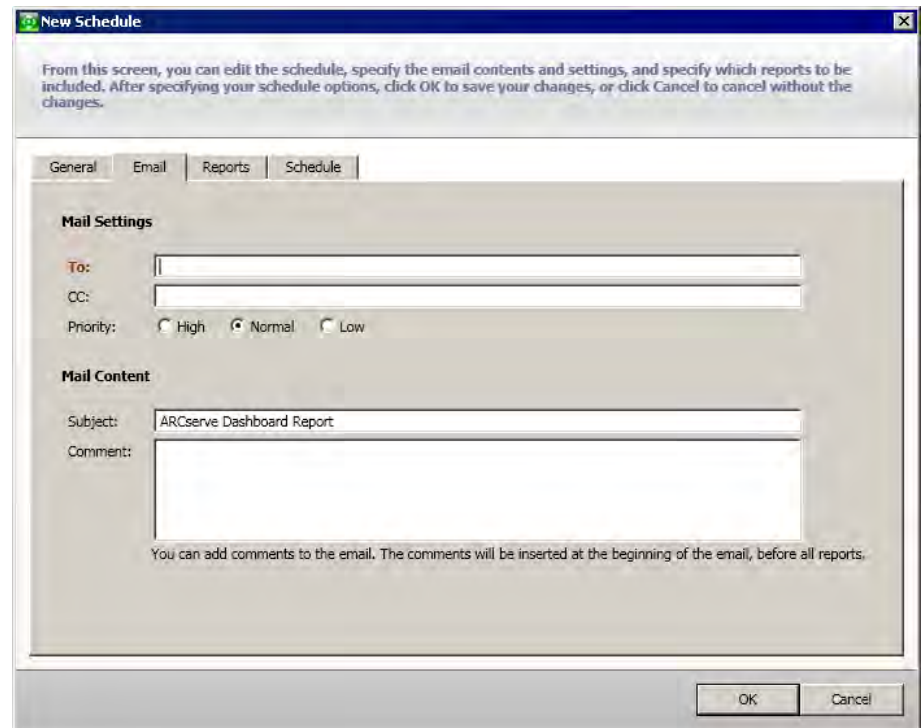


3. Enter a schedule name and a brief description for the new schedule.

The new report name and corresponding description are saved.

- Click the Email tab.

The email settings dialog opens.



The screenshot shows a Windows-style dialog box titled "New Schedule". At the top, a message states: "From this screen, you can edit the schedule, specify the email contents and settings, and specify which reports to be included. After specifying your schedule options, click OK to save your changes, or click Cancel to cancel without the changes." Below this is a tabbed interface with four tabs: "General", "Email", "Reports", and "Schedule". The "Email" tab is currently selected. Under the "Mail Settings" section, there are input fields for "To:" and "CC:", and a "Priority:" section with three radio buttons: "High", "Normal" (which is selected), and "Low". Under the "Mail Content" section, there is a "Subject:" field containing the text "ARCServe Dashboard Report" and a larger "Comment:" text area. At the bottom right of the dialog are "OK" and "Cancel" buttons. A small note at the bottom of the dialog reads: "You can add comments to the email. The comments will be inserted at the beginning of the email, before all reports."

- Enter the email address for each recipient of the scheduled e-mail in the To field. (You can also enter recipient information in the CC field). There must be at least one recipient in the To box.

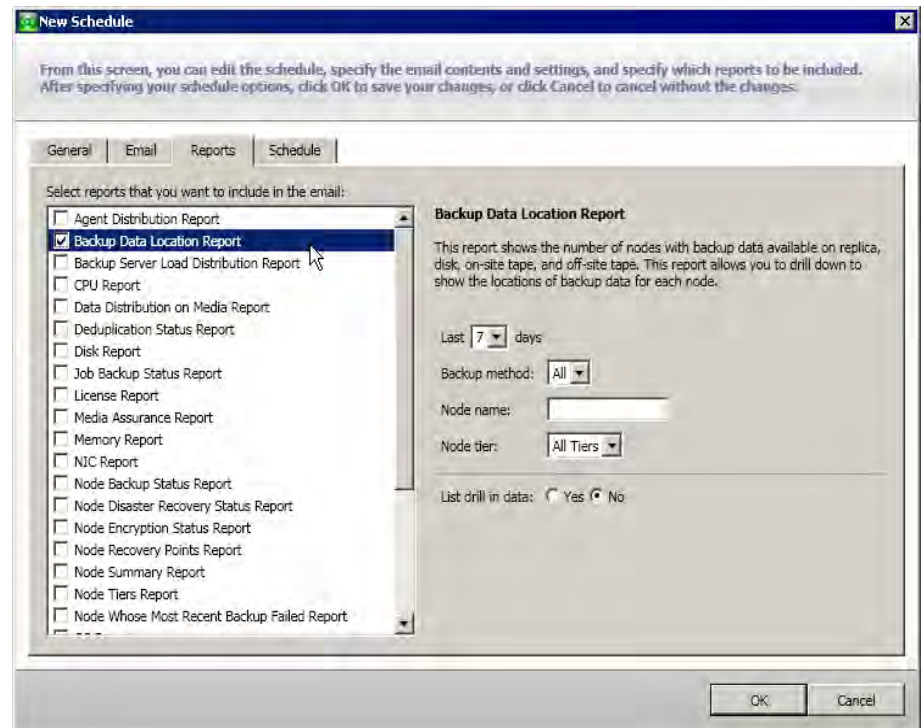
Note: To enter multiple email addresses, each address must be separated by a semi-colon character.

You can also specify the priority of the scheduled email (high, medium, or low), add a comment to be included in the email, and enter the email subject. (If you do not enter a subject, a pop-up confirmation window opens when you click the OK button).

The new report email settings are saved.

- Click the Reports tab.

The reports settings dialog opens.



- Select the report(s) to be included in the email and the parameters for each report.

The Reports tab consists of two parts: the report list and the report parameter collector. From the left pane, you can select which report(s) to be sent by checking the corresponding check box. When you highlight a report name, the right pane displays the corresponding name, description, and parameters of the selected report. From this pane, you can specify the parameters of the report being sent. These parameters are used when generating the report at the scheduled time.

The report settings for the new report are saved.

8. Click the Schedule tab.

The schedule settings dialog opens.

The screenshot shows a 'New Schedule' dialog box with a title bar and a close button. Below the title bar is a descriptive text: 'From this screen, you can edit the schedule, specify the email contents and settings, and specify which reports to be included. After specifying your schedule options, click OK to save your changes, or click Cancel to cancel without the changes.' Below this text are four tabs: 'General', 'Email', 'Reports', and 'Schedule'. The 'Schedule' tab is selected. The dialog is divided into three main sections: 'Repeat Method', 'Scheduled Time', and 'Reoccurrence'. The 'Repeat Method' section has a dropdown menu with 'Every number of days' selected, and a text field 'Every 1 day(s)'. The 'Scheduled Time' section has a 'Time' field set to '8:00' and a label 'Hour : Minute, e.g. 13:00'. The 'Reoccurrence' section has a 'Start from' dropdown set to '11/20/2008', and a 'Repeat Until' section with three radio buttons: 'Forever' (selected), 'End date' (with a date field set to '11/30/2008'), and 'Number of times' (with a text field set to '1'). At the bottom right are 'OK' and 'Cancel' buttons.

9. Select the scheduling parameters for sending the corresponding email.

Scheduling information consists of three parts: Repeat Method, Scheduled Time, and Reoccurrence.

Repeat Method

There are three Repeat Method schedule options from which you can select the days the emails (with the specified reports included).

- **Every several days**

If you select Every several days, you can then select the number of days or interval between emails. If you specify the interval to 1, this means the email is sent every day.

- **Every selected weekdays**

If you select Every selected weekdays, you can then select the day(s) of the week (Monday through Sunday) that the email is sent. You can select multiple days of the week. By default, for a new schedule, the setting is all workdays (Monday through Friday).

- **Some day of every month**

If you select Some day of every month, you can then specify the day number and the direction the day number is counted from. The direction can be counted from beginning or from the end of every month.

Scheduled Time

You can specify the time of the day that the email is sent. The time selections are specified in 24-hour format.

Reoccurrence

You can specify the date when the schedule become active (the date to start the repeat from), and when the repeat schedule terminates. You can select to repeat forever, repeat to an end date, or repeat a specified number of times.

By default, the start date is always the current day (today) and the schedule is repeated forever.

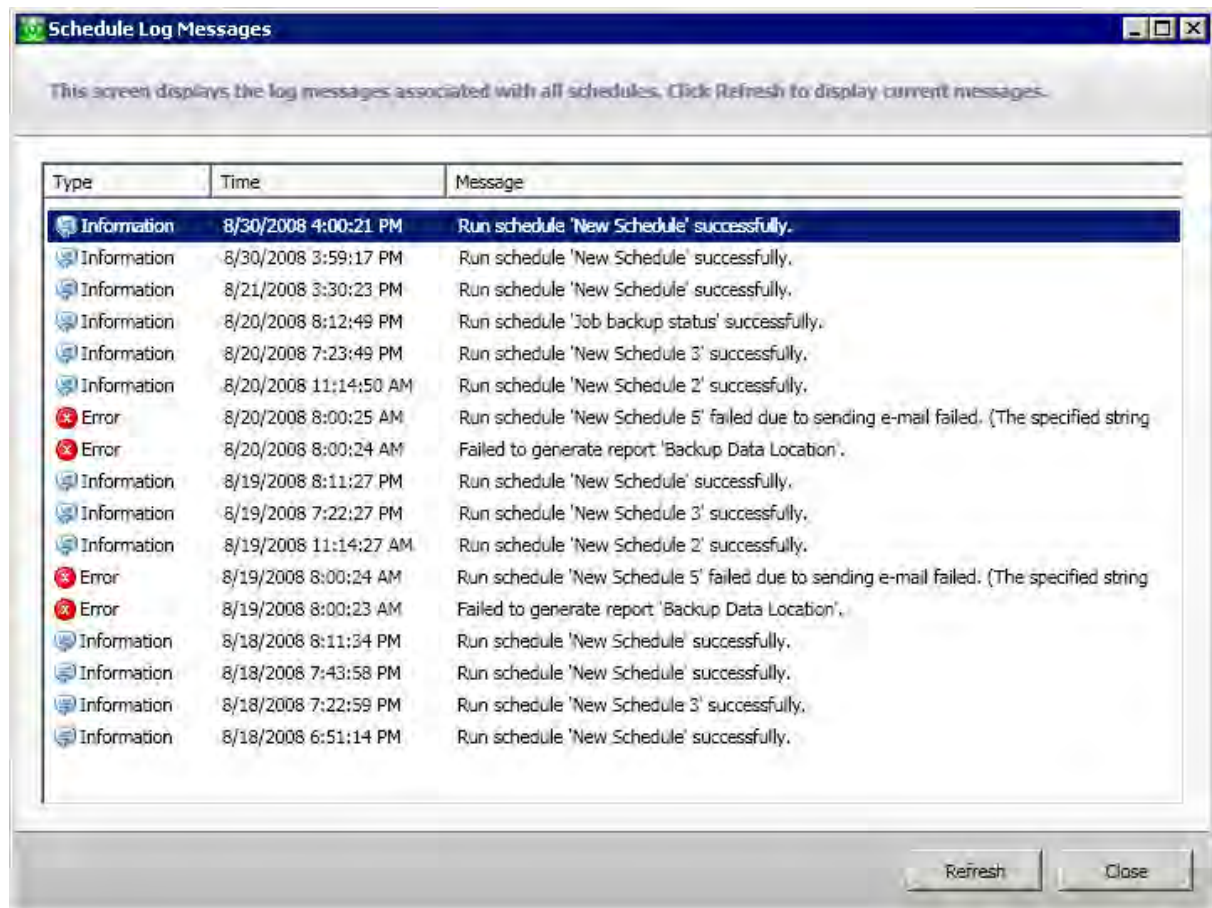
10. Click OK.

The Email configuration settings and Email content are saved.

Tracking Status of Email Schedules

From the Schedule Manager dialog, you can also click the Log Messages button to display the Log Message window and check for any log messages of the schedule runs. This provides you with the status of each schedule, whether it ran successfully or failed, and the possible causes of a failure (if applicable). To read the complete text for long error messages which are truncated, you can hover over the entry to display a tool-tip with the complete message text.

Note: The messages logged for Email Schedules are pruned automatically based on the settings defined for pruning of Activity Log records in the Server Admin (by default, every 14 days). For more information about pruning Activity Logs, see the *Administration Guide* or online help.



Report-Specific Options

The following report-specific options can be individually set to customize each CA ARCserve Backup Dashboard report. Each of these options has a default value, which can also be globally reset for all reports if necessary.

Number of Days

You can specify to filter the displayed list that is included in the report based upon the last number of days. The Last Days field contains a drop-down menu with a preset listing of the most commonly used data collection time periods (1, 3, 7, and 30 days) to select from. You can also manually enter a value in this field.

Default: 7 days

Number of Nodes

You can specify to filter the number of nodes that is included in the report. Depending upon other settings, this field displays the top specified number of nodes for the corresponding category. The Top nodes field contains a drop-down menu with a preset listing of the more commonly used data collection number of nodes (5, 10, 20, 40, 100, 200, and 400) to select from. In addition, you can also manually enter any value in this field.

Default: 5 nodes

Backup Methods

You can specify to filter the displayed list of nodes that is included in the report based upon the backup method that was used for each node. The Backup Method is a drop-down menu and lets you select All, Full, Incremental, or Differential.

Default: All

Server

You can specify to filter the displayed information that is included in the report based upon the corresponding CA ARCserve Backup server. The Server is a drop-down menu and lets you select all CA ARCserve Backup servers or an individual CA ARCserve Backup server (Primary or Member) that is part of the CA ARCserve Backup Domain that you are logged into. (If you are logged in as a Stand-alone server, this list only displays your Stand-alone server).

Default: All Servers

Node tier

Specifies the tier category for the nodes you want to monitor.

The node tiers are configured into three categories, with Tier 1 representing high-priority nodes, Tier 2 representing middle-priority nodes, and Tier 3 representing low-priority tiers. The Node Tier field contains a drop-down menu listing each tier category to select from.

For more information, see [Node Tiers](#) (see page 38).

Default: All Tiers

Severity Filter

You can specify to filter the displayed list of messages that is included in the report based upon the severity of the message. The Severity Filter is a drop-down menu and lets you select All, Information, Errors, Warnings, or Errors and Warnings.

Default: Errors and Warnings

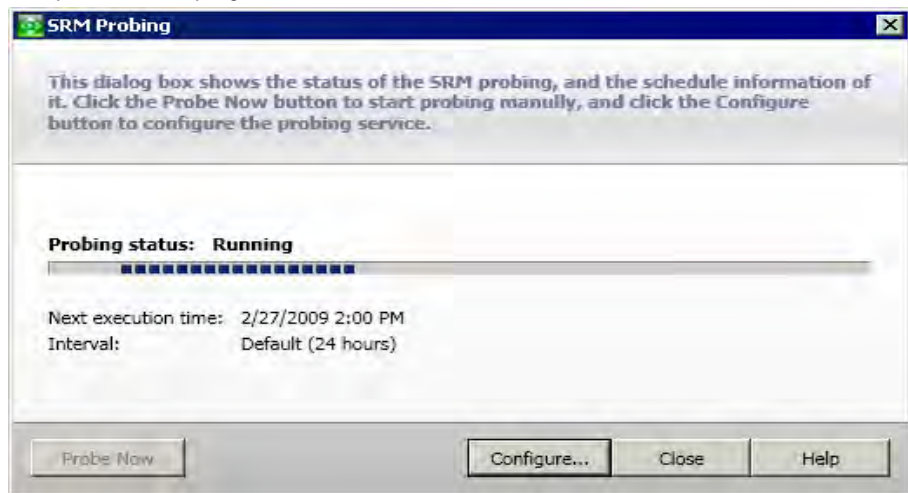
SRM Probe Settings

The SRM probe is a data-collection utility that when invoked, probes or communicates with all machines in your storage environment that have CA ARCserve Backup agents r12.5 running on a supported Microsoft Windows Operating System. These machines send back an updated response containing all related information to be included in the SRM-type reports.

Note: For a list of supported Windows operating systems, see the CA ARCserve Backup readme file

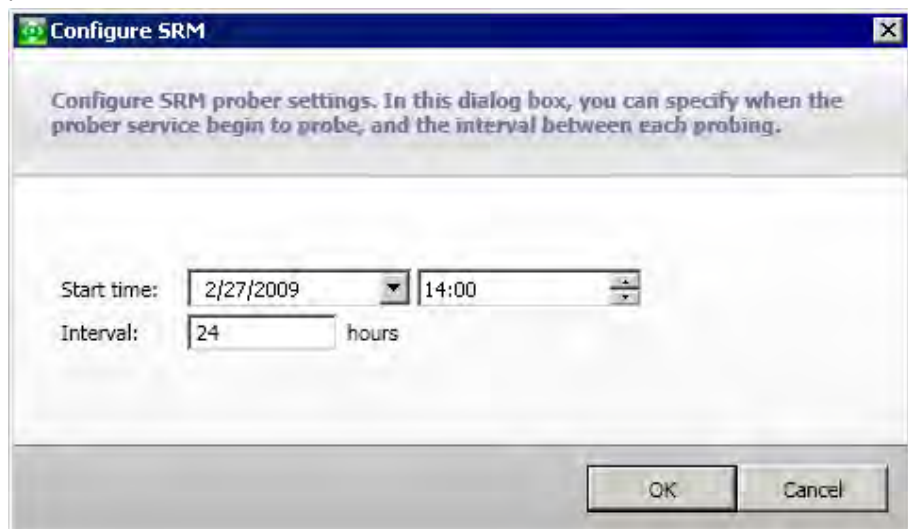
From the global options toolbar, you can click the SRM Probing button to open the SRM Probing dialog. From this dialog you can select to immediately initiate an SRM probe or configure the SRM probe settings to perform this probe at a scheduled time.

- To initiate an immediate probe, click the Probe Now button. The status of the probe is displayed.



- To configure the SRM Probe settings, click the Configure button. The Configure SRM dialog opens.

By default, CA ARCserve Backup Dashboard is scheduled to perform this SRM probe every day at 2:00 PM. From this dialog, you can modify this schedule to change the start date, time, and interval (hours) between probes.



Note: If the SRM probe process is causing a problem (either taking too much time to complete or affecting the use of your system resources), see the Troubleshooting topic [SRM data probe performance problem](#) (see page 143) to enhance this performance to meet your needs.

Chapter 2: Using Dashboard

This section contains the following topics:

[Use CA ARCserve Backup Dashboard](#) (see page 31)

[Dashboard Groups](#) (see page 33)

[Node Tiers](#) (see page 38)

[Node Information](#) (see page 39)

[Agent Upgrade Alert](#) (see page 40)

Use CA ARCserve Backup Dashboard

The CA ARCserve Backup Dashboard is a user interface tool that provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment. This dashboard view lets you quickly and easily monitor relevant information to help you manage the performance and operation of your backup and SRM environment. Dashboard lets you quickly and easily monitor a wide variety of backup environment information and produce exportable reports for each monitored area.

Important! Make sure all CA ARCserve Backup services are up and running prior to using CA ARCserve Backup Dashboard. For more information about starting CA ARCserve Backup services, see the *Administration Guide*.

Note: Dashboard can only be accessed by users having CA ARCserve Backup Administrator, Monitor Operator, and Report Operator assigned user profile roles. For more information about User Profiles, see the *Administration Guide* or online help.

To use CA ARCserve Backup Dashboard

1. You can access the CA ARCserve Backup Dashboard from the Monitor & Reports Menu on the Navigation Bar of the CA ARCserve Backup Manager Console or from the Quick Start menu.



The CA ARCserve Backup Dashboard main screen appears, displaying a snapshot view that provides status reports of the specified CA ARCserve Backup environment.

2. The CA ARCserve Backup Dashboard GUI consists of two report content panes on the left side and a report display window on the right. The two report content panes display a complete list of available All Reports (in alphabetical order) and a list of any of your customized pre-selected Dashboard Groups. The report display window shows the selected report(s).

Note: For more information about each of the displayed reports, see the corresponding report descriptions.

Dashboard Groups

A Dashboard Group is a customized collection of reports that when selected displays the specified reports as a pre-configured grouping. Dashboard Groups let you organize the display of reports based upon your specific needs or preferences. Dashboard Groups help you focus on the status within specific areas of your environment. You can display the reports contained within a Dashboard Group by clicking the group name. In addition, when you hover the mouse cursor over a particular group name, a tool tip box appears under the cursor displaying the name of the group and a list of the reports contained within that group.



CA ARCserve Backup Dashboard lets you create, modify, and delete Dashboard Groups. When you add a new group, the created group is accessible for use only by that user. If you create a new group, it is not visible to other users. For example, if user A creates a group, user B will not see that group.

CA ARCserve Backup Dashboard contains several pre-configured default groups, which if necessary can be modified, but not deleted. In addition to the default groups, you can also create your own customized Dashboard Groups, selecting the individual reports that are displayed in the group. Each Dashboard Group must contain at least one report and a maximum of four reports.

The pre-configured default groups are as follows:

Backup Status Dashboard Group

Contains the following reports: Node Backup Status Report, Job Backup Status Report, Top Nodes with Failed Backups Report, and Nodes Whose Most Recent Backup Failed Report.

Encryption Dashboard Group

Contains the following reports: Node Encryption Status Report and Tape Encryption Status Report.

Recovery Point Dashboard Group

Contains the following reports: Node Recovery Points Report, Virtual Machine Recovery Points Report, Recovery Point Objective Report, and Media Assurance Report.

Virtualization Dashboard Group

Contains the following reports: Virtual Machine Recovery Points Report and Virtualization Most Recent Backup Status Report.

Deduplication Dashboard Group

Contains the following reports: Deduplication Status Report and Data Distribution on Media Report.

Client Node Hardware Information Dashboard Group

Contains the following reports: NIC Report, CPU Report, Memory Report, and SCSI/Fiber Card Report.

Client Node Storage Information Dashboard Group

Contains the following reports: Volume Report and Disk Report.

Client Node Software Information Dashboard Group

Contains the following reports: Node Tiers Report, Agent Distribution Report, Node Summary Report, and License Report.

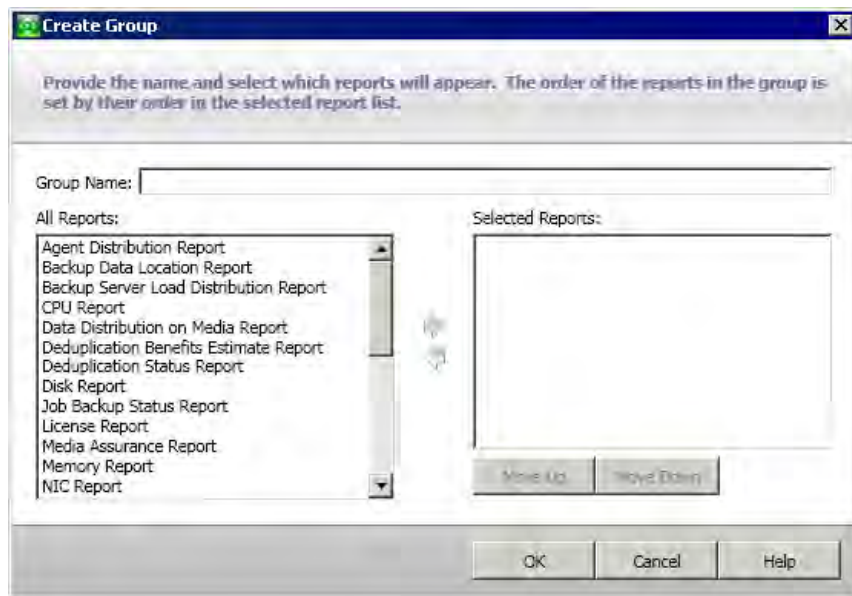
Add a Dashboard Group

CA ARCserve Backup Dashboard lets you add new Dashboard Groups that display your customized grouping of reports when selected. A Dashboard Group must contain at least one report and a maximum of four reports.

Add a Dashboard Group

1. From the Dashboard Groups pane, click the Add button.

The Create Group dialog opens, displaying a listing of all available reports.



2. Enter a Group Name for the group being created.
Note: You cannot have two groups with the same name.
3. From the All Reports box, select the report(s) to be included in the new group and click the right arrow icon.

The reports are added to the Selected Reports box. A Dashboard Group must contain at least one report.

Note: Multiple reports can be selected for a group by using the "CTRL" or "SHIFT" key combinations.

4. The order that the reports are displayed in the Dashboard window is determined by the order that they are listed in the Selected Reports box. If necessary, you can customize the order that the reports are displayed by using the Move Up or Move Down buttons.

The first report listed is displayed in the top left position, the second is in the top right, the third is the bottom row left, and the fourth is the bottom row right.

5. Click OK to save the changes.

The name of the new group appears on the Dashboard Groups list and can be selected.

Modify a Dashboard Group

CA ARCserve Backup Dashboard lets you modify an existing Dashboard Groups to change the display of your customized grouping of reports when selected.

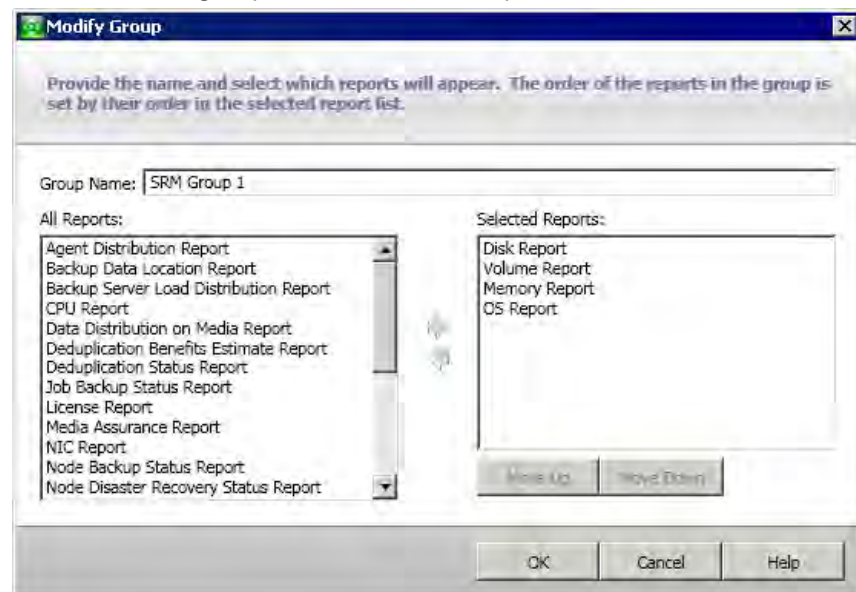
Modify a Dashboard Group

1. From the Dashboard Groups pane, select an existing group that you want to modify.

The Modify button becomes enabled.

2. Click the Modify button.

The Modify Group dialog opens, displaying a listing of the reports included in the selected group and all available reports.



3. Use the left and right arrow icons to add or remove reports from the Selected Reports box.

The reports are added to or removed from the Selected Reports box.

Note: A Dashboard Group must contain at least one report.

You can also modify the group name or the order that the reports are displayed.

The first report listed is displayed in the top left position, the second is in the top right, the third is the next row left, the fourth is the next row right, and so on.

4. Click OK to save the changes.

The modified group appears in the Dashboard Groups list and can be selected.

Delete a Dashboard Group

CA ARCserve Backup Dashboard lets you delete an existing Dashboard Group. You can delete any modifiable group; however, built-in default groups cannot be deleted.

Delete a Dashboard Group

1. From the Dashboard Groups pane, select an existing group that you want to delete.

The Delete button becomes enabled.

2. Click the Delete button.

A confirmation dialog appears asking you if you are sure you want to delete this group.

3. Click OK to delete the Dashboard Group (or Cancel to stop the process).

The selected group name is deleted from the Dashboard Groups list.

Node Tiers

You can use the CA ARCserve Backup Server Admin to change the assigned priority classifications of your CA ARCserve Backup the nodes. The priority classifications are divided into three tier groupings (Tier 1, Tier 2, and Tier 3), with Tier 1 representing the high-priority (business-critical) nodes and Tier 3 representing low-priority nodes. These tiers are used to filter the information displayed on the CA ARCserve Backup Dashboard by the priority level of the monitored nodes.

The Node Tier Configuration dialog contains three priority categories, and is automatically populated when a node is added to your system and browsed. By default, Tier 1 is configured to include all CA ARCserve Backup servers (Primary and Member) and any nodes with CA ARCserve Backup application agents installed (such as Oracle, Microsoft Exchange, Microsoft SQL Server, Microsoft Sharepoint, and so on), and Tier 3 is configured to include all other nodes (having file system agents installed). Tier 2 is not configured to include any nodes, and is available for customized use.

The node assignments for each tier can be reconfigured and customized to meet your individual needs by using the Node Tier Configuration dialog, which is accessed from the CA ARCserve Backup Server Admin or from the Backup Manager (right click 'Windows systems' in Source tab).

Notes:

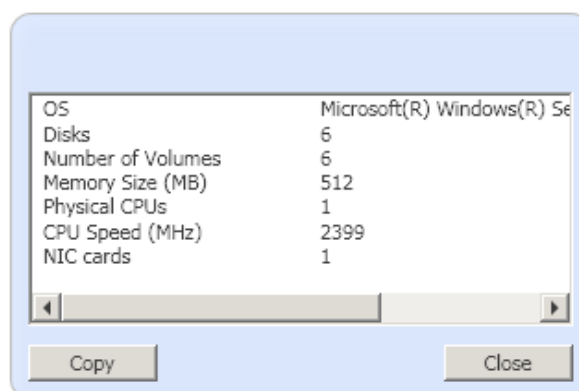
- For more information about Node Tier Configuration, see the *Administration Guide* or the online help.
- For more information about monitoring node tiers, see [Node Tiers Report](#) (see page 103).

Node Information

All Dashboard reports that include a listing of node names also have the added capability to quickly and easily display summary information about each node. When you select a node name and right-click the mouse button, a pop-up window appears with related node information.

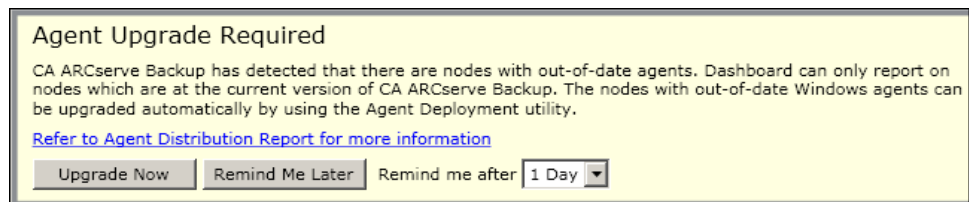
From this pop-up window, you can also click the Copy button to copy the node information content to a holding queue where it can then be pasted into an email or any other text editor such as MS Word, Notepad, etc.

Note: If your backup environment contains Unix/Linux/Mac agents at version r12.5, this window will not display any information for such nodes because SRM information collection is not supported for non-windows nodes.



Agent Upgrade Alert

When you access Dashboard, CA ARCserve Backup Dashboard probes your backup environment to detect if any installed CA ARCserve Backup agents are at a version prior to r12.5. Dashboard can only monitor and report on nodes that have CA ARCserve Backup agents with r12.5 or later. If it detects out-of-date agents, an Agent Upgrade Required alert is displayed, indicating that nodes within your backup environment that have CA ARCserve Backup agents prior to r12.5. This alert also lets you quickly and easily upgrade your out-of-date Windows agents now, request to be reminded after a specified time period has elapsed, or be reminded later.



If you select to be reminded at a later time, the Agent Upgrade Required alert disappears and is replaced by a small reminder window to inform you that Dashboard will not provide report information for any out-of-date agents.

CA ARCserve Backup has detected agents prior to r12.5. Dashboard will not report on any agents prior to r12.5. [Click here for more information about upgrading these agents.](#)

Note: If you have not installed the Agent Deployment package during your CA ARCserve Backup primary server installation, you can upgrade your out-of-date agents by clicking Upgrade Now button in the Agent Upgrade Required alert window and specifying the path of the Agent Deployment package on your CA ARCserve Backup installation media. For more information about the Agent Deployment package, see the *Implementation Guide*.

It is important to maintain your entire backup environment at the most current version to ensure your valuable data is being properly protected and to take full advantage of the latest features and technology being offered by CA ARCserve Backup.

Chapter 3: Dashboard Reports

This section contains the following topics:

[CA ARCserve Backup Dashboard Report Types](#) (see page 41)
[Agent Distribution Report](#) (see page 44)
[Backup Data Location Report](#) (see page 48)
[Backup Server Load Distribution Report](#) (see page 51)
[CPU Report](#) (see page 54)
[Data Distribution on Media Report](#) (see page 57)
[Deduplication Benefits Estimate Report](#) (see page 60)
[Deduplication Status Report](#) (see page 62)
[Disk Report](#) (see page 65)
[Job Backup Status Report](#) (see page 68)
[License Report](#) (see page 73)
[Media Assurance Report](#) (see page 75)
[Memory Report](#) (see page 78)
[NIC Report](#) (see page 81)
[Node Backup Status Report](#) (see page 84)
[Node Disaster Recovery Status Report](#) (see page 89)
[Node Encryption Status Report](#) (see page 94)
[Node Recovery Points Report](#) (see page 98)
[Node Summary Report](#) (see page 101)
[Node Tiers Report](#) (see page 103)
[Node Whose Most Recent Backup Failed Report](#) (see page 106)
[OS Report](#) (see page 109)
[Recovery Point Objective Report](#) (see page 111)
[SCSI/Fiber Card Report](#) (see page 115)
[Tape Encryption Status Report](#) (see page 118)
[Top Nodes with Failed Backups Report](#) (see page 122)
[Top Nodes with Fastest/Slowest Backup Throughputs Report](#) (see page 125)
[Virtual Machine Recovery Points Report](#) (see page 127)
[Virtualization Most Recent Backup Status Report](#) (see page 130)
[Volume Report](#) (see page 133)

CA ARCserve Backup Dashboard Report Types

The CA ARCserve Backup Dashboard reports are basically categorized into two types of reports; Backup Environment Reports and Storage Resource Management (SRM) Reports. In addition, some of the reports have an enhanced capability to drill down into the report to display more detailed information.

Backup Environment Type Reports

The backup environment reports provide you with a snapshot overview of your backup infrastructure. These reports let you quickly and easily monitor relevant information to help you manage the performance and operation of your backup environment. The backup environment reports provide information such as: overall status of the specified CA ARCserve Backup domain, servers, nodes, and/or jobs; media having encrypted/unencrypted sessions; status of your virtualized environments; deduplication benefits. In addition, these backup environment reports also provide the added capability to drill down into any specific area of the environment to get a more focused view of the status of each area.

It is important to evaluate these reports in tandem with each other to compare results and get a better overall picture of what is occurring in your backup environment.

Note: For backup environment reports, if you are accessing Dashboard for the first time and no backup data is displayed, you may need to wait until your first backup job has been performed before data is collected and displayed.

SRM Type Reports

The Storage Resource Management (SRM) reports let you easily monitor your entire storage environment at a glance and measure the status of all related resources. The SRM reports let you perform performance analysis, real-time reporting, and evaluate trended behaviors of all the Windows nodes in your storage environment. By understanding your storage environment and the behavior of the individual storage components, you can to quickly find any potential bottlenecks and prevent interruption of service.

The SRM reports provide system information related to nodes in your backup infrastructure such as: amount of used and available storage space, amount of memory, version of operating systems, network interface cards installed along with their speed, processor architecture and speed, what nodes are accessing shared storage or external media through SCSI or Fiber Cards. In addition, the SRM reports also provide the added capability to drill down into any specific area of the environment to get a more focused view of the status of each area.

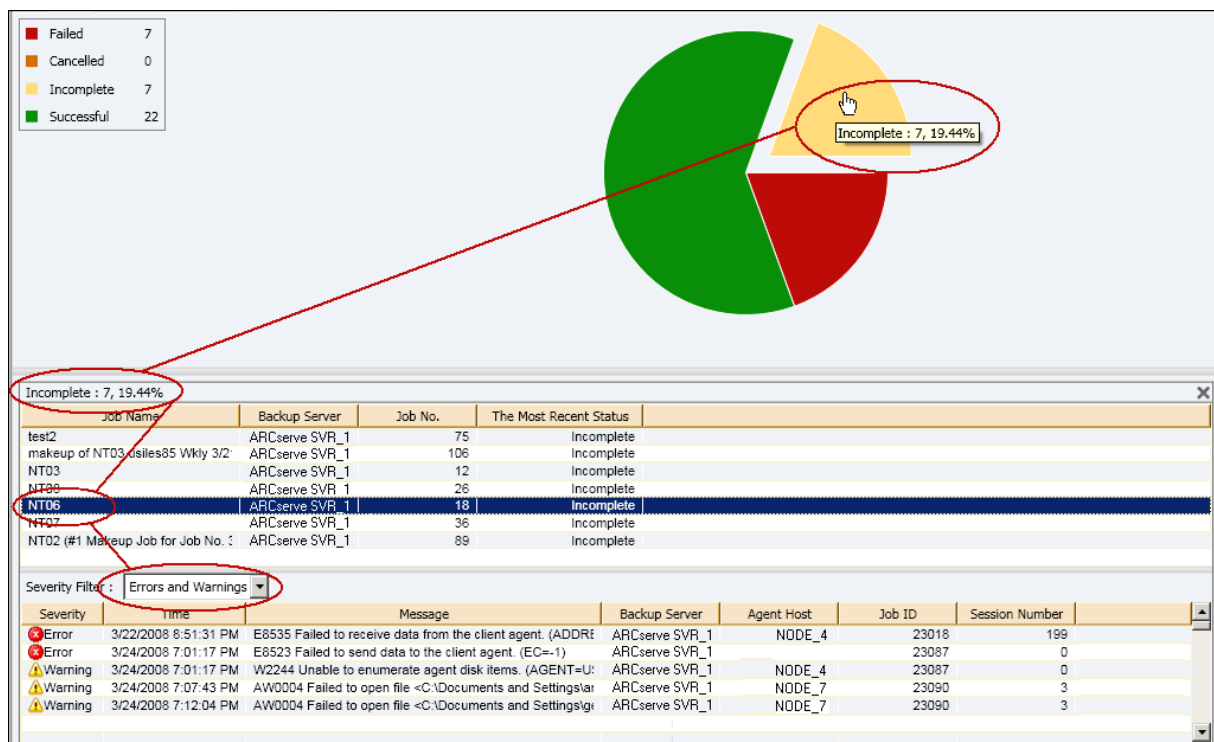
It is important to evaluate these SRM reports in tandem with each other to compare results and get a better overall picture of what is occurring in your storage environment.

Note: For SRM reports, if you are accessing Dashboard for the first time and no SRM data is displayed, you may need to wait until your first SRM probe has been performed before data is collected and displayed. By default, this SRM probe and data refresh occurs at 2 PM every day. However, if you want to immediately display SRM information, you can initiate an immediate probe by clicking on the Probe Now button on the SRM Probing dialog. For more information, see [SRM Probing Settings](#) (see page 29).

Drill Down Reports

Some of the reports have an enhanced capability to drill down into the report to display more detailed information. For these reports, you can click on any of the status categories to drill down from a display of summary information to a more focused and detailed report view about that particular category.

In addition, some reports also let you drill down further by clicking on the name of an individual job or node to display a more detailed listing of all log messages associated with that selected job or node.



Agent Distribution Report

The Agent Distribution Report displays the version of all CA ARCserve Backup agents that are installed on each node. Dashboard only supports CA ARCserve Backup r12.5 and its related agents. To fully utilize Dashboard and take advantage of its features, all agents must also be at the r12.5 version. If an agent is not at the r12.5 version, the corresponding data for that node is not displayed on any of the associated Dashboard reports. A drop-down menu is provided to let you filter the display by the selected type agent. You can specify to include all agents or an individual agent. The drop-down menu includes all "active" agents, which means any agent that has been previously backed up using CA ARCserve Backup.

This report can be used to quickly determine the version status of your CA ARCserve Backup agents and identify which agents need to be upgraded.

Report Benefits

The Agent Distribution Report is helpful in analyzing and determining which version of the CA ARCserve Backup agents are installed on each node. Dashboard only supports CA ARCserve Backup r12.5 and its associated agents.

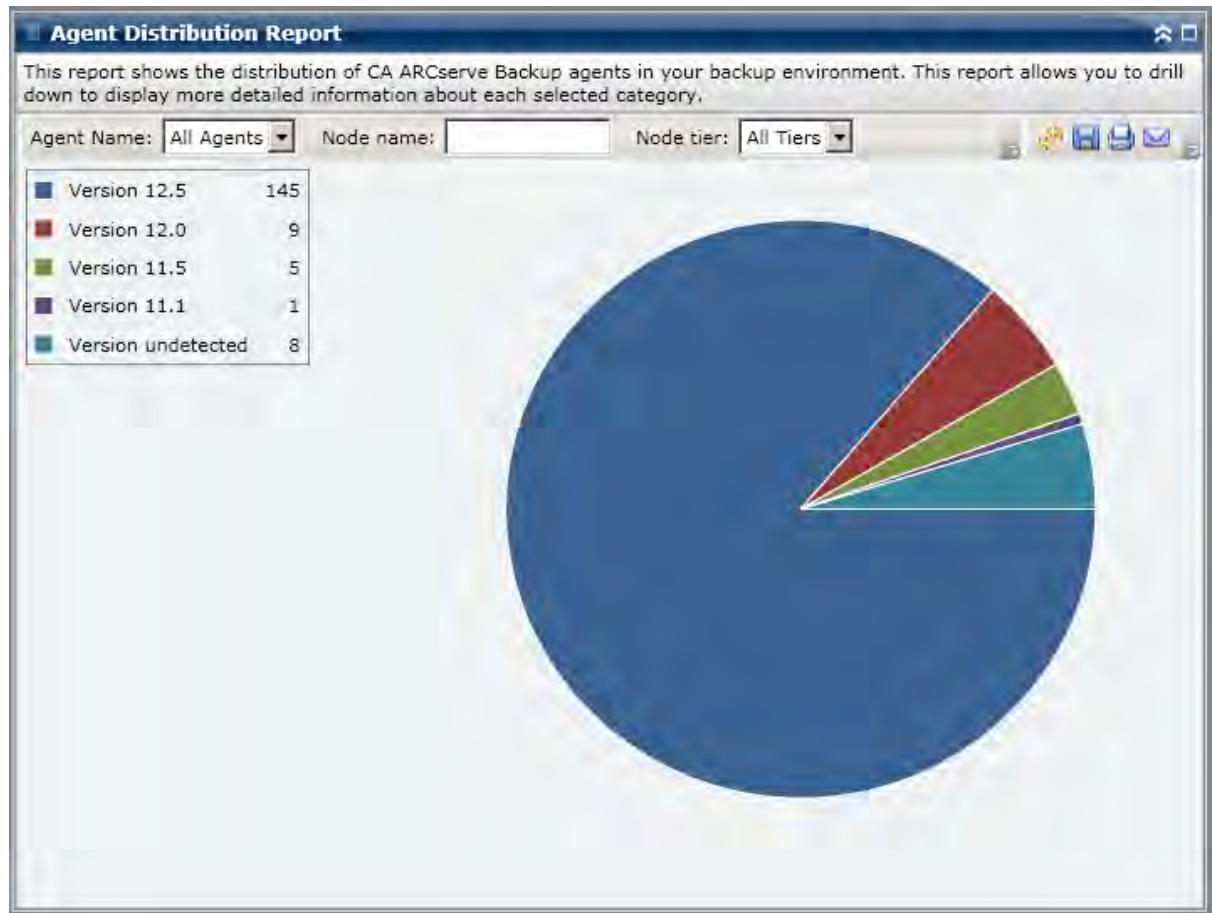
If you find that not all your backup data is being displayed on the various Dashboard reports, you can use this report to determine if some or all of your CA ARCserve Backup agents have not been updated to the r12.5 version. To take full advantage of the latest features offered by the CA ARCserve Backup agents, as well as by Dashboard, you should always maintain the most up-to-date version of these products.

To upgrade to the latest version of your CA ARCserve Backup agents:

- Contact Technical Support at <http://ca.com/support> for online technical assistance and a complete list of locations, primary service hours, and telephone numbers or you can use the Agent Deployment tool in the Administration Section of the Navigation bar of CA ARCserve Backup. ,
- Use the Agent Deployment tool, which is available from the Administration section of CA ARCserve Backup.

Report View

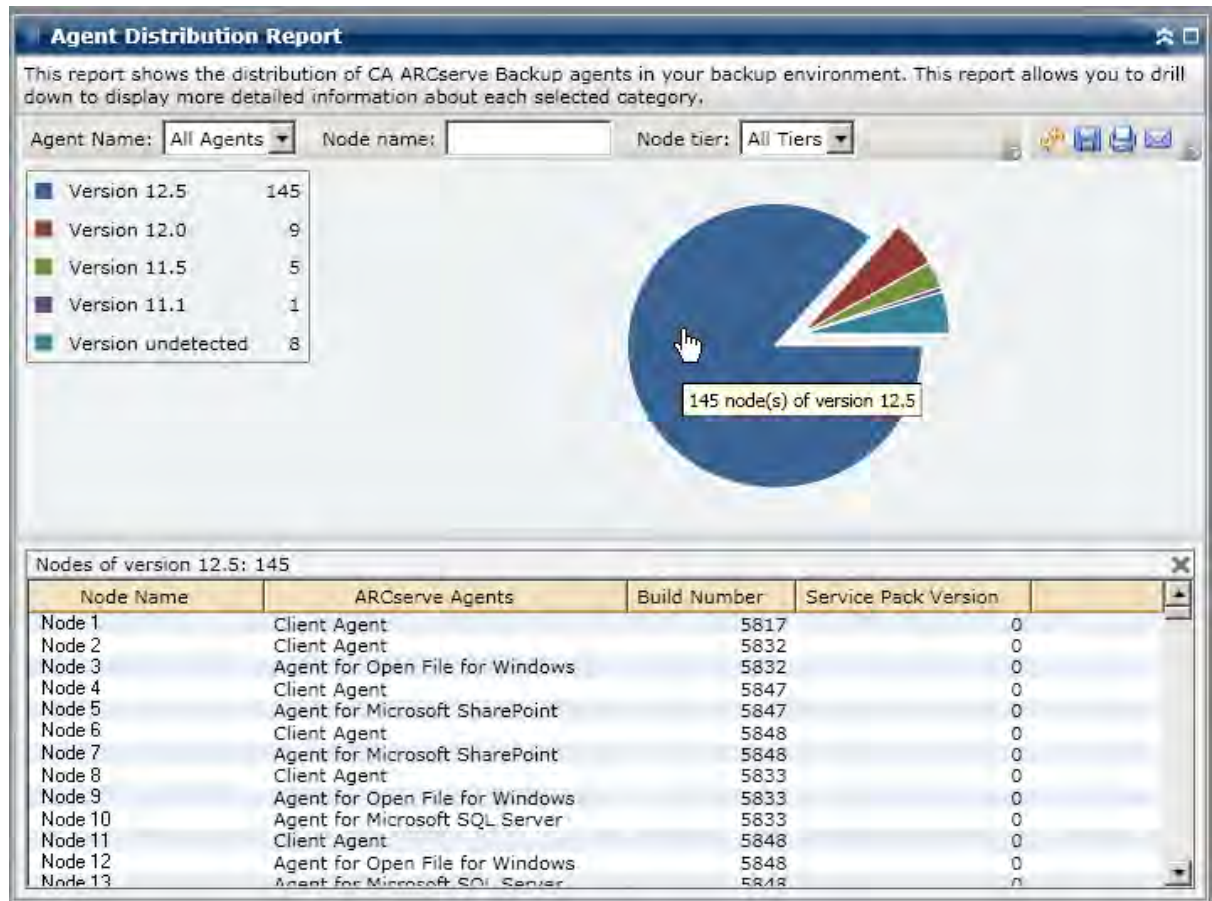
The Agent Distribution Report is displayed in a pie chart format, showing the version distribution of the selected agent name.



Drill Down Reports

The Agent Distribution Report can be further expanded to display more detailed information. You can click the pie chart to get details of agent information as a table.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



The Agent Distribution Report will only display the Service Pack (SP) version of nodes that have CA ARCserve Backup agents at r12 or later release. For the earlier releases, the SP information can be identified from the "Build" column in the report by using the following table to convert the build number to the corresponding SP number.

Note: For more information contact CA support at <http://ca.com/support>

Release	Starting Build Number	GA	SP1	SP2	SP3	SP4
r11.5	3884	X				
	4144		X			
	4232			X		
	4402				X	
	4490					X
r11.1	3060	X				
	3100		X			
	3200			X		
r11	2670	X				
r9.0.1	2020	X				
	2100		X			
	2200			X		
r 9.0	1868	X				
Note: GA indicates the General Availability (or initial) release of this version.						

Backup Data Location Report

The Backup Data Location Report displays the number of nodes and the location of the backed up data for those nodes. This report can be used to evaluate how well your backup infrastructure and plan is protecting your data. In addition, this report also lets you select the quickest and most efficient means to recover this data if necessary. From this report, you can analyze the various locations of your protected data at four possible recovery location categories (Replicated, Disk, Tape Onsite, and Tape Offsite) and help you determine the most efficient means to recover the backed up data from.

Replicated

Nodes that were replicated by CA XOssoft and backed up by CA ARCserve Backup as XOssoft scenarios.

Disk

Nodes that were backed up to disk (including FSD, VTL devices, and deduplication devices).

On-Site:

Nodes that were backed up to tape and the tape is located on-site.

Off-Site:

Nodes that were backed up to tape and the tape is located off-site.

Report Benefits

The Backup Data Location Report is helpful in analyzing and determining the effectiveness of your protected data environment. From this report you can get a snapshot view of your overall backup infrastructure and determine if your data is well-protected.

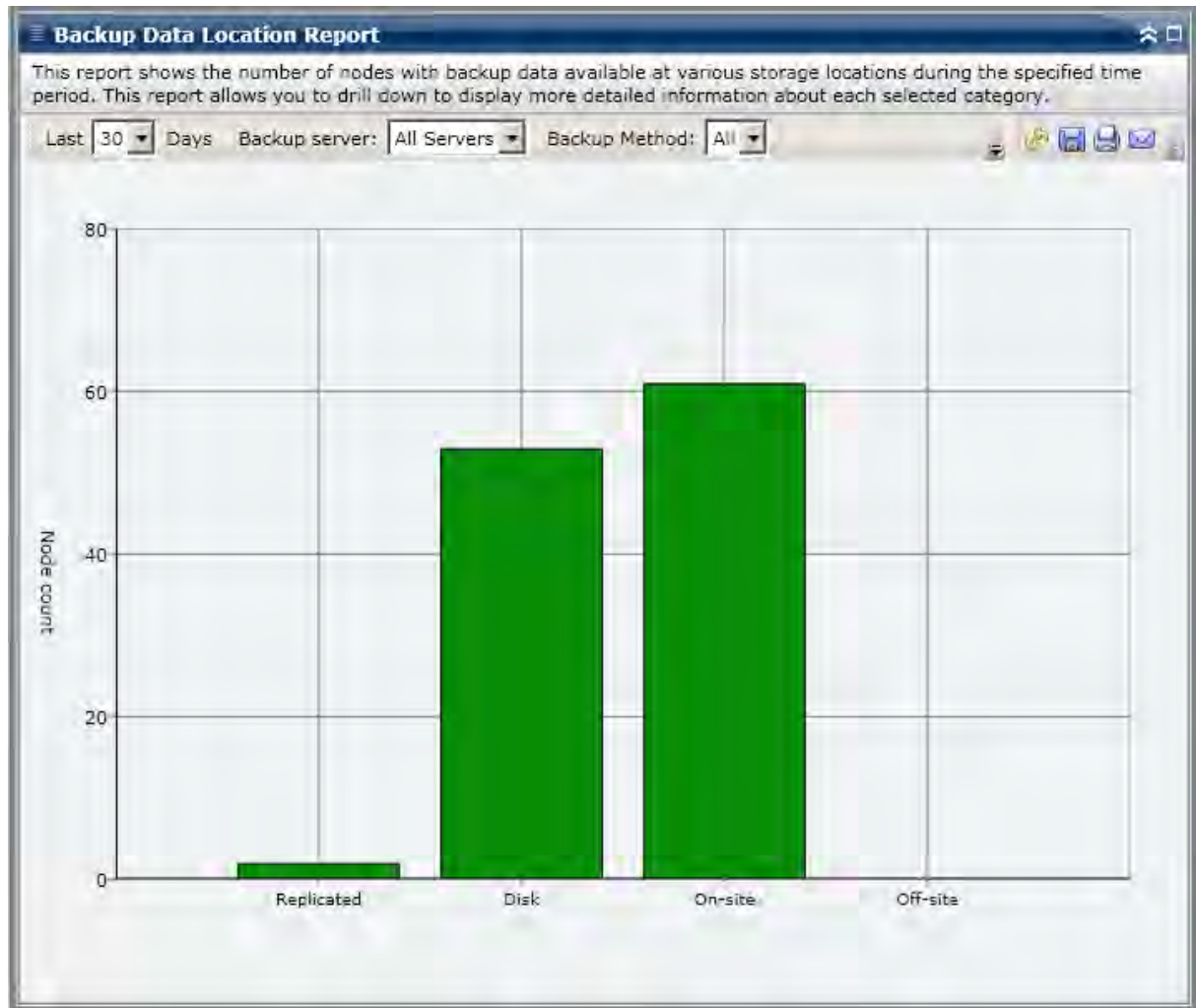
For example, if from this report you see that most of your protected data is located on an onsite tape, but not also located on an offsite tape, then you should modify your backup plan because your data is not well-protected in the event of a local disaster.

In addition, this report can also be helpful to determine the most efficient means to recover the backed up data from if necessary.

For example, if from this report you see that the data that you want to recover was backed up on onsite tape or disk and also on offsite tape, it is generally quicker to recover from the local tape or disk instead of from the remote location. As a result, you would select the onsite tape source or disk for the data recovery if necessary.

Report View

The Backup Data Location Report is displayed in a bar chart format, showing the number of nodes with backup data at various recovery locations.

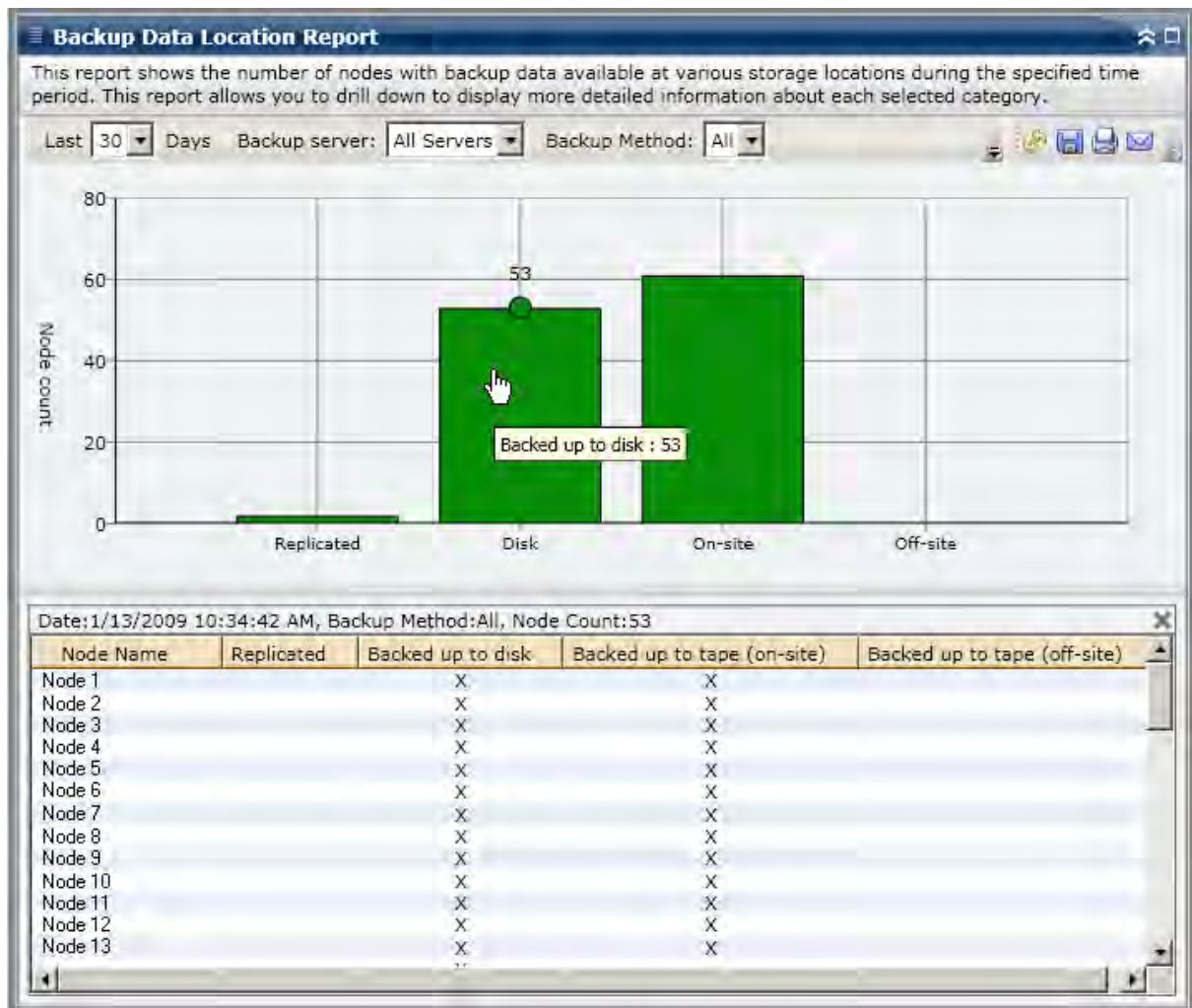


Drill Down Reports

The Backup Data Location Report can be further expanded to display more detailed information. You can click on any of the status categories to drill down from a display of summary information to a more focused and detailed report about that particular category.

For example, if you click on the Tape Onsite category, the report summary changes to display a filtered list of all nodes that were backed up to an *onsite tape* during the last specified time period. The report also displays any other location categories for the same backed up nodes to help you determine the best location to recover the data from if necessary.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



Backup Server Load Distribution Report

The Backup Server Load Distribution Report lists the load distribution of data on each CA ARCserve Backup server during the last specified number of days.

Report Benefits

The Backup Server Load Distribution Report is helpful in analyzing and determining which CA ARCserve Backup servers are more utilized than others for backed up data, and which ones could be better utilized. From this report you can get a snapshot view of which servers are performing the bulk of the backup work, and help you to determine what can be done to better balance the load, if necessary.

Report View

The Backup Server Load Distribution Report can be displayed as either a pie chart or as a bar chart.

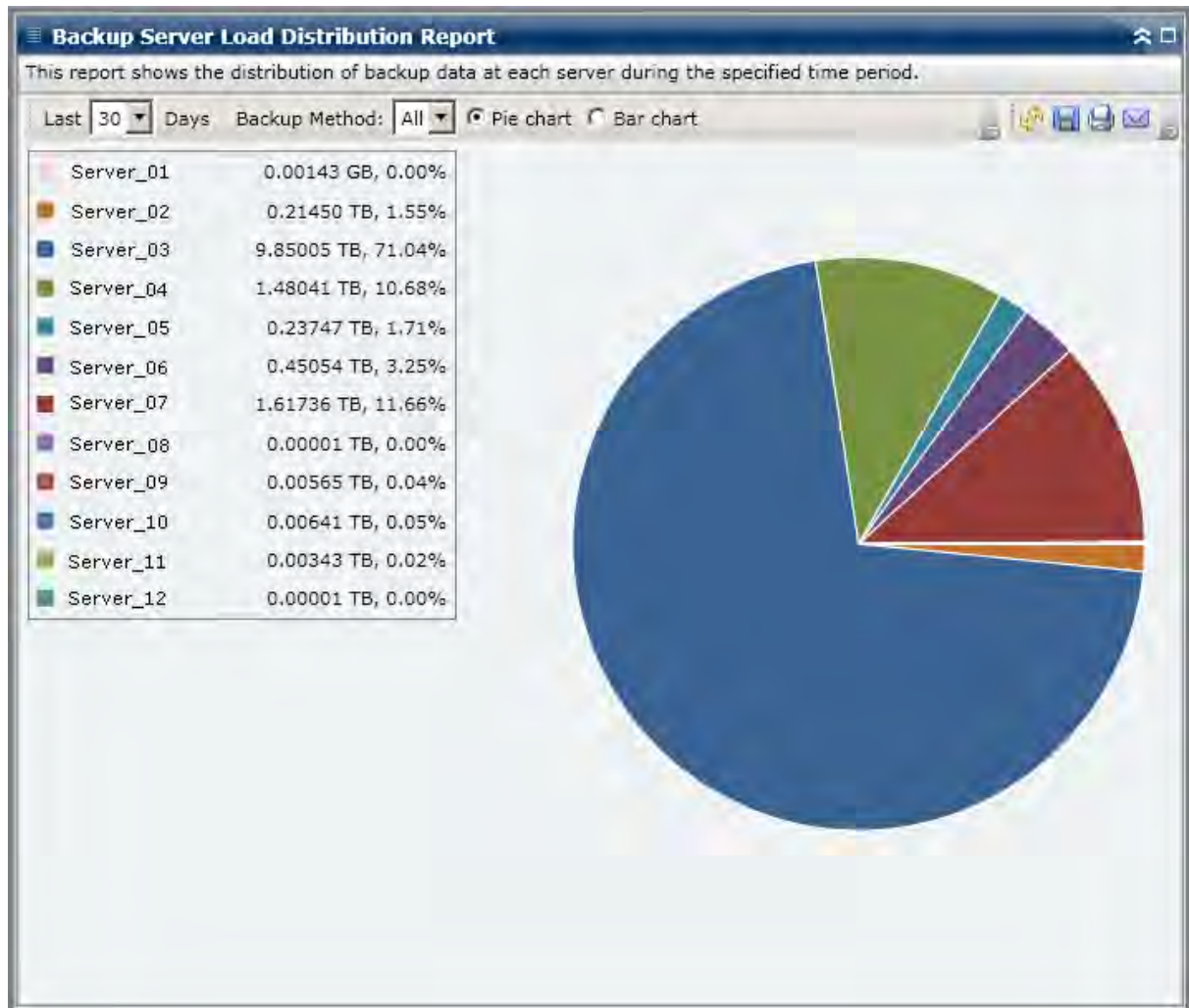
Note: If a media is reformatted, the amount of reported data in the Backup Server Load Distribution Report does not count data from any old reformatted media.

For example, if you perform 1GB backups for seven days, the report displays a load distribution for 7GB of data. However, if you reformat the oldest media and refresh the report, the report now displays a load distribution for only 6GB of data.

Pie Chart

The pie chart provides a high-level overview of how the backed up data is distributed between the CA ARCserve Backup servers for all days during the last specified number of days. The status categories shown in the pie chart represent a percentage of the total backup data distribution for those servers.

Pie chart view displays data distribution for the specified number of days for each server in TeraBytes (TB).

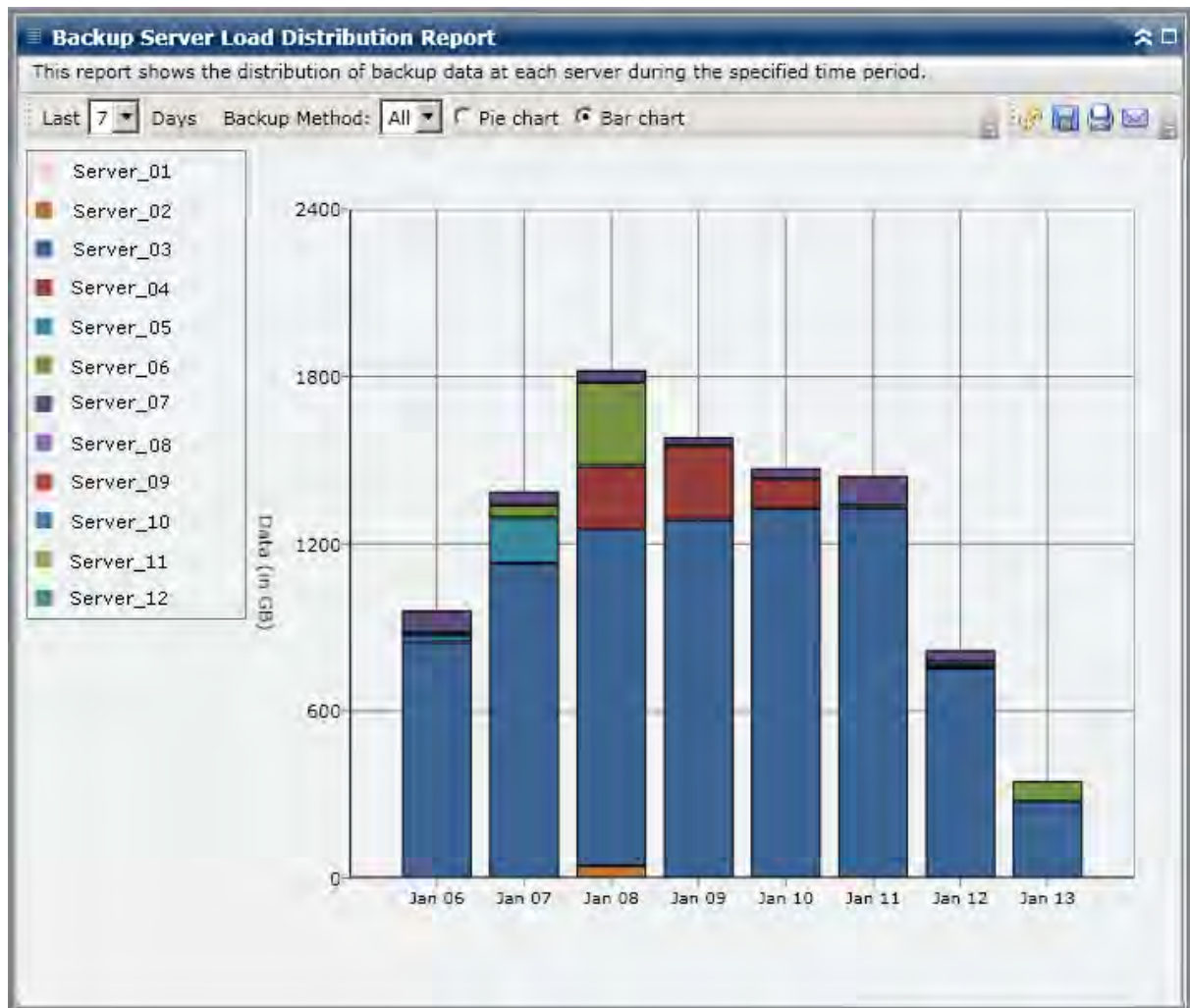


Bar Chart

The bar chart provides a detailed level view of how the backed up data is distributed between CA ARCserve Backup servers for each day during the last specified number of days. The status categories shown in the bar chart represent the daily backup data distribution for those servers.

Bar chart view displays data distribution for the specified number of days for each server in GigaBytes (GB).

Note: By default, CA ARCserve Backup Dashboard only displays bar chart information for a maximum of 90 days. Increasing the number of displayed days to more than 90 days would result in the bar chart information not being legible. If you specify to display report information for more than 90 days, the bar chart limits the display to only 90 days, regardless of the number of days entered. This limitation does not apply to pie chart views of the same report. (The maximum number of displayed days for a pie chart is 999 days).



CPU Report

The CPU Report is an SRM-type report that displays the number of Windows nodes within your CA ARCserve Backup Domain, organized by different central processing unit (CPU) properties. You can filter this report to display which selected CPU property you want to classify the nodes by.

Report Benefits

The CPU Report is helpful in quickly classifying machines based on the amount of CPU's, the manufacturer of the CPU, or the architecture of the CPU (32-bit versus 64-bit). You can get an overall view to analyze and determine which CPUs are more effective than others for backup jobs, and which ones could be potential problem areas.

For example, if you identify a node having a slower throughput value, you can monitor the CPU speed of that node through this report. You can look for patterns in behavior among the slower CPUs or among the same manufacturer. A 32-bit CPU node may have a slower throughput compared to a 64-bit CPU node.

You can also use the fastest throughput values as reference points to analyze why these CPUs are performing well. You can compare the slower CPUs to the faster CPUs to determine if you actually have a problem or if both sets of values are similar, maybe the slower CPUs are not performing poorly.

This report helps you determine if you need to upgrade your CPU hardware.

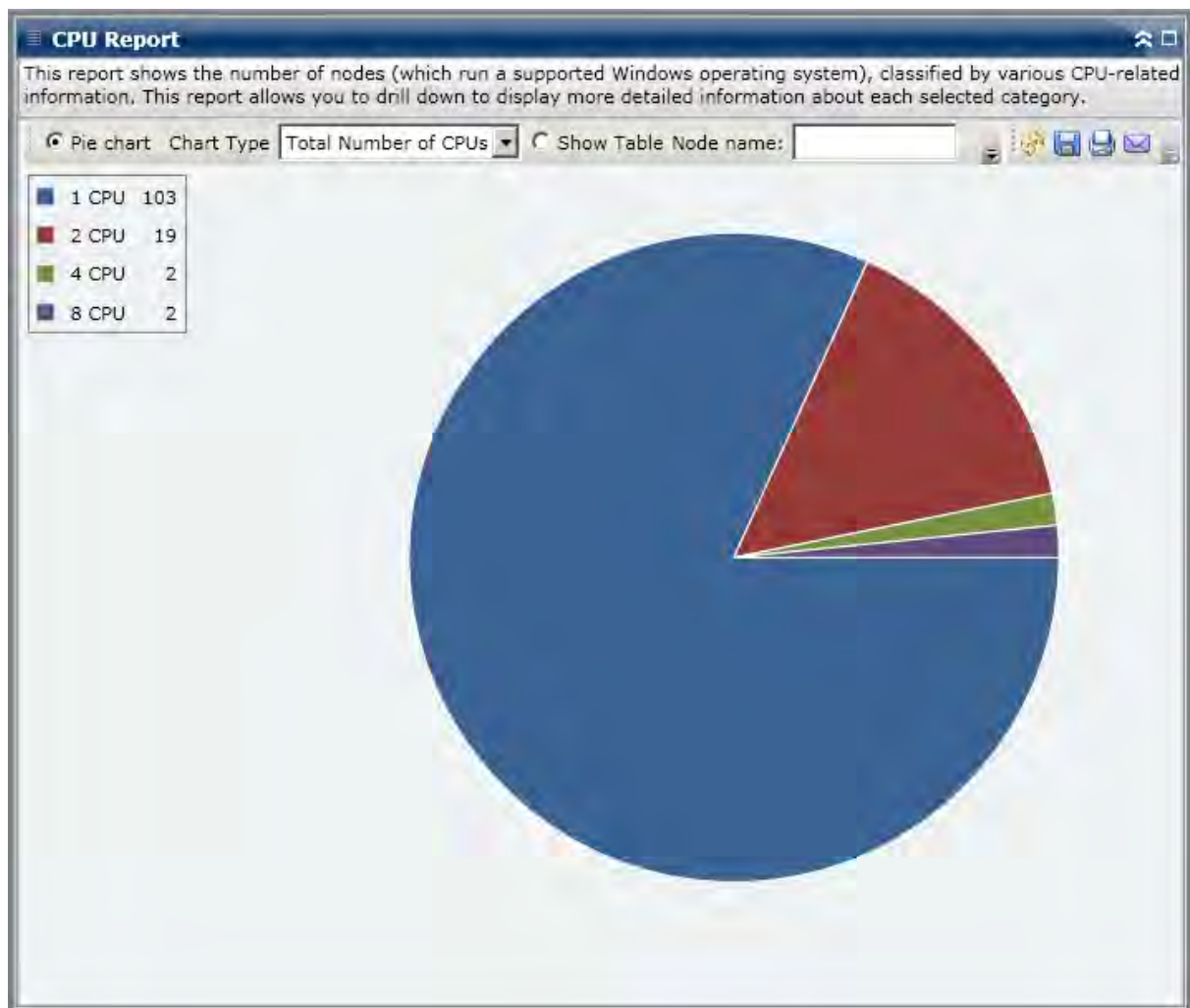
Always look for patterns in behavior to isolate potential problem CPUs and determine if nodes with the same CPUs are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The CPU Report can be displayed in either a pie chart or as a full table.

Pie Chart

The pie chart format provides a high-level overview of the nodes within your CA ARCserve Backup Domain and lets you view the corresponding CPU information based upon specified filters. The Chart Type dropdown menu lets you select how to display the node CPU quantity information and can be based upon either the Physical attribute of the CPU (single or multiple), the manufacturer (Intel or AMD), or the architecture (32-bit or 64-bit).



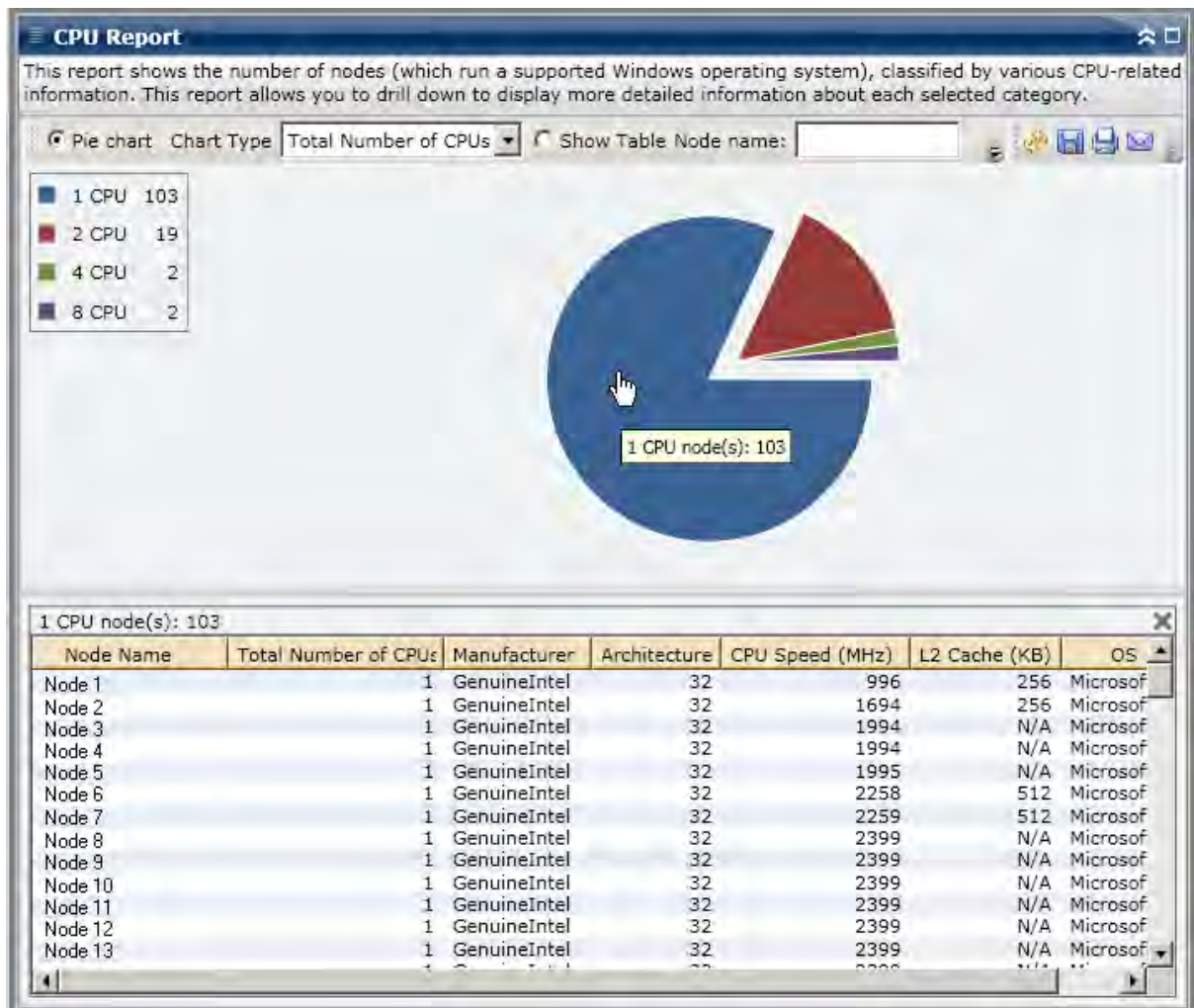
Show Table

The Table view format provides more detailed information about each node within your CA ARCserve Backup Domain. The table format includes all available CPU information, such as the physical structure, manufacturer, architecture, speed, cache, and OS for all Node CPU categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The CPU Report can be further expanded from the Pie chart view to display more detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



Data Distribution on Media Report

The Data Distribution on Media Report displays the amount and distribution of data that was backed up to different types of media (deduplication device, disk, and tape) during the last specified number of days. For the deduplication device media and tape with hardware compression, this report also shows a comparison of the raw data size to the compressed data size (in GB).

Report Benefits

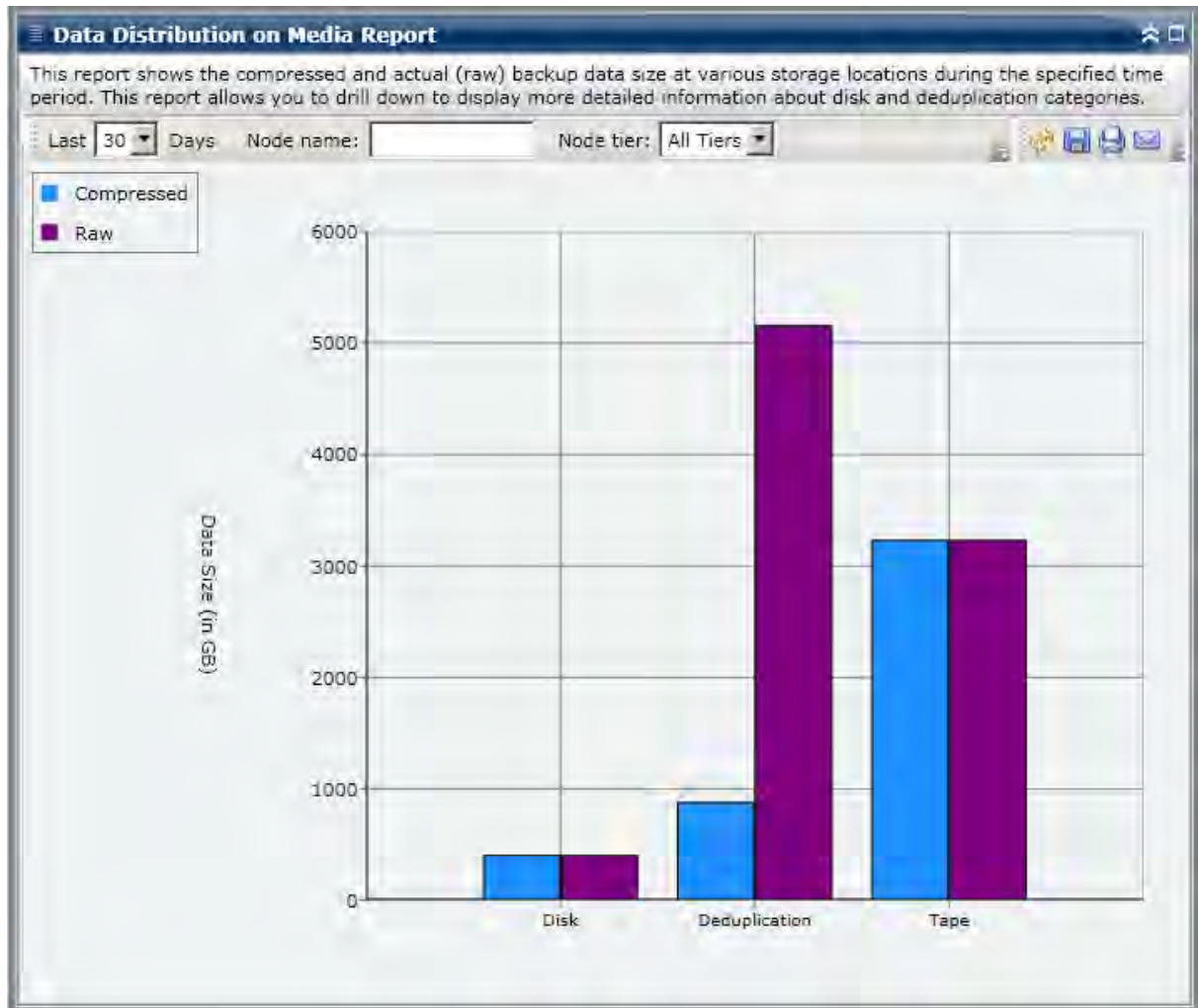
The Data Distribution on Media Report is helpful in analyzing all servers within your CA ARCserve Backup Domain to see how your data is distributed on various types of backup media. From this report you can also determine the amount of savings (backup size) gained by compressing your data during backup. By having this knowledge, you can quickly and easily determine how this savings in backup size can also result in a savings to the backup resources needed.

For example, from this report you can see that within your CA ARCserve Backup Domain, the compressed backup data located on a deduplication device is much smaller in size than the raw backup data would have been. If this report also shows that you have other data that was backed up to a disk (and therefore not compressed), you should consider using more deduplication to improve your backup efficiency. In addition, you can also determine whether you need less backup tapes to store your compressed data.

Note: Data that is saved on tapes has no backup size savings unless the tape supports hardware compression. Only data that is compressed and saved on deduplication devices result in a significant backup size savings.

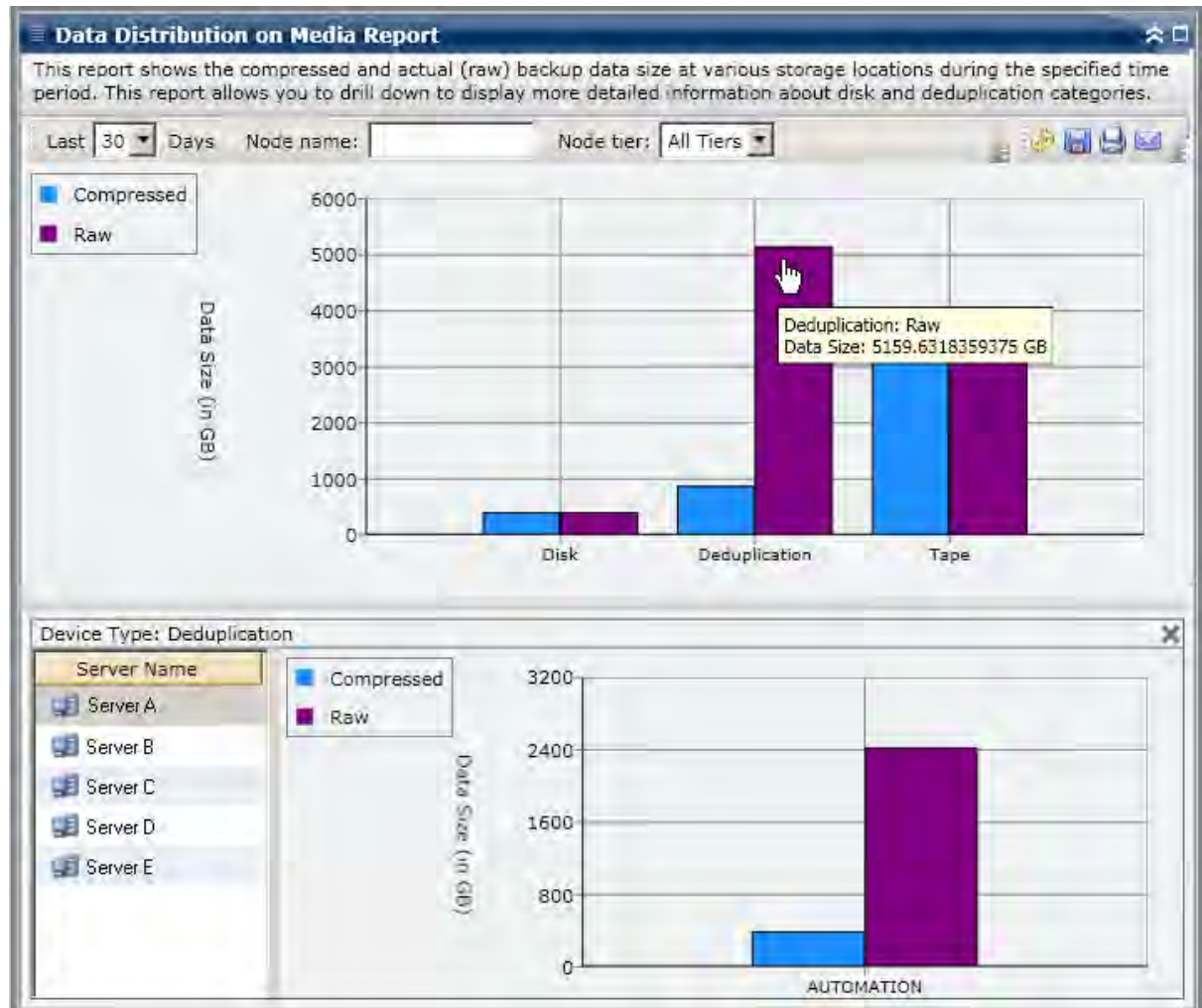
Report View

The Data Distribution on Media Report is displayed in a bar chart format, showing the amount of backup data (in GB) within your CA ARCserve Backup Domain that has been distributed on the different types of media during the last specified number of days. The types of media displayed are Deduplication Devices, Disk, and Tape. The Deduplication Device media is further divided into two separate categories for comparing the savings of compressed data size and raw data size.



Drill Down Reports

The Data Distribution on Media Report can be further expanded to display more detailed information. You can click on either of the Deduplication or Disk categories to drill down and display detailed bar charts for each individual deduplication device or disk device (FSD and VTL) within the corresponding CA ARCserve Backup server. (The drill-down capability does not apply to media in the Tape category). This detailed display shows the compressed data size and raw data size on each device and lets you compare the savings.



Deduplication Benefits Estimate Report

The Deduplication Benefits Estimate Report displays the estimated savings of backup space if you use a deduplication device.

Report Benefits

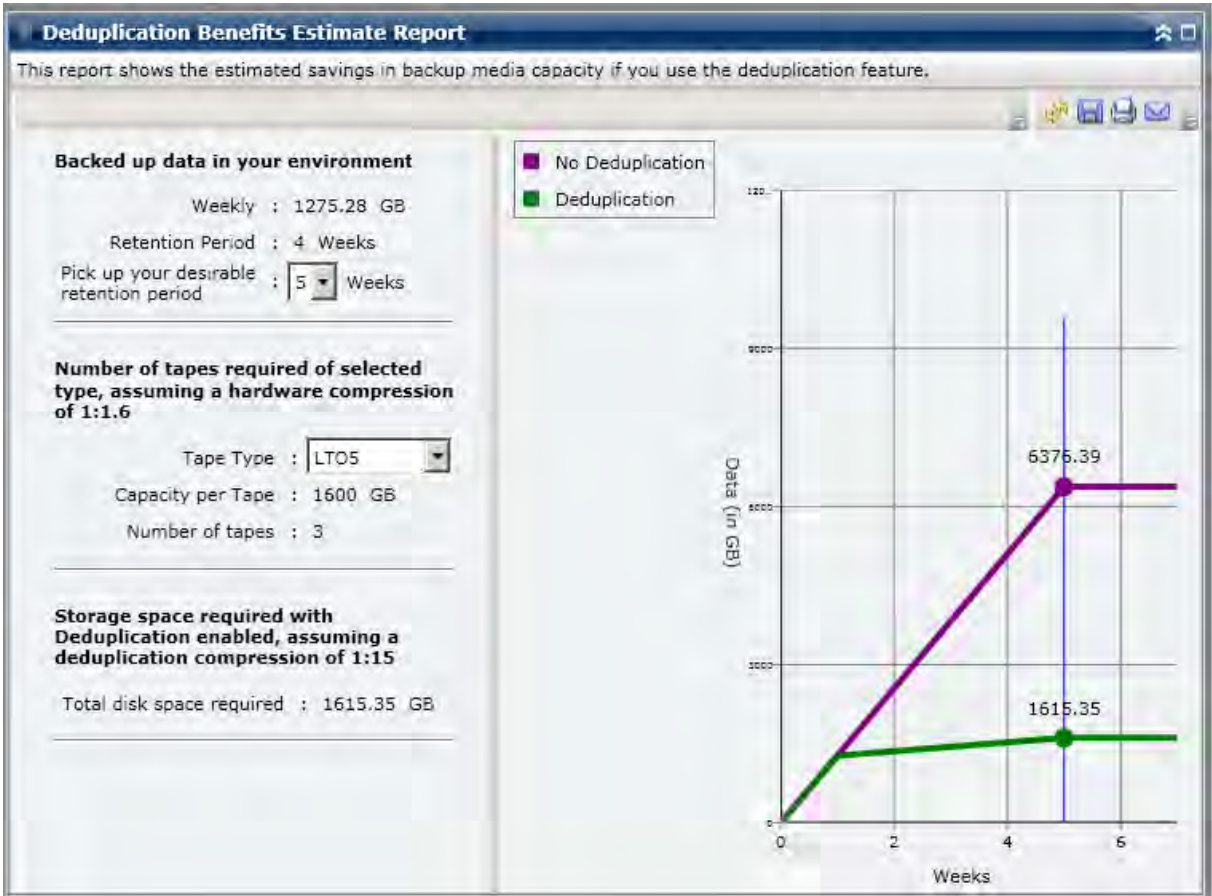
The Deduplication Benefits Estimate Report is helpful in analyzing and determining your backup capacity savings if you use or do not use the CA ARCserve Backup deduplication feature. This report is based upon the assumption that you are backing up same amount of data with and without deduplication and provides an estimated savings in capacity needed. From this report, you can then easily translate this capacity savings into a cost savings that would be realized by using less space on your hard drive rather than purchasing tapes.

For example, if you perform weekly backups of 1 TB of data and want to retain this data for 4 weeks, this equates to occupying 4 TB of space on tapes. If the average capacity of your backup tape is 500 GB, it would then require approximately 8 tapes to store this backup data, assuming no hardware compression. If you assume a hardware compression of 1.6:1, you would then require approximately 6 tapes to store this backup data.

Now from this report, you can easily see that if you perform a backup of the same amount of data but use the deduplication feature with a low average compression ratio of 1:15, this would equate to needing only 1230 GB of hard drive space (approximately). You can then further determine your average cost to store data on the number of tapes compared to the cost of occupying a much less amount of hard drive space.

Report View

The Deduplication Benefits Estimate Report is displayed in graph format showing the amount of backed up data (in GB) and the retention period (in weeks). The display is grouped by the type of tape being used and displays the corresponding capacity per tape and number of these tapes required to back up your data. This report lets you easily see the projected savings in required storage space (and related cost) if you used or did not use deduplication.



Deduplication Status Report

The Deduplication Status Report displays the number of nodes that were backed up using a deduplication device during the last specified number of days. This report shows which of those nodes have and have not benefited from deduplication, along with the amount of savings realized.

Report Benefits

The Deduplication Status Report is helpful in analyzing and determining which nodes have benefited from deduplication and the amount of savings (backup size) that were gained for each node. By having this knowledge, you can quickly and easily determine how this savings in your backup size can also result in a savings to the backup resources needed.

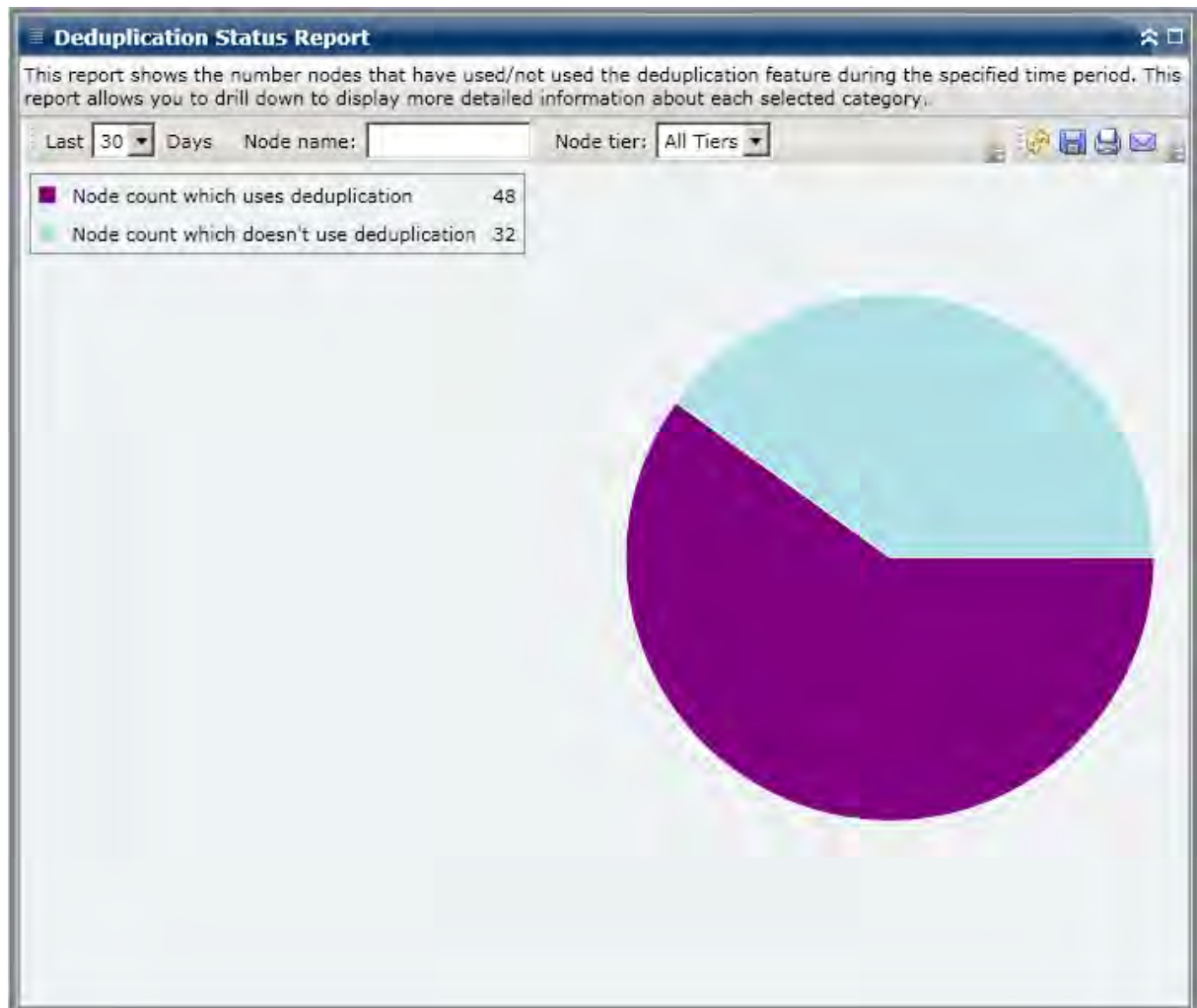
For example, if from this report you see that most of your nodes have benefited from deduplication, and the amount of actual savings between the raw backup size and the compressed backup size is significant, you should consider using deduplication for more backups to improve your backup efficiency. In addition, you can also determine whether you need less backup tapes to store your compressed data.

Note: Data that is saved on tapes has no backup size savings unless the tape supports hardware compression. Only data that is compressed and saved on deduplication devices result in a significant backup size savings.

Report View

The Deduplication Status Report is displayed in a pie chart format, showing the number (and percentage) of nodes that benefited from deduplication and the number of nodes that did not.

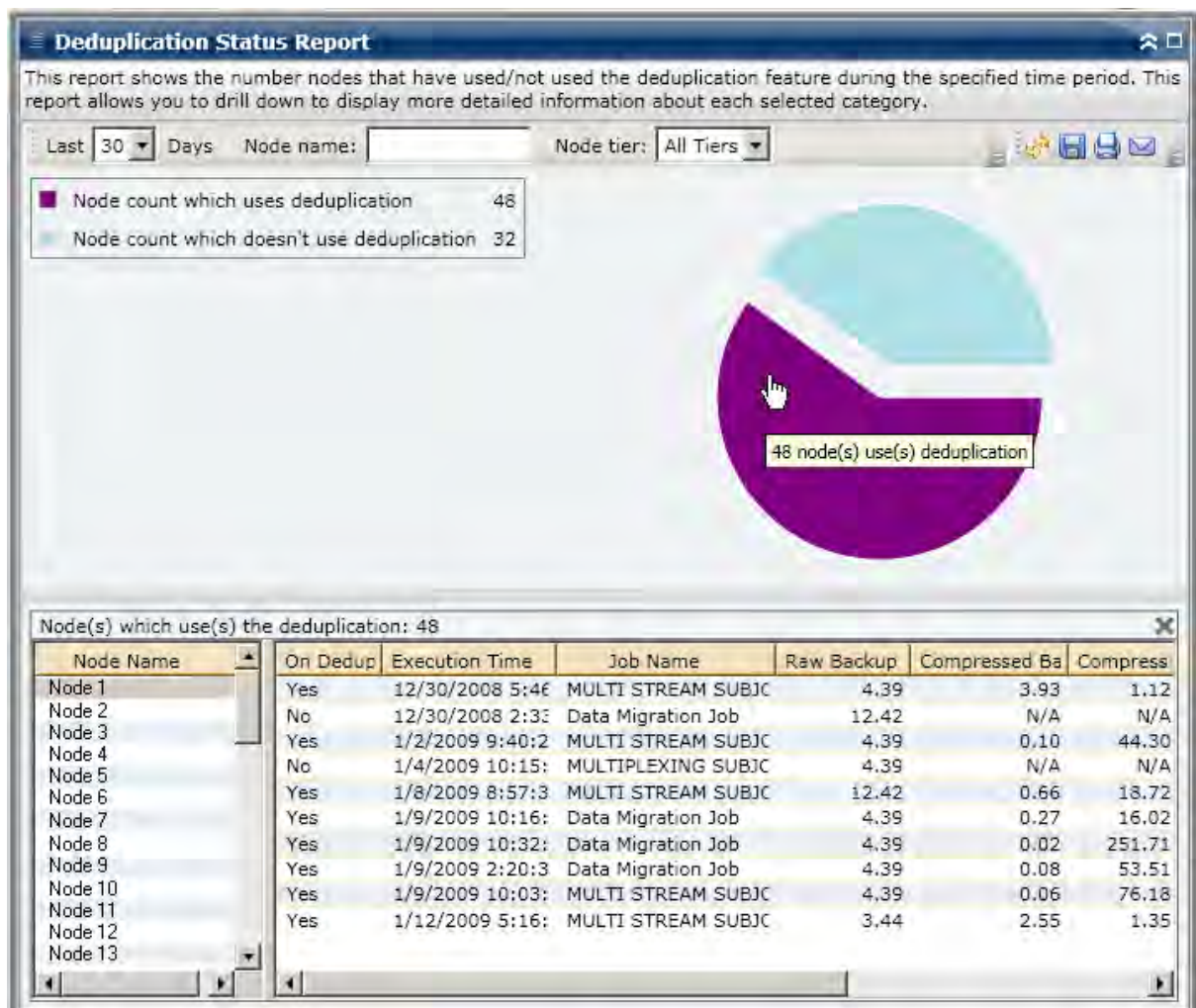
- Node count which benefited from deduplication is defined as the number of nodes that have one or more sessions which used a deduplication device, and the calculated compressed backup size is less than the raw backup size.
- Node count which did not benefit from deduplication is defined as the number of nodes that have one or more sessions which used a deduplication device, and the calculated compressed backup size is not less than the raw backup size.



Drill Down Reports

The Deduplication Status Report can be further expanded to display more detailed information. You can click on either of the two pie chart categories to display a detailed listing of all nodes associated with that category that were backed up during the specified time period. The drill down report includes an easy-to-see comparison of the raw backup data size and the compressed data size for each node, and lets you quickly determine the benefits of deduplication.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



Disk Report

The Disk Report is an SRM-type report that displays the disk information for all Windows nodes within your CA ARCserve Backup Domain, organized by the amount of allocated disk space in each node. A disk can be allocated and still have free space. The unused space can be re-allocated to another disk. Free space is reported in the Volume Report.

Report Benefits

The Disk Report is helpful in quickly classifying machines based on the amount of space allocated to each disk. This report displays the total amount of partitioned space on each physical hard drive. You can get an overall view to analyze and determine which disks have space that is not allocated and can potentially be reallocated to another disk.

You can use this report in conjunction with the Volume Report to analyze the amount of allocated space compared to the amount of used space.

For example, if from this report you see that a particular disk has a low amount of allocated space, you should then check the Volume Report to compare the allocated space to the amount of space being used. If the allocated space is low, but the used space is high, you should investigate the reason for this non-allocated space and if possible, create a new volume to better utilize your available space.

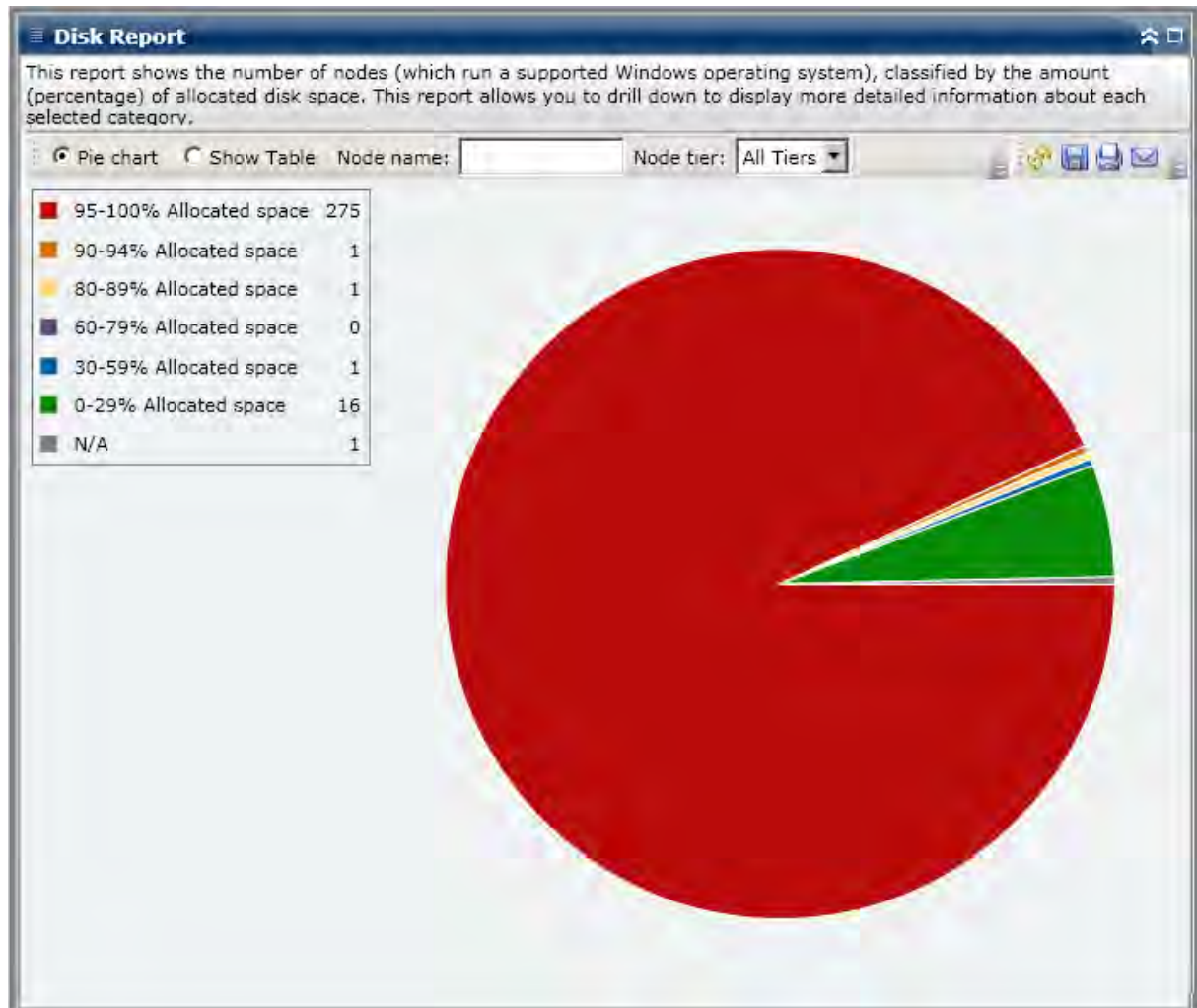
Always look for patterns in behavior to isolate potential problem disks. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Disk Report is displayed in a pie chart format or table format.

Pie Chart

The pie chart provides a high-level overview of the disks in your environment, sorted by pre-configured used disk space ranges (in percentage). You want to make sure that your disks are allocated properly because if space is not allocated, then it cannot be used.



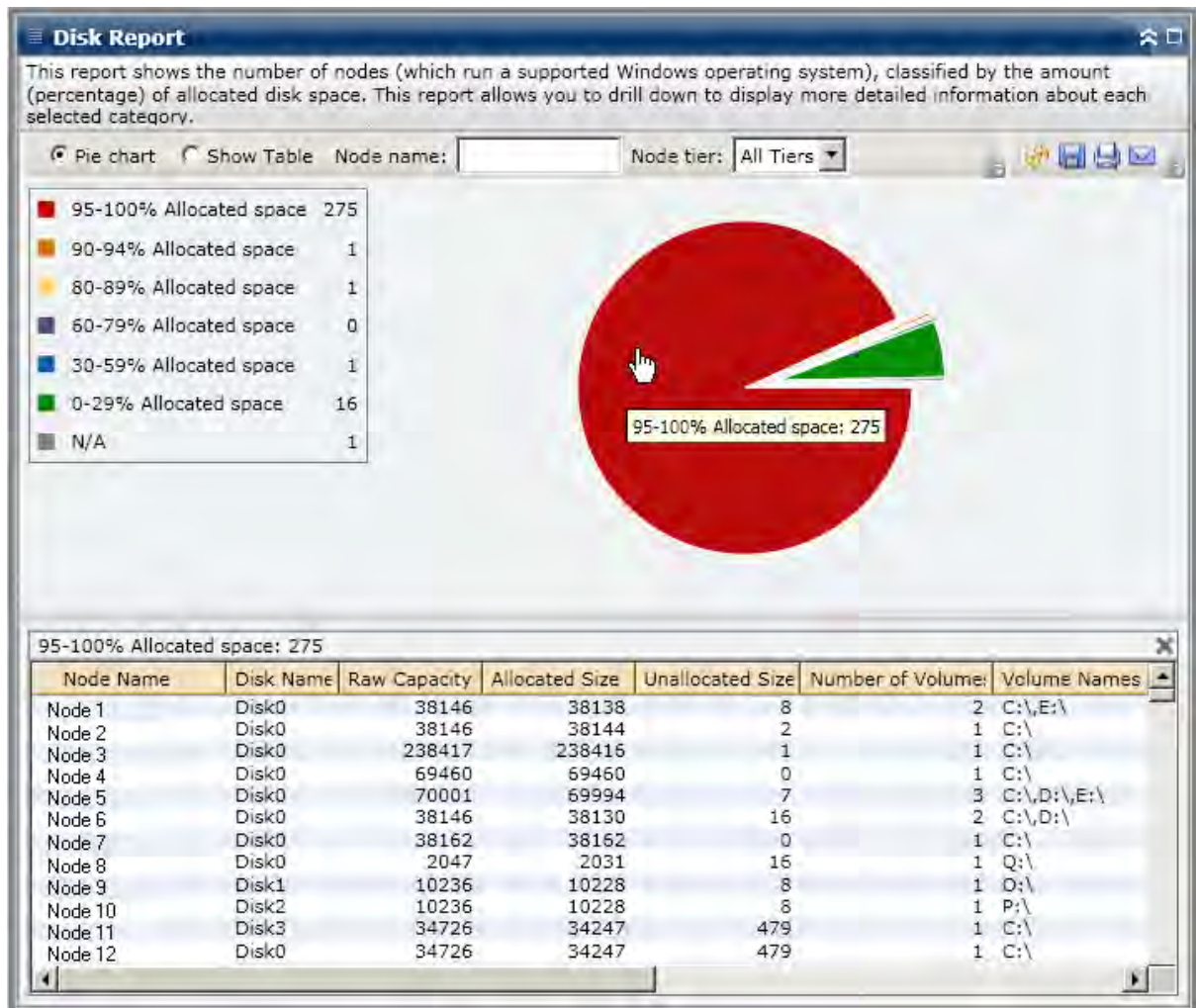
Show Table

If you select Show Table, the Disk Report displays more detailed information in table format, listing the Node Name, OS, Disk Name, Manufacturer, Type, Size, Used Space, Unused Space, Number of Volumes and Volume Names for all of the allocated space categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Report

The Disk Report can be further expanded from the Pie chart view to display a drill-down report with the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



Job Backup Status Report

The Job Backup Status Report lists the most recent status results of all backup jobs (Full, Incremental, and Differential) that were initiated for the specified servers during the last specified number of days.

By default, CA ARCserve Backup r12.5 maintains job records for 180 days. If you want Dashboard to display job records for a different time period, you can add a registry key and set the desired day range. You can define the job pruning interval by adding a new registry key as follows:

To configure the job pruning time interval setting in the Registry Editor

1. Open the Registry Editor.
2. Expand the tree in the browser of the Registry Editor by selecting the following:

`HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\Base\Database\`
3. Add a new DWORD Value and name it "JobPruningDays"
4. Double-click the JobPruningDays key to open the Edit DWORD Value dialog. You can now modify the DWORD setting and set a specific time interval to prune job records from CA ARCserve Backup database.
5. When you finish configuring the JobPruningDays key for the SRM probe, close the Registry Editor.

Report Benefits

The Job Backup Status Report is helpful in analyzing and determining which jobs are more effective than others, and which ones could be potential problem areas.

For example, generally you can use this report to check the status of the most recent backup jobs from a job perspective. If the backup status from the previous day is all green (successful), you know that you had a good backup. However, if the backup status is red (failed), you can quickly analyze the activity log in the drill-down report to determine the problem area and fix it with minimal delay. You can also monitor the jobs on a daily basis to identify any trends in the behavior of backup jobs in your environment.

Always look for patterns in behavior to isolate potential problem jobs and determine if the same jobs are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem backup jobs.

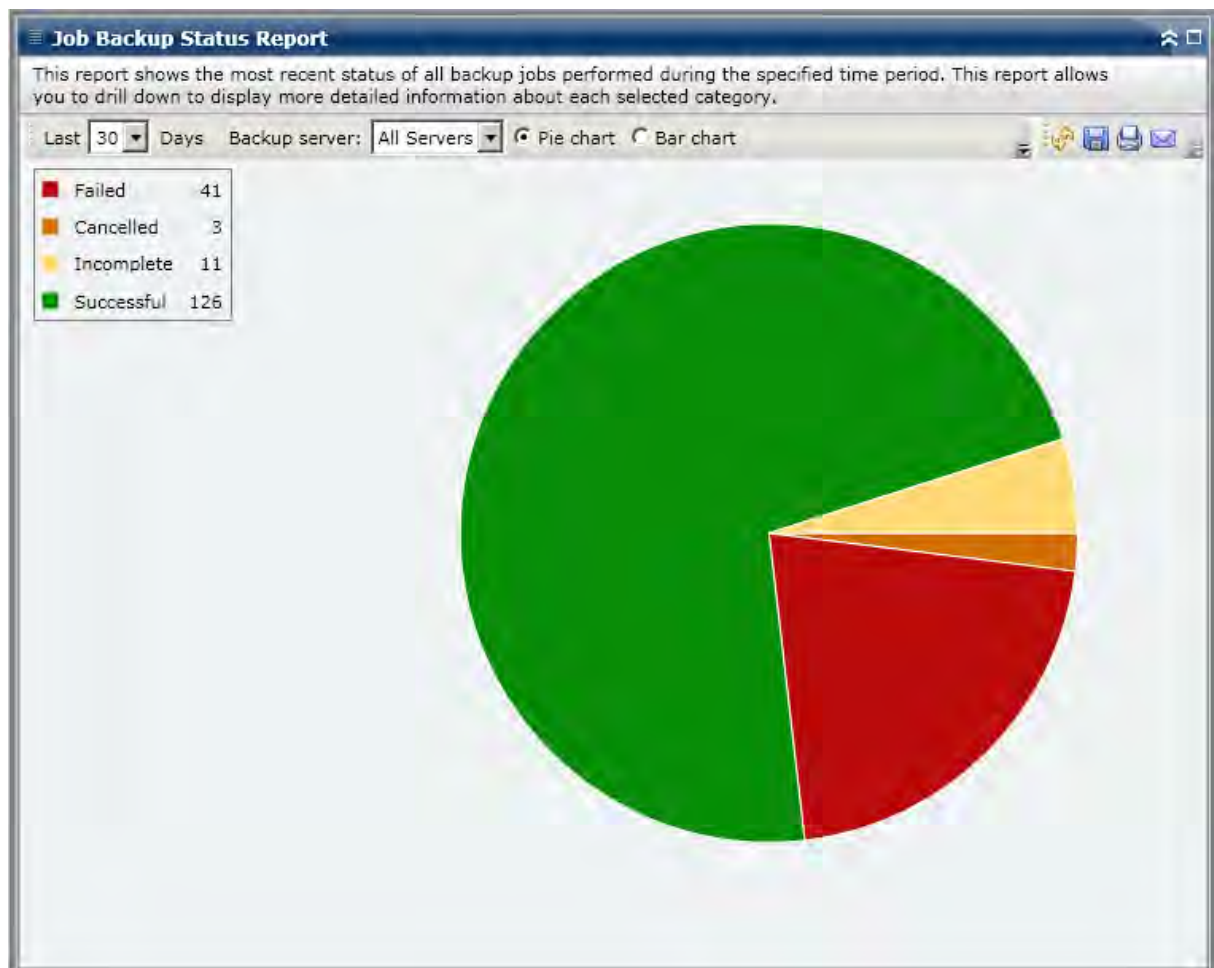
Report View

The Job Backup Status Report can be displayed as either a pie chart or as a bar chart.

Note: By default, CA ARCserve Backup only retains Activity Log information for 14 days. If you want CA ARCserve Backup Dashboard to display Activity Log information for more than 14 days, you must modify the "Prune activity logs older than" option to increase the log retention period. For more information about modifying Activity Log settings, see the Administration Guide.

Pie Chart

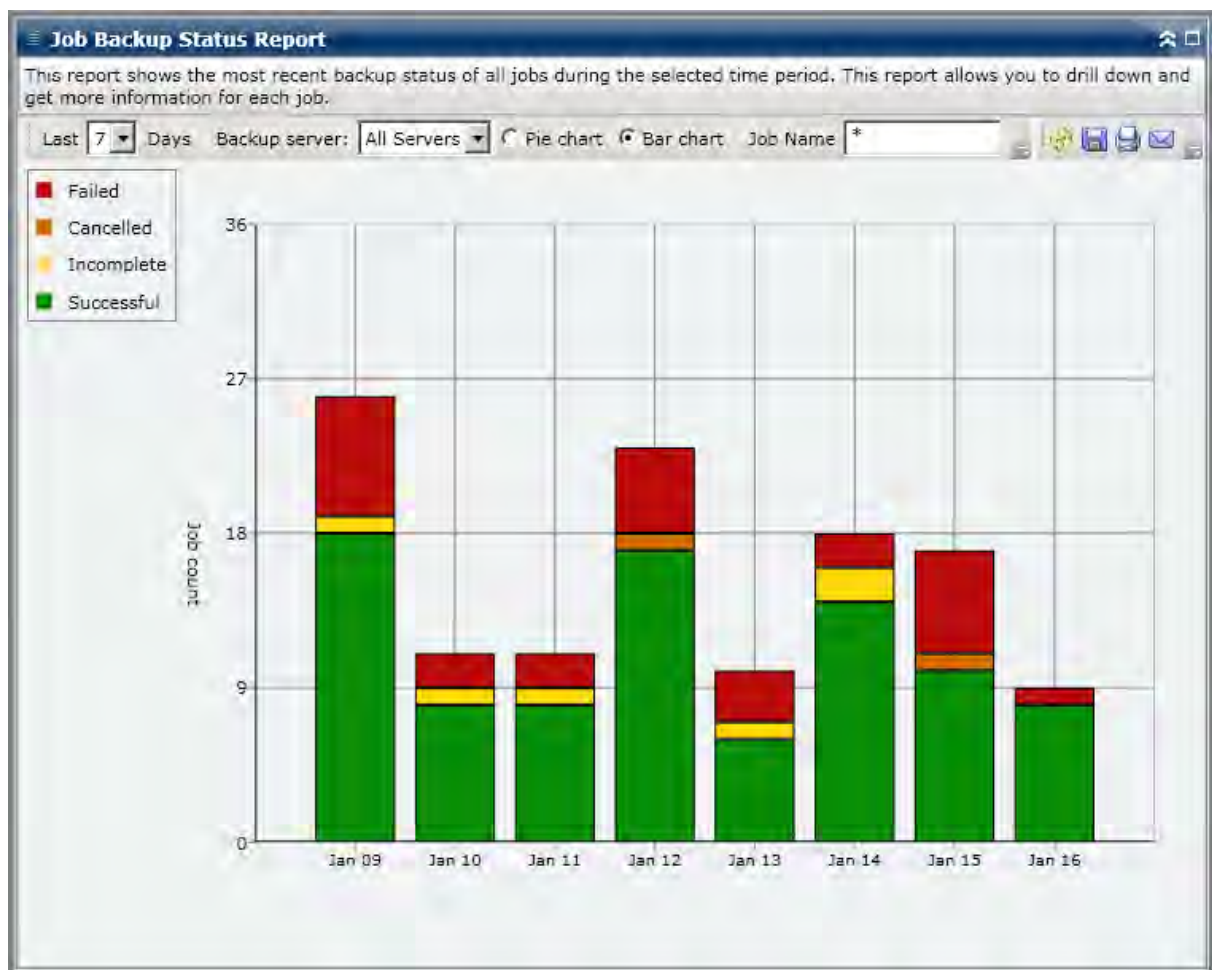
The pie chart provides a high-level overview of backup jobs for the selected server for all days of the specified time period. The status categories shown in the pie chart represent a percentage of the total number of backup jobs for that server during the last specified number of days, with the most recent status being considered for every job.



Bar Chart

The bar chart provides a more detailed level view of backup jobs for the selected server during each day of the specified time period. The status categories shown in the bar chart represent the daily number of backup jobs for that server during the last specified number of days.

Note: By default, CA ARCserve Backup Dashboard only displays bar chart information for a maximum of 90 days. Increasing the number of displayed days to more than 90 days would result in the bar chart information not being legible. If you specify to display report information for more than 90 days, the bar chart limits the display to only 90 days, regardless of the number of days entered. This limitation does not apply to pie chart views of the same report. (The maximum number of displayed days for a pie chart is 999 days).



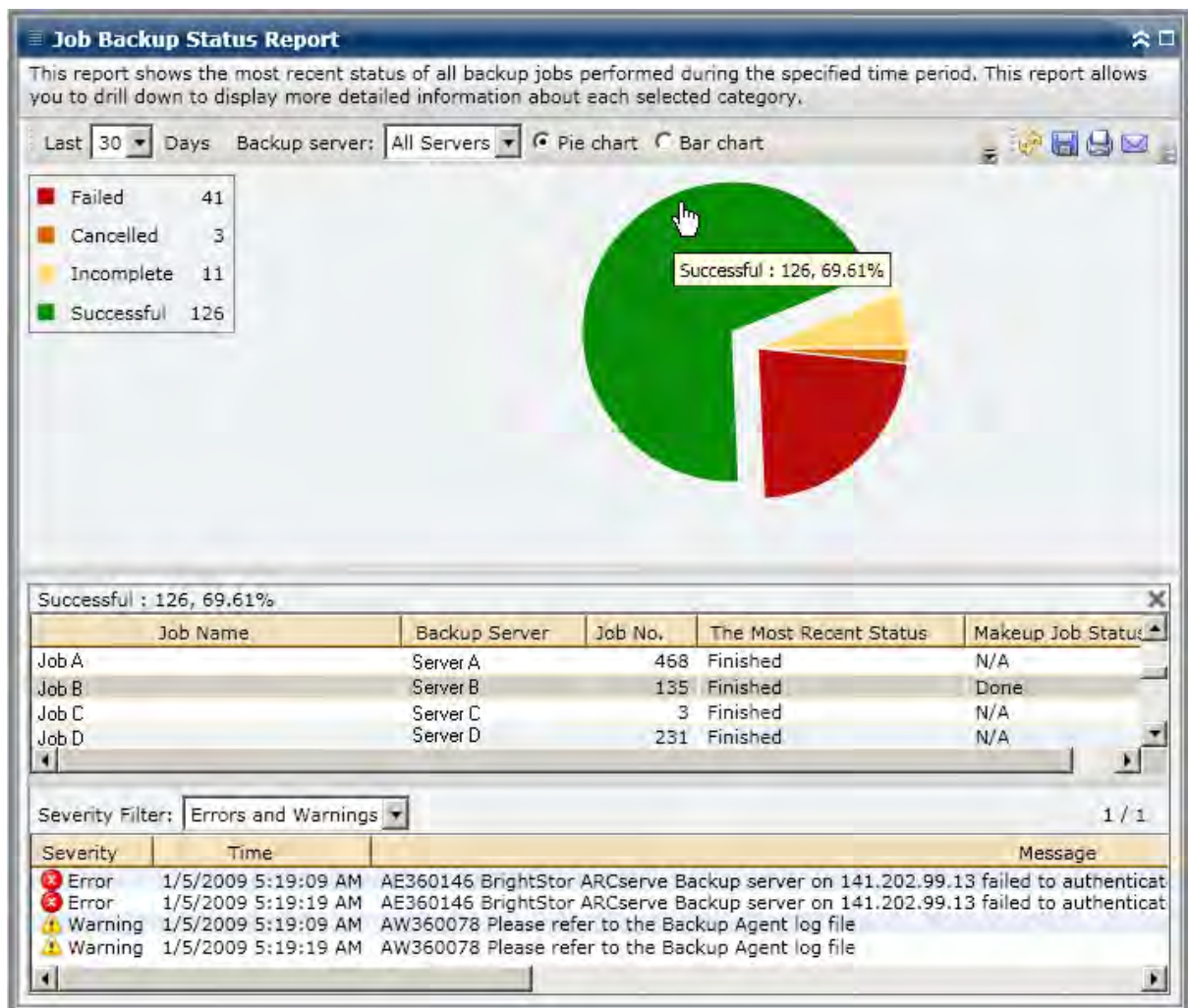
Drill Down Reports

The Job Backup Status Report can be further expanded to display more detailed information. You can double-click on any status category (from either the pie chart view or the bar chart view) to drill down from a report of summary information to a more focused and detailed report about that particular category. For example, if you click on the Incomplete category, the report summary changes to display a filtered list of just the backup jobs that were *not completed* during the specified time period.

In addition, this report displays the status of any associated makeup job. The makeup job status can be one of the following:

- **Created**- A makeup job has been created and is ready in the job queue, but has not been run yet.
- **Not Created**- After the initial backup job failed, there was no attempt to create a makeup job. You should verify that the job was properly configured to create a makeup job in case of failure. This column can be ignored for successful, incomplete, or cancelled backup jobs.
- **Active**- A makeup job has been created and is running. The status of the makeup job is unknown yet.
- **Finished**- After the initial backup job failed, the makeup job has been completed and is finished running. From the Most Recent Status column, you can view the corresponding final status of the makeup job, with the possible results being Finished, Incomplete, or Failed.

Note: From the bar chart view, you can also drill down to display a filtered list of jobs for a status category on a single day.



You can drill down further in this report by clicking on the name of an individual job to display a more detailed listing of all log messages associated with that job. You can also filter the list by specifying the severity of the messages displayed (Error & Warning, Error, Warning, Information, or All).

Note: Dashboard uses pagination to display the first 100 log messages. You can click on the Next page button to view further messages.

Note: From this drill down report, you can click on any listed error or warning message to display the related troubleshooting help topic with the corresponding reason and corrective action.

License Report

The License Report displays the license information for all CA ARCserve Backup agents and server options that are used within your CA ARCserve Backup domain. If the Usage Count for an agent or option is greater than the corresponding Licensed Count, the entry will be displayed in red to indicate that a potential licensing problem exists and could result in a backup failure.

In addition, a yellow alert bar is also displayed at the top of the report to further highlight this potential problem condition and request that you check the Agent Distribution Report for more detailed information about out-of-date agents.

- The Component Type drop-down menu is provided to let you filter the display by agents or server options. You can specify to display the license information for all agents and options or filtered for just the agents or for just the options.
- The Component Name drop-down menu is provided to let you filter the display for an individual agent or server option. The Component Name drop-down menu includes all "active" agents and server options, which means any agent or option that has been licensed for use within your CA ARCserve Backup domain.
- The Version drop-down menu is provided to let you filter the display by the release version number of the agent or server option. You can specify to display the license information for all versions or filtered for just r11.1, r11.5, r12, r12.1, or r12.5 versions of the agents and options.

This report can be used to quickly determine the license counts and usage of your CA ARCserve Backup agents and server options, and lets you identify which agents and options may have a potential license problem.

Report Benefits

The License Report is helpful in analyzing and determining which CA ARCserve Backup components (agents and server options) are being used within your CA ARCserve Backup domain and if they are adequately licensed. From this report you can get a snapshot view of your licensing information and determine the comparison of your component usage to your component licensing.

For example, if you find that your backups are failing repeatedly on specific machines, you may not be properly licensed to use certain CA ARCserve Backup components on that machine. From this report you can quickly determine if you have adequate license count for your current usage. If the license count for your CA ARCserve Backup agents or options is less than the usage count, you may be attempting to perform a backup using unlicensed components.

Report View

The License Report is displayed in a table format, listing the CA ARCserve Backup licensed components (agents and server options) within your CA ARCserve Backup domain, along with their corresponding license count, usage count, and release version of the component.

License Report			
This report shows the total number of licenses issued for all CA ARCserve Backup server options and agents, as well as the license usage.			
Check the Agent Distribution Report for a complete listing of which nodes contain out-of-date agents.			
⚠ A potential product license problem may exist. If the license usage count is more than the license issued count, your backup will fail. Please verify that your license count is accurate to meet your backup requirements.			
Component Type	All	Component Name	All Components
		Version	All Versions
Component Name	Licensed Count	Usage Count	Version
Agent for Advantage Ingres	25	0	12.1
Agent for FreeBSD	50	0	12.5
Agent for IBM Informix	1	1	12.5
Agent for Microsoft Exchange	25	4	12.5
Agent for Microsoft SharePoint	0	1	12.0
Agent for Microsoft SharePoint	0	1	12.1
Agent for Microsoft SharePoint	25	2	12.5
Agent for Microsoft SQL Server	10	1	12.0
Agent for Microsoft SQL Server	10	1	12.1
Agent for Microsoft SQL Server	25	4	12.5
Agent for Open Files	50	50	12.5
Agent for Open Files	10	14	12.5
Agent for Open Files for Virtual Machines	0	36	12.5
Agent for Oracle	25	5	12.5
Agent for Oracle for UNIX	25	5	12.5
Agent for Sybase	1	1	12.5
Agent for Virtual Machines	100	82	12.5
Application Server Suite	25	0	12.5
Backup Agent for Apple Macintosh	50	0	12.5
CA ARCserve Backup	75	19	12.5
Central Management Option	51	1	12.5
Client Agent for Linux	50	0	12.5
Client Agent for NetWare	50	0	11.1
Client Agent for UNIX	50	4	12.5
Client Agent for Windows	0	2	11.5
Client Agent for Windows	5	1	12.0
Client Agent for Windows	5	1	12.1
Client Agent for Windows	150	64	12.5
Database Server Suite	25	0	12.5

Media Assurance Report

This report shows the number of nodes that have/have not been scanned to ensure that the sessions on the media are restorable. This report can be used to determine if the data from your nodes is properly protected on the media and provides a means to quickly identify and resolve potential problem areas with restoring your backups.

Report Benefits

The Media Assurance Report is helpful in analyzing and determining which nodes are adequately backed up and protected for a data restore, and which ones could be potential problem areas. You should not have to wait until you attempt to perform a data restore to discover that your backup was not good. Media assure provides an increased sense of security that the data that has been backed up to media is good and can be restored if necessary. By performing random scans of the backed up media, CA ARCserve Backup almost eliminates the possibility that restoring your backed up will fail.

Generally if a specific node contains high-priority data (Tier 1), you would want to have some assurance that your data can be restored quickly and completely if necessary.

For example, all nodes that contain high-priority data (Tier 1) should be included in the "Nodes with Assured Sessions" category to assure the data can be restored. If from this report, you discover that some high-priority nodes are included in the "Nodes without Assured Sessions" category, you should modify your scan schedule as necessary to ensure these Tier 1 nodes are properly scanned, protected, and checked.

A good practice is to review this report in conjunction with the Node Recovery Points Report to make sure you not only have adequate recovery points, but also assure the data is guaranteed good to restore.

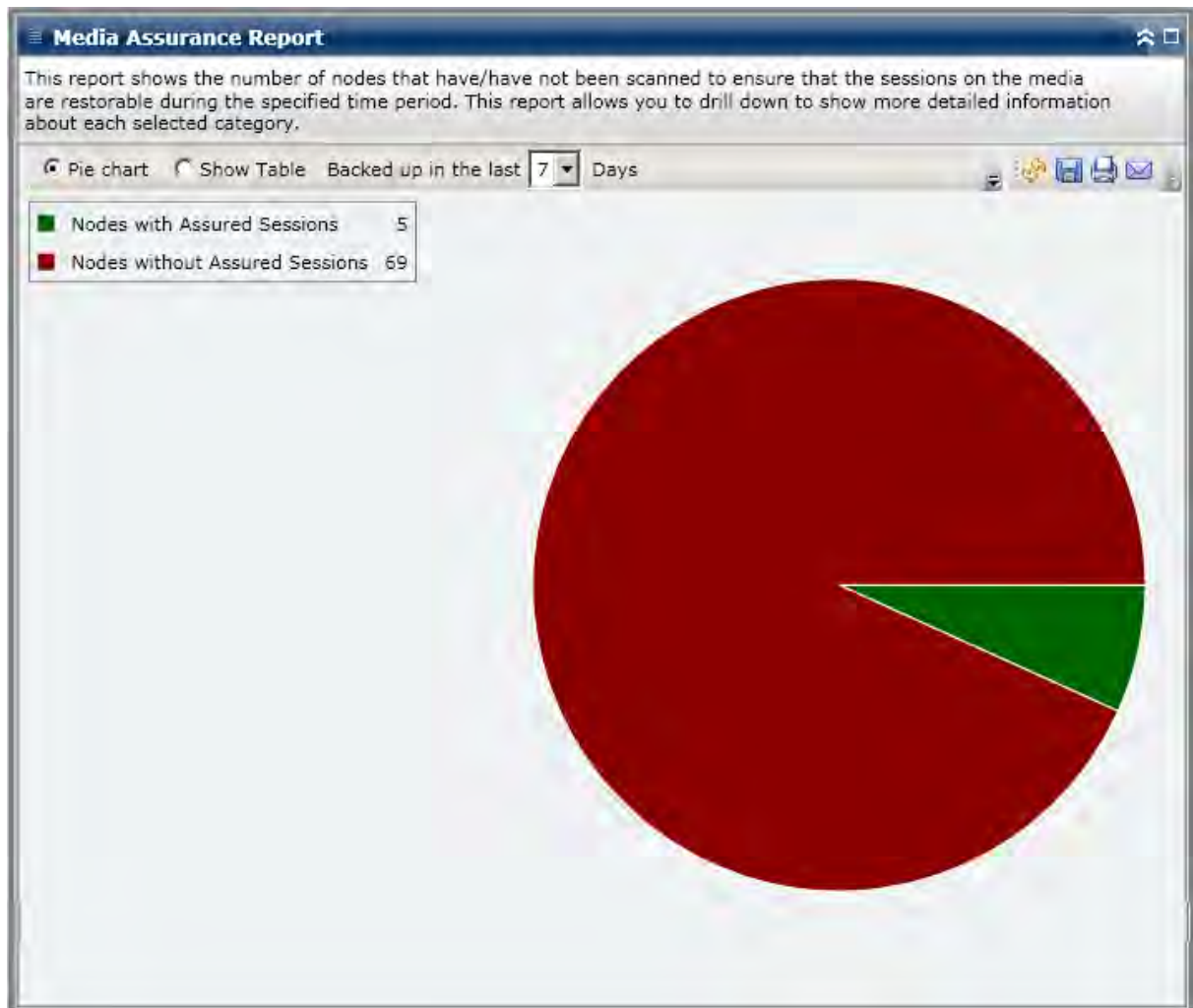
Report View

The Media Assurance Report can be displayed as either a pie chart or as a table.

Note: The date range filter for this report applies to the number of days since the last backup was performed, and not the number of days since the last media scan was performed.

Pie Chart

The pie chart shows the distribution of nodes (number and percentage) that have/have not been scanned to ensure that the sessions on the media are restorable for all days during the last specified number of days.



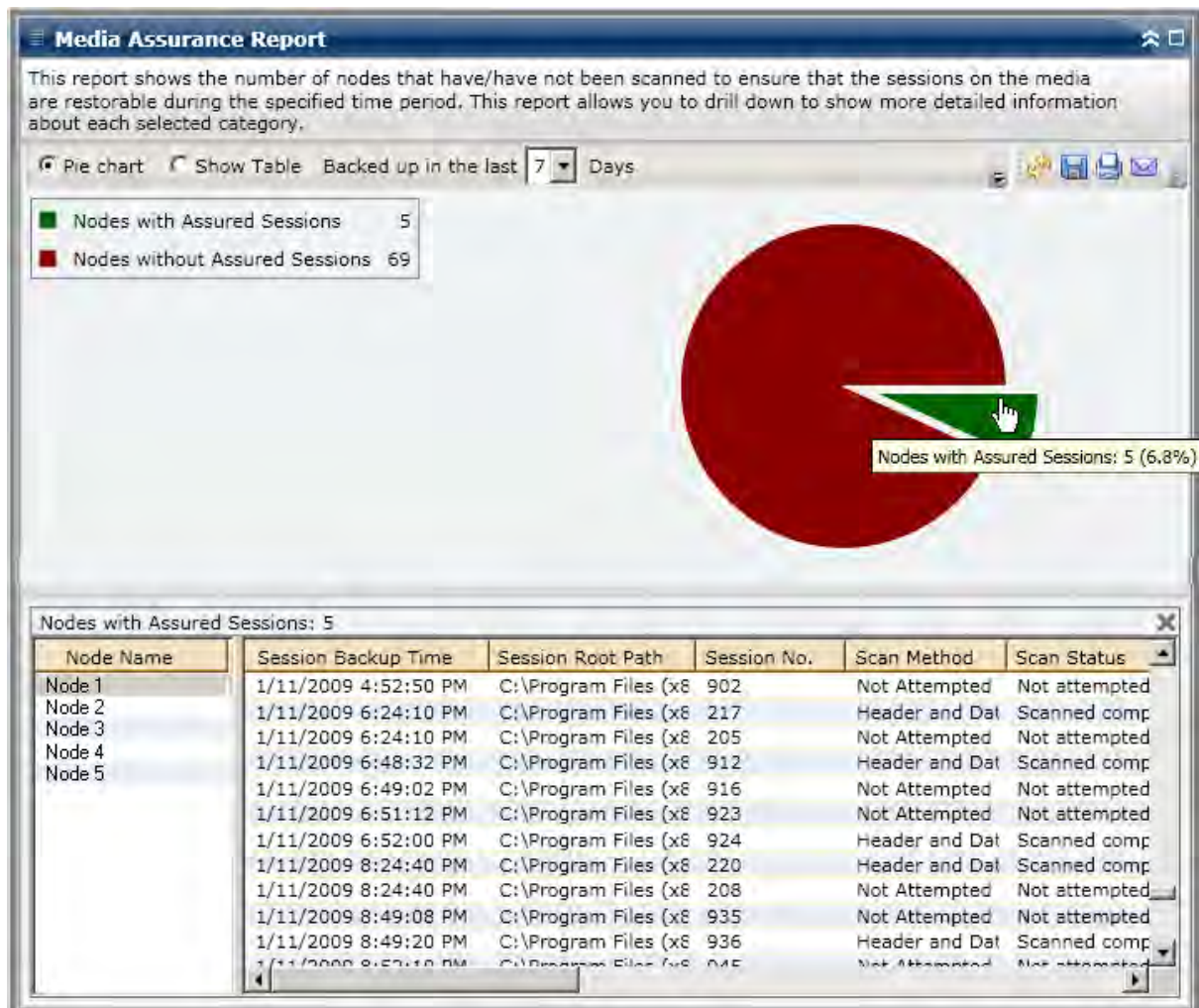
Show Table

If you select Show Table, the Media Assurance Report displays more detailed information in table format listing the Node Name, along with corresponding information about the backups, scan sessions, and media.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The Media Assurance Report can be further expanded from the Pie chart view to display the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



Memory Report

The Memory Report is an SRM-type report that displays the memory information for all Windows nodes within your CA ARCserve Backup Domain. This report categorizes the nodes by the amount of memory contained in each node.

Report Benefits

The Memory Report is helpful in quickly classifying machines based on the amount of memory. You can get an overall view to analyze and determine if the amount of memory is a factor for backup jobs. You may want to make sure that the nodes in your high priority tiers have the most memory.

For example, if from this report you see that a particular node has a slow throughput value, you can quickly determine the amount of memory the node has and look for patterns in behavior among the nodes with less memory or among the nodes with the most memory. You can also use the fastest throughput values as reference points to analyze how much memory is required to perform well. You can compare the slower nodes to the faster nodes to determine if you actually have a problem with memory or if both sets of values are similar, maybe the slower nodes are not performing poorly due to lack of memory.

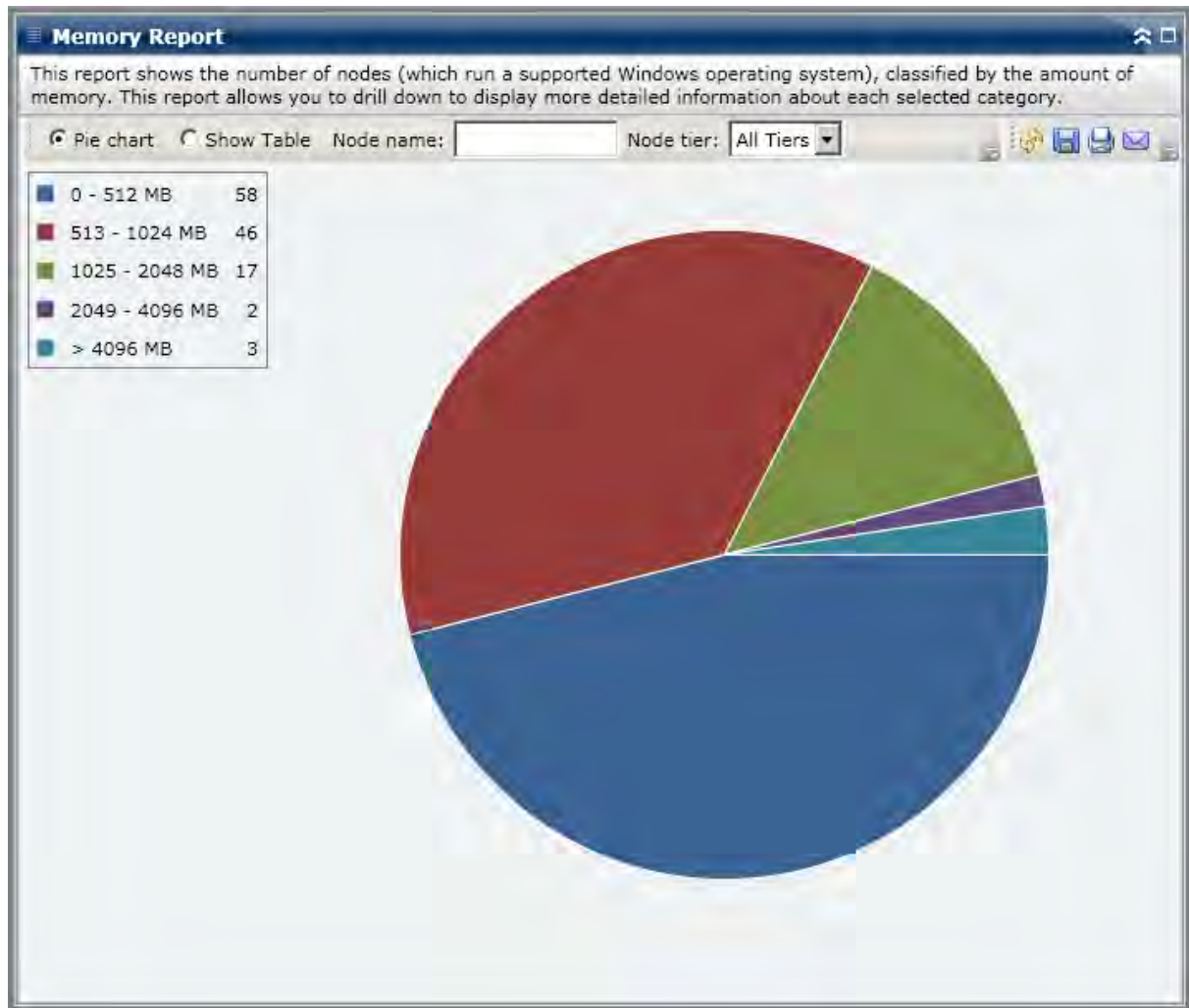
Always look for patterns in behavior to isolate potential problem with memory and determine if nodes with the same amount of memory are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Memory Report can be displayed as either a pie chart or as a table.

Pie Chart

The pie chart shows the memory information for all nodes. The data is populated into the pre-configured categories. The total memory is reported for each node, regardless of how many slots the node may be using.



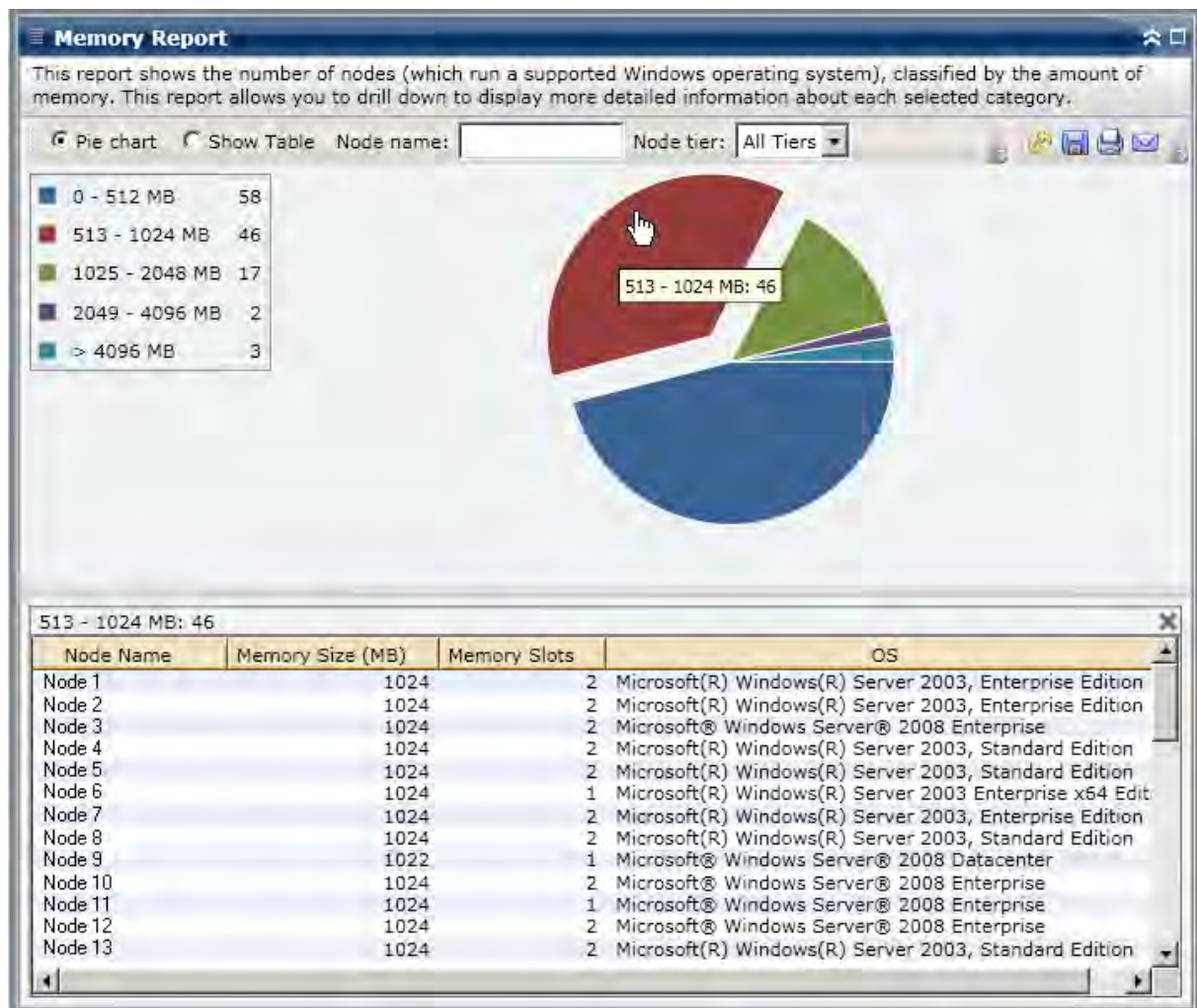
Show Table

If you select Show Table, the Memory Report displays more detailed information in table format listing the Node Name, OS, Memory Size, Memory Slots, and Speed for all of the allocated space categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The Memory Report can be further expanded from the Pie chart view to display the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



NIC Report

The NIC Report is an SRM-type report that shows the Windows nodes within your environment, categorized by the speed of the Network Interface Card (NIC).

Report Benefits

The NIC Report is helpful in quickly classifying machines based on the NIC speed, sorted into pre-configured categories. You can get an overall view to analyze and determine which NICs are more effective than others for backup jobs, and which ones could be potential problem areas.

For example, if you identify a node having slower throughput values, you can monitor the NIC speed of that node through this report. A slower NIC may be a possible reason for slower throughput values. Look for patterns in behavior among the slower NICs or among the same manufacturer.

You can also use the fastest throughput values as reference points to analyze why these NICs are performing well. You can compare the slower NICs to the faster NICs to determine if you actually have a problem or if both sets of values are similar, maybe the slower NICs are not performing poorly. You can also use this report to determine if you need to upgrade your NIC hardware.

Always look for patterns in behavior to isolate potential problem NICs and determine if nodes with the same type of NIC are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

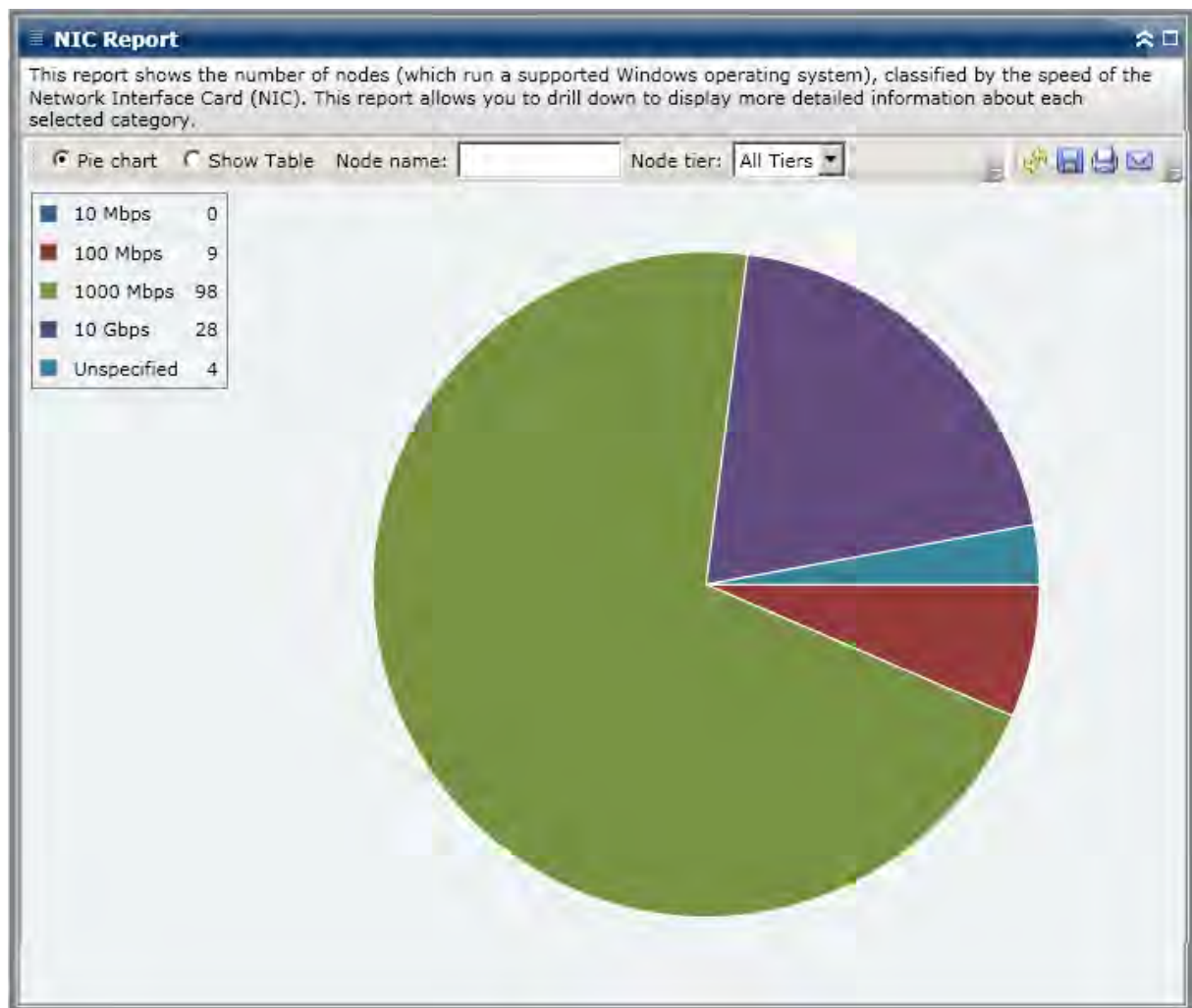
Report View

The NIC Report can be displayed as either a pie chart or as a table.

Note: The “unspecified” category indicates that the network card speed could not be detected by Dashboard. For example, it may be because the card is disconnected from the network or it may be detected at an incorrect speed.

Pie Chart

The pie chart shows the memory information for all nodes. The data is populated into the pre-configured categories.



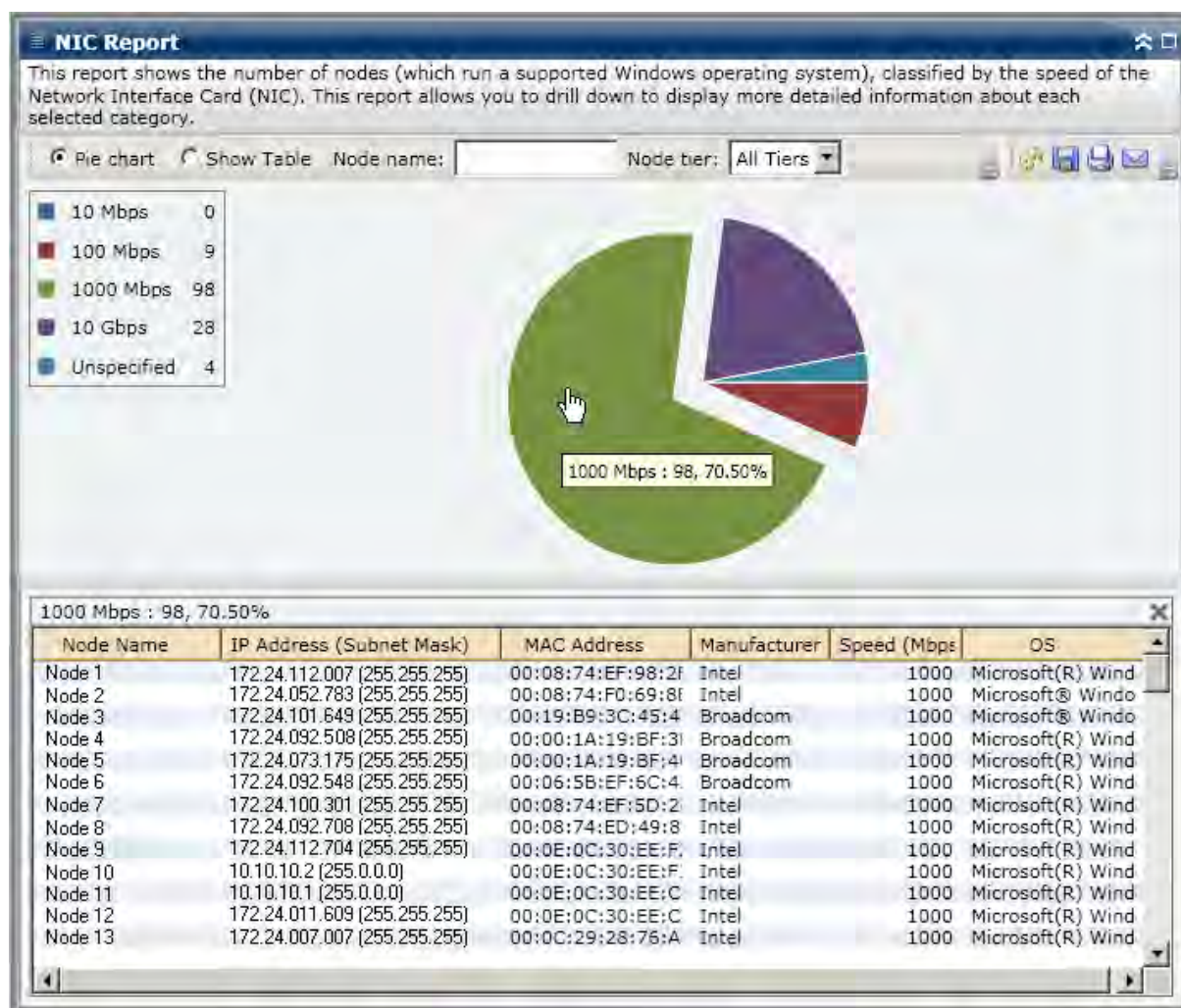
Show Table

If you select Show Table, the NIC Report displays more detailed information in table format listing the Node Name, OS, Manufacturer, Speed, and MAC Address for all of the NIC categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The NIC Report can be further expanded from the Pie chart view to display the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category. Each NIC is displayed on a separate line, even if they are in the same node.



Node Backup Status Report

The Node Backup Status Report lists the most recent status results of all nodes that were backed up during the last specified number of days.

Report Benefits

The Node Backup Status Report is helpful in analyzing and determining which nodes are more effective than others for backup jobs, and which ones could be potential problem areas.

For example, generally you can use this report to check the status of the most recent backup jobs from a node perspective. If the backup status from the previous day is all green (successful), you know that the corresponding node had a good backup. However, if the backup status is red (failed), you can quickly analyze the activity log in the drill-down report to determine the problem area and fix it with minimal delay. You can also monitor the status of nodes on a daily basis to identify any trends in the behavior of node status jobs in your environment.

Always look for patterns in behavior to isolate potential problem nodes and determine if the same nodes are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

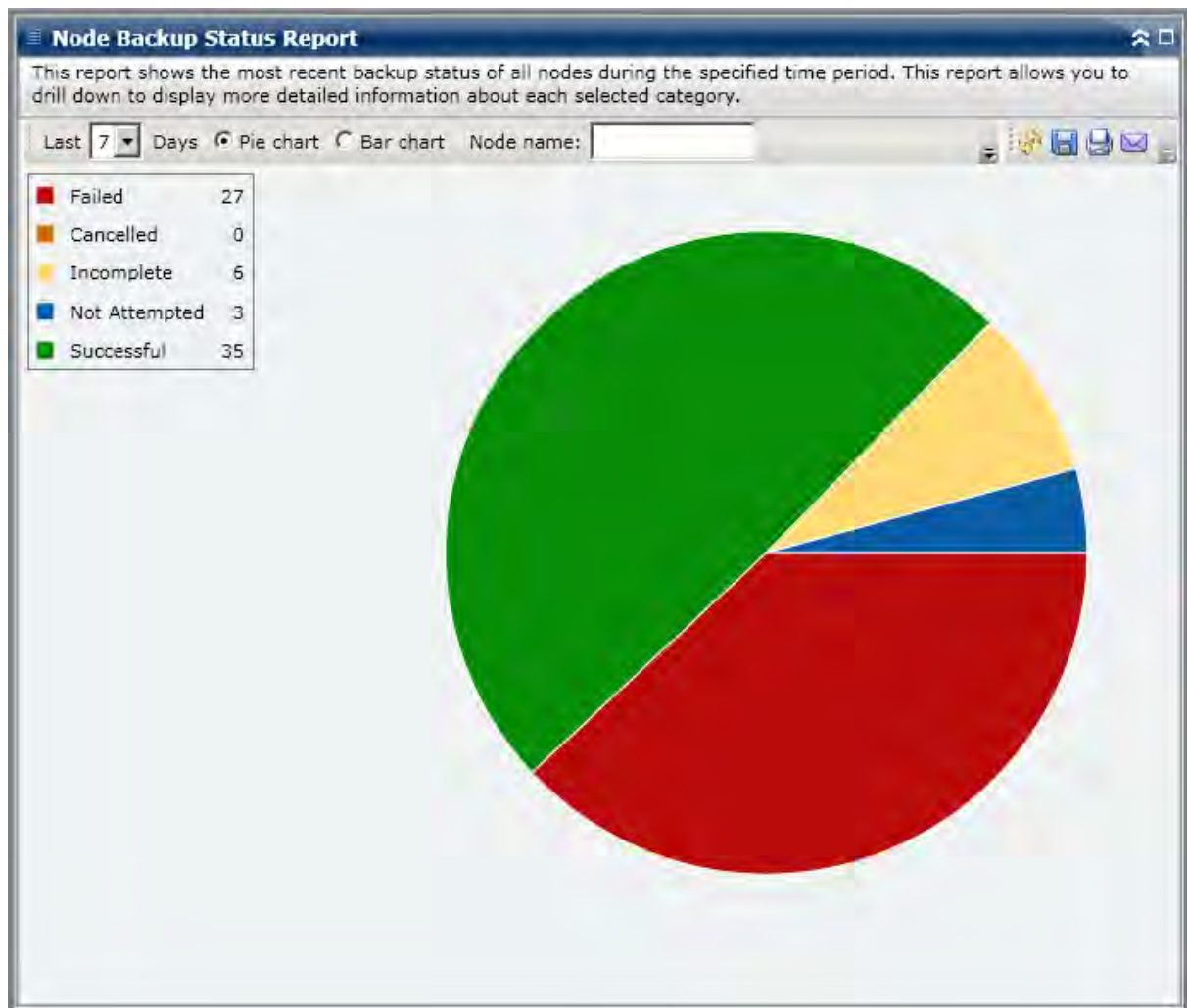
Report View

The Node Backup Status Report can be displayed as either a pie chart or as a bar chart.

Note: By default, CA ARCserve Backup only retains Activity Log information for 14 days. If you want CA ARCserve Backup Dashboard to display Activity Log information for more than 14 days, you must modify the "Prune activity logs older than" option to increase the log retention period. For more information about modifying Activity Log settings, see the Administration Guide.

Pie Chart

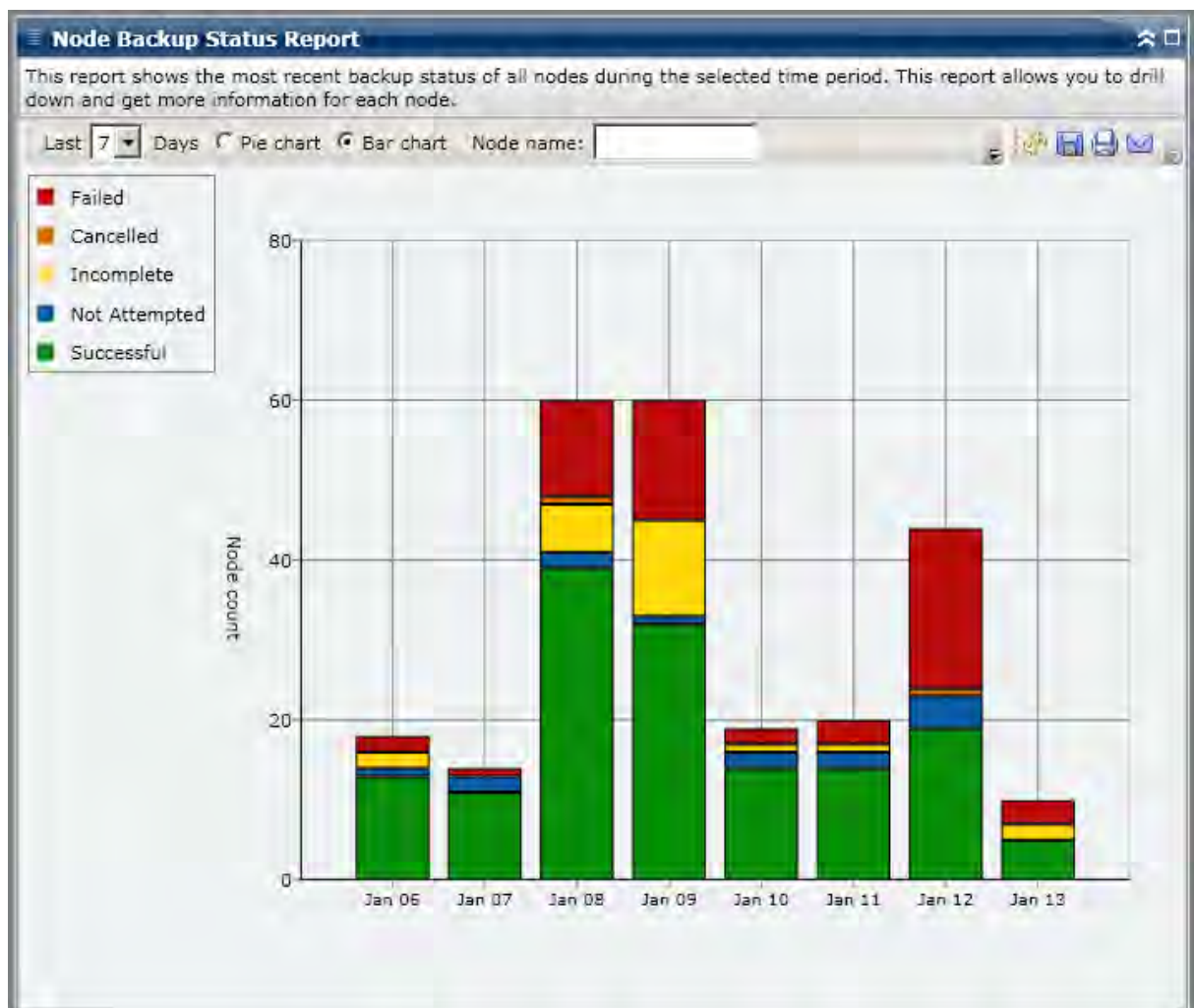
The pie chart provides a high-level overview of nodes that were backed up for all days of the specified time period. The status categories shown in the pie chart represent a percentage of the total number of nodes that were backed up during the last specified number of days, with the most recent backup status being considered for every node.



Bar Chart

The bar chart provides a more detailed level view of the nodes that were backed up for each day of the specified time period. The status categories shown in the bar chart represent the daily number of nodes that were backed up during the last specified number of days.

Note: By default, CA ARCserve Backup Dashboard only displays bar chart information for a maximum of 90 days. Increasing the number of displayed days to more than 90 days would result in the bar chart information not being legible. If you specify to display report information for more than 90 days, the bar chart limits the display to only 90 days, regardless of the number of days entered. This limitation does not apply to pie chart views of the same report. (The maximum number of displayed days for a pie chart is 999 days).

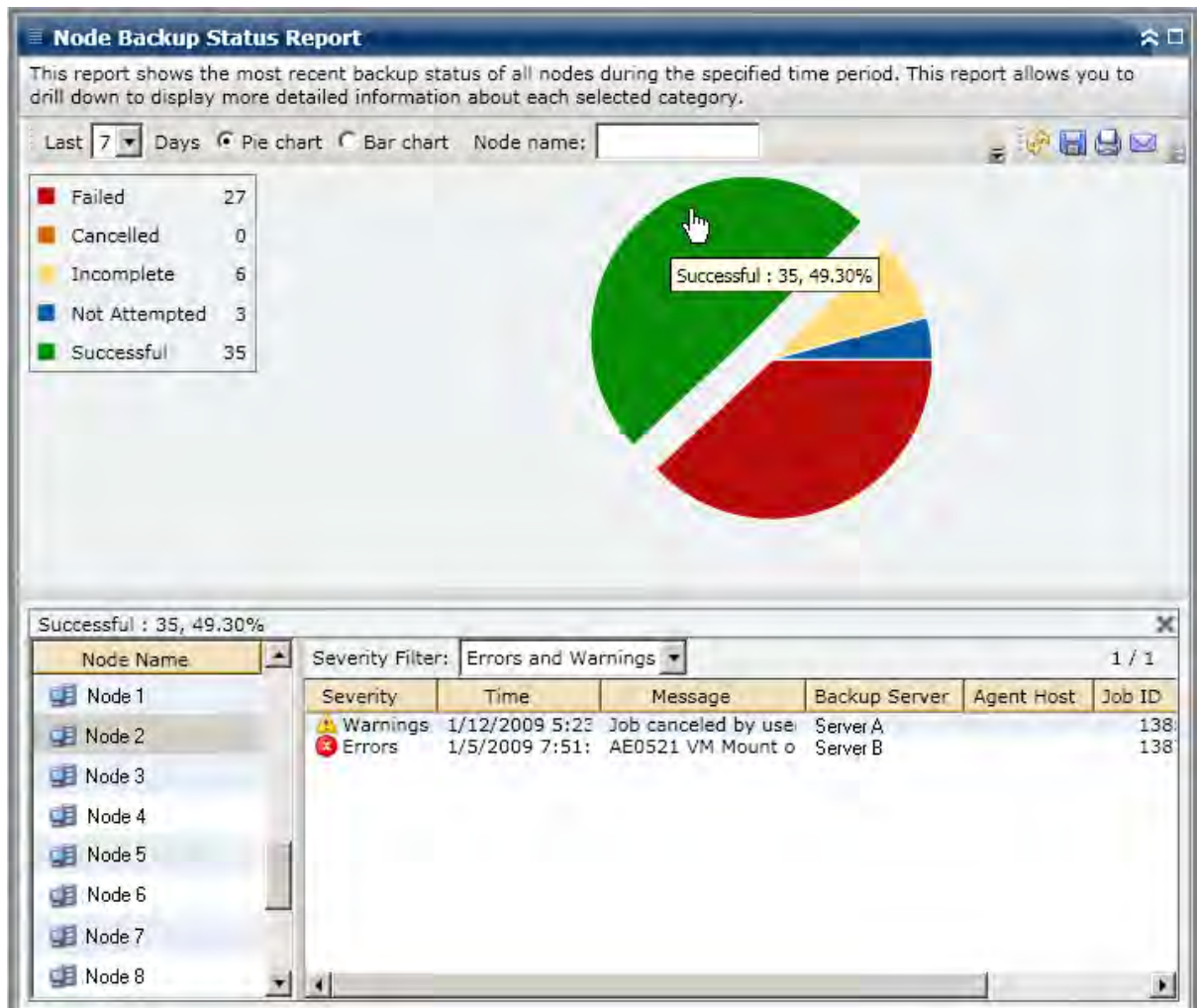


Drill Down Reports

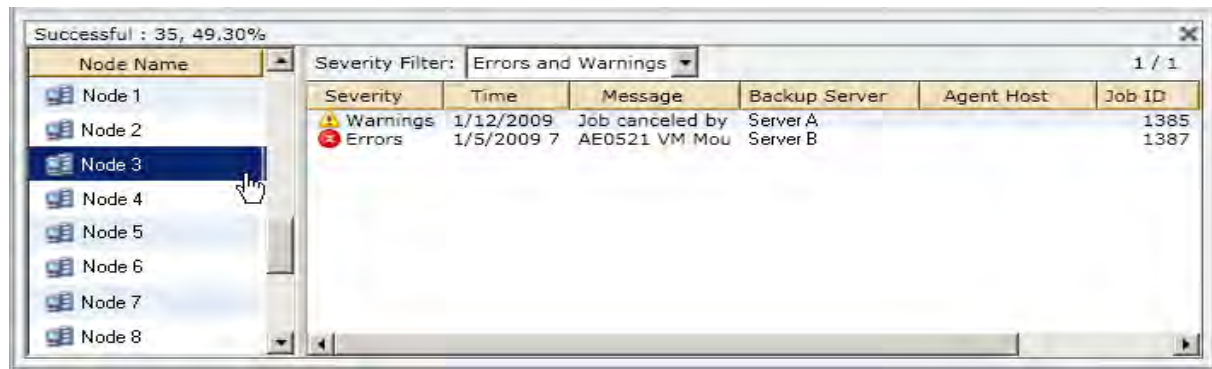
The Node Backup Status Report can be further expanded from the Pie chart view to display more detailed information. You can click on any status category (from either the pie chart view or the bar chart view) to drill down from a report of summary information to a more focused and detailed report about that particular category.

Note: From the bar chart view, you can also drill down to display a filtered list of nodes for a status category on a single day.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



You can then drill down further in this report by clicking on the name of an individual node to display a listing of all log messages associated with that node. You can also filter the list by specifying the severity of the messages displayed (Error & Warning, Error, Warning, Information, or All).



Note: Dashboard uses pagination to display the first 100 log messages. You can click on the Next page button to view further messages.

Note: From this drill down report, you can click on any listed error or warning message to display the related troubleshooting help topic with the corresponding reason and corrective action.

Node Disaster Recovery Status Report

This Node Disaster Recovery Status Report displays the number of nodes that were successfully backed up during the specified time period and which of those nodes contain and do not contain disaster recovery (DR) protected information. The nodes that contain DR protected information can be recovered by using either of the following processes:

- CA ARCserve Backup Disaster Recovery Option
- CA ARCserve Backup Agent for Virtual Machines (to create a full VM image that would then be available for recovery purposes).

The nodes that do not contain DR protected information can have the data restored, but cannot be recovered. The Nodes Disaster Recovery Status Report is helpful in analyzing and determining which nodes are adequately protected for disaster recovery, and which ones could be potential problem areas.

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic events or natural disasters. There are many time consuming tasks, including installation of the base operating systems and setup of the servers, which would usually have to be manually performed after a disaster. The disaster recovery process lets you restore your server reliably, making more efficient use of time by taking you from boot media, to backup media, to an operational state and allows users with minimal server configuration experience to recover sophisticated systems. Disaster recovery is based on the concept of collecting and saving machine-specific information before a disaster strikes.

For more information about the Disaster Recovery Option, see the *Disaster Recovery Option Guide*. For more information about the Agent for Virtual Machines, see the *Agent for Virtual Machines Guide*.

Note: If it is detected that you do not have the CA ARCserve Backup Disaster Recovery Option installed, a warning message is displayed at the top of this report, informing you of this potentially dangerous condition.

 CA ARCserve Backup for Windows Disaster Recovery Option is not installed

Report Benefits

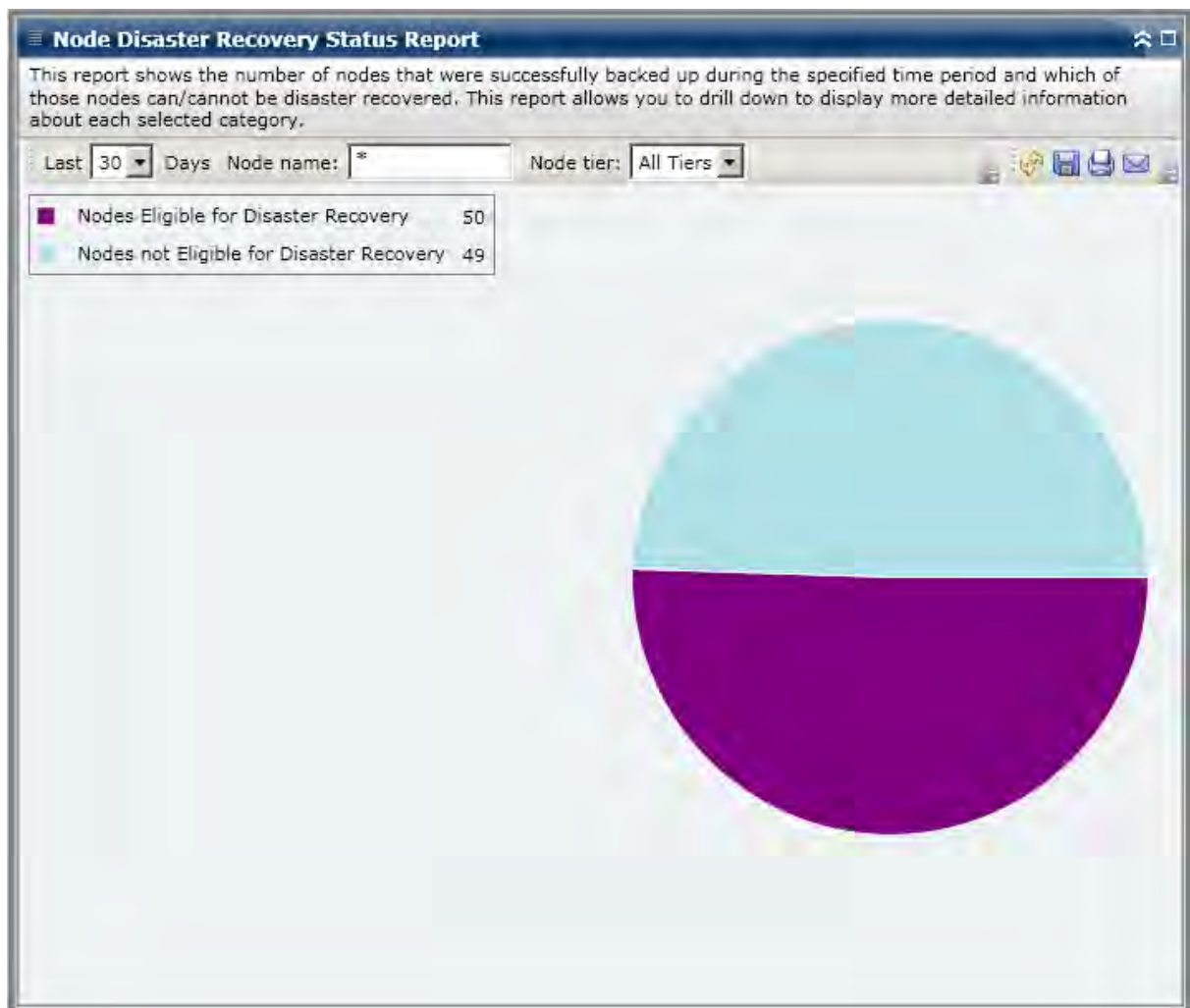
The Nodes Disaster Recovery Status Report is helpful in analyzing and determining which nodes are adequately protected for disaster recovery, and which ones could be potential problem areas.

For example, if from this report you see that some of your more critical or high-priority data is being backed up on a node that does not contain the Disaster Recovery Option, you should first check to see if you have the option installed, but maybe not properly configured to be used. If you find that you do not have this option installed, you should improve your data protection by adding this option before it is too late. If you find from this report that one of your important nodes do not have DR information, you should start running full node backups of that node (including system state) to ensure that the node can be successfully recovered.

Report View

The Node Disaster Recovery Status Report is displayed in a pie chart format, showing the number (and percentage) of nodes that contain disaster recovery (DR) information and the number of nodes that do not contain DR information.

- Nodes Eligible for Disaster Recovery are defined as nodes that have one or more sessions that were backed up and contain DR information during the specified time period.
- Nodes Not Eligible for Disaster Recovery are defined as nodes that do not have any sessions that were backed up and contain DR information during the specified time period.

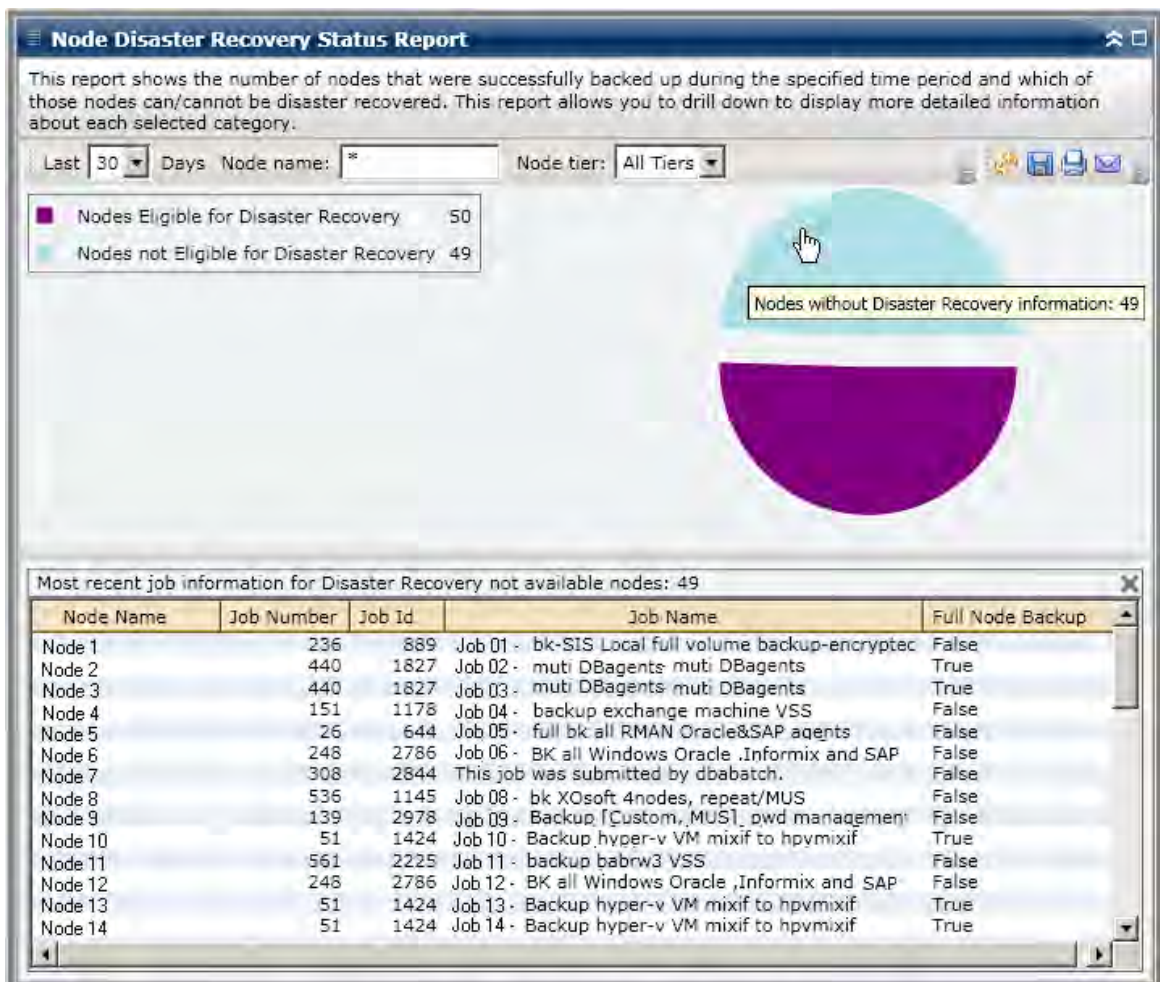


Drill Down Reports

The Node Disaster Recovery Status Report can be further expanded from the Pie chart view to display more detailed information. You can click on either of the two pie chart categories to display a detailed listing of all nodes associated with that category during the specified time period. This drill down report includes the node names, along with the associated DR-related information for each category.

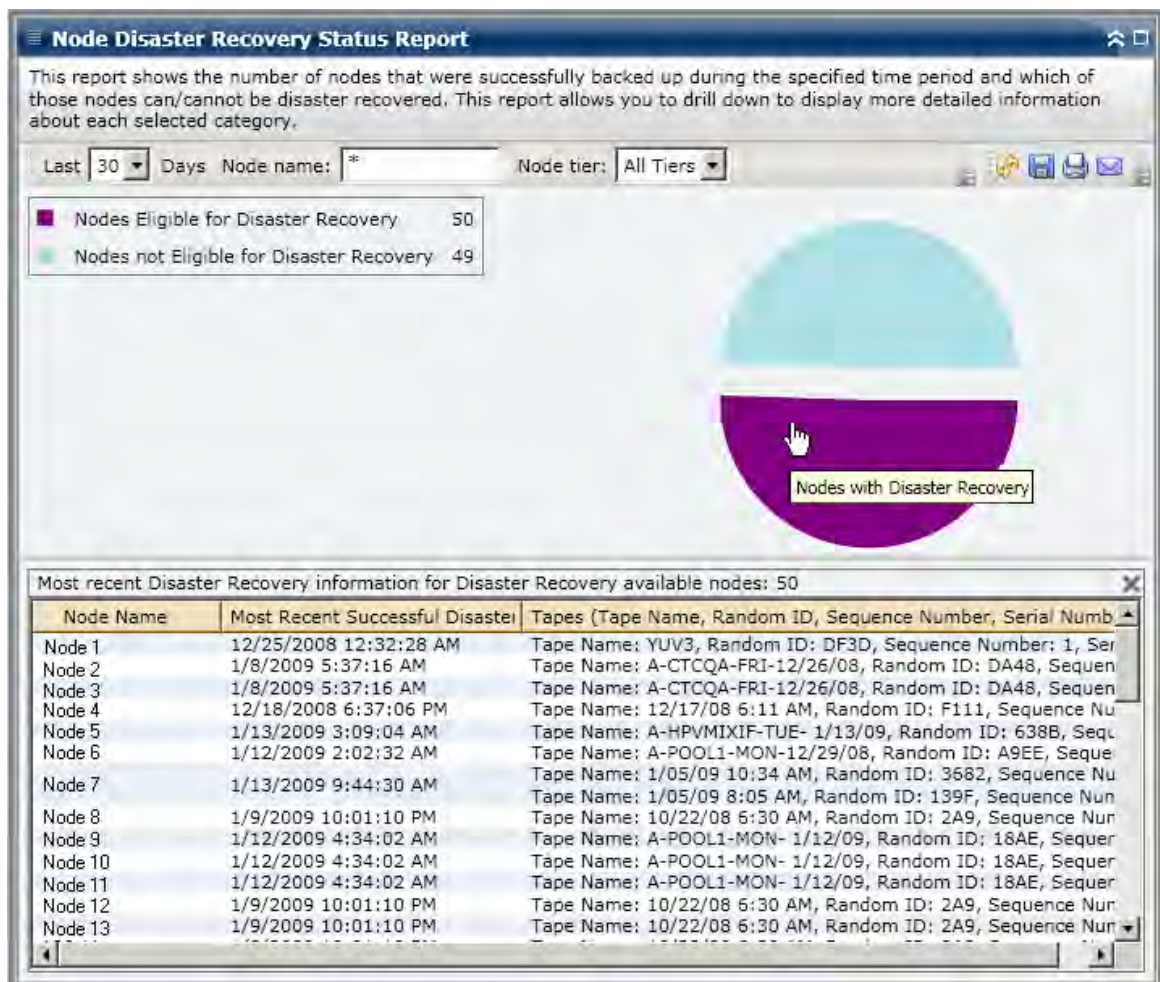
Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

- If you drilled down in the Nodes Not Eligible for Disaster Recovery category the corresponding table also displays the job number for the most recent backup job for that node, the Job name, and whether or not the most recent backup job was a Full backup.



- If you drilled down in the Nodes Eligible for Disaster Recovery category the corresponding table would also display the time and date of the most recent successful DR backup, tape information (name, random ID, sequence number, and serial number), the location of the DR information, and the method used to back up the DR information (backed up by CA ARCserve Backup or replicated by CA ARCserve Backup XOSoft)

Note: For a specific node, if the Node Recovery Points Report indicates that disaster recovery is not available, but the Node Disaster Recovery Status Report indicates that disaster recovery is available for this same node, this is because of a difference in how the information is reported. The Node Recovery Points Report displays the DR information corresponding to the most recent recovery point, while the Node Disaster Recovery Status Report displays the information if there is at least one DR session available within the specified time period.



Node Encryption Status Report

The Node Encryption Report displays the number of nodes that have been backed up to tape with and without encrypted backup sessions during the specified time period. This report can be used to determine if sensitive data on your nodes is properly protected and provides a means to quickly identify and resolve potential problem areas with your backups.

Report Benefits

The Node Encryption Status Report is helpful in analyzing and determining which nodes are adequately protected, and which ones could be potential problem areas. Encryption of data is critical for both security purposes and for your company to remain compliant. The displays in this report can be filtered by the Tier categories assigned to each node, with Tier 1 being your high-priority nodes and Tier 3 being the low-priority nodes. For more information about Node Tier Configuration, see the Administration Guide.

From this report you can quickly determine if you have sensitive data on nodes that are not encrypted and therefore subject to a security risk.

For example, from this report you can easily see if you have any Tier 1 nodes that are not encrypted. If you have non-encrypted Tier 1 nodes that contain sensitive data on them, you immediately know that your data is not being properly protected. You need to re-evaluate your backup strategy before a problem occurs.

Likewise, from this report you can see if you have non-sensitive data on nodes that are being encrypted and therefore not only wasting valuable resources (time and money), but also slowing down your backup efforts.

For example, if from this report you see that you have Tier 3 nodes that do not contain sensitive data but the data is still being encrypted, you should re-evaluate your backup strategy to ensure proper use of resources and time.

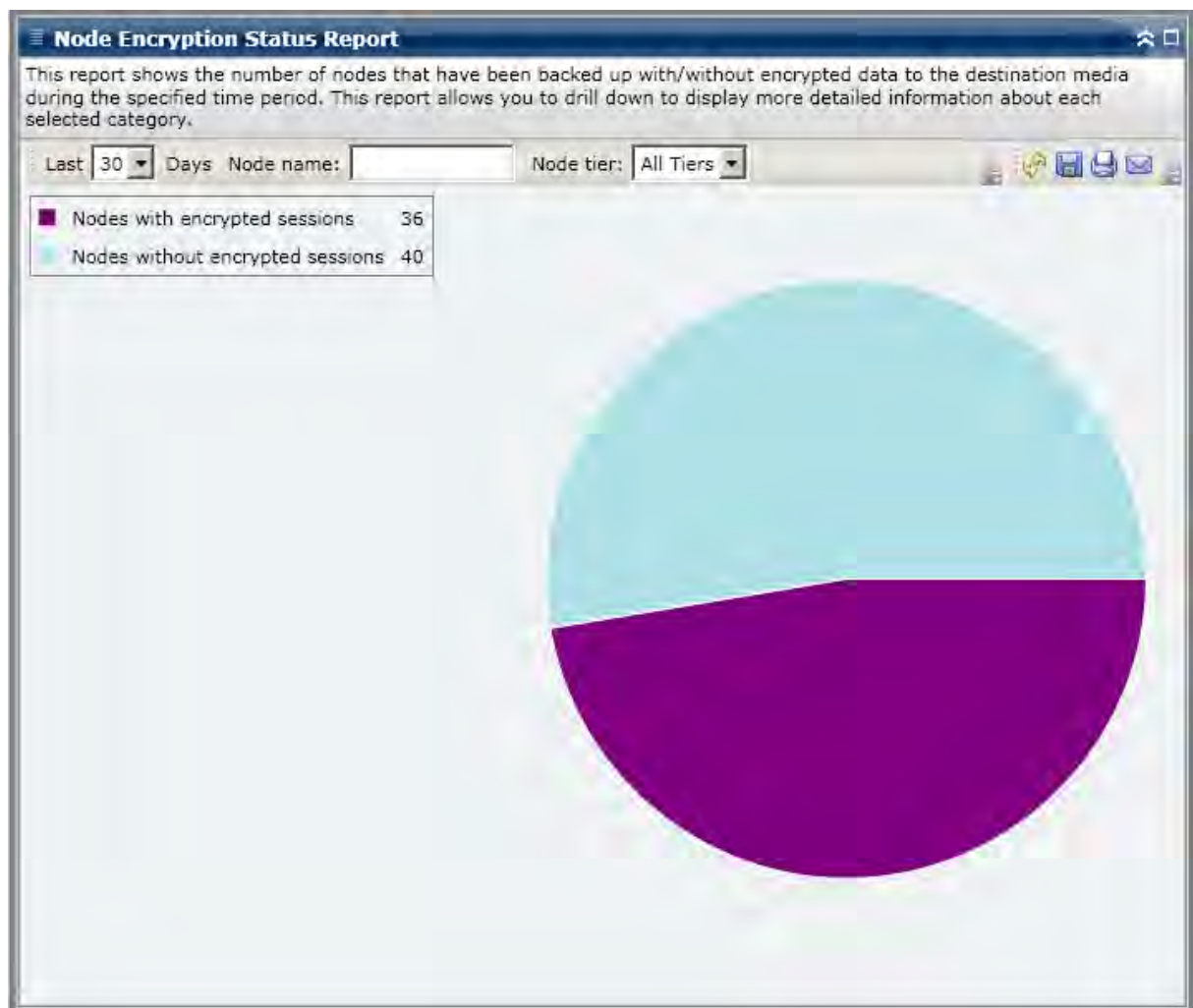
In addition, you can also see if all data on a specific node has been encrypted to ensure both proper security and use of resources.

For example, if within your company Department A has sensitive data on the same node as Department B data which is not sensitive. From this report you can quickly see that not all data on a specific node has been encrypted. You can then research your backup status to determine if the Department A data is encrypted and the Department B data is not, and re-evaluate your backup strategy if necessary.

Report View

The Node Encryption Status Report is displayed in a pie chart format, showing the number (and percentage) of nodes that were backed up and contain encrypted sessions and the number of nodes that were backed up and do not contain encrypted sessions during the specified period of time. The display can be further filtered by Tier categories, with Tier 1 representing high-priority tiers, and Tier 3 representing low-priority nodes.

- Nodes with encrypted sessions are defined as nodes that have one or more encrypted backup sessions during the specified time period.
- Nodes without encrypted sessions are defined as nodes that do not have any encrypted backup sessions during the specified time period.



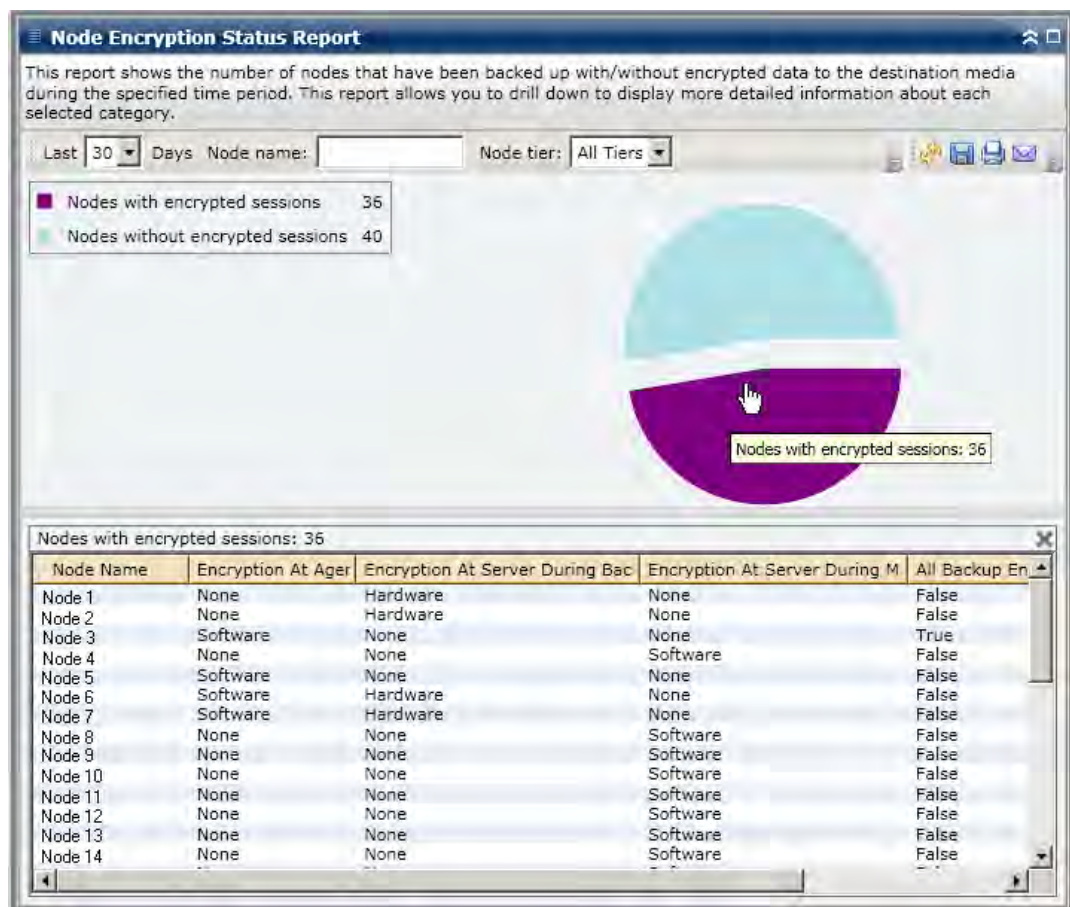
Drill Down Reports

The Node Encryption Status Report can be further expanded in the Pie chart view to display more detailed information. You can click on either of the two categories to display a detailed listing of all nodes associated with that category during the specified time period. This drill-down report includes the Node names, along with the encryption-related information for each category.

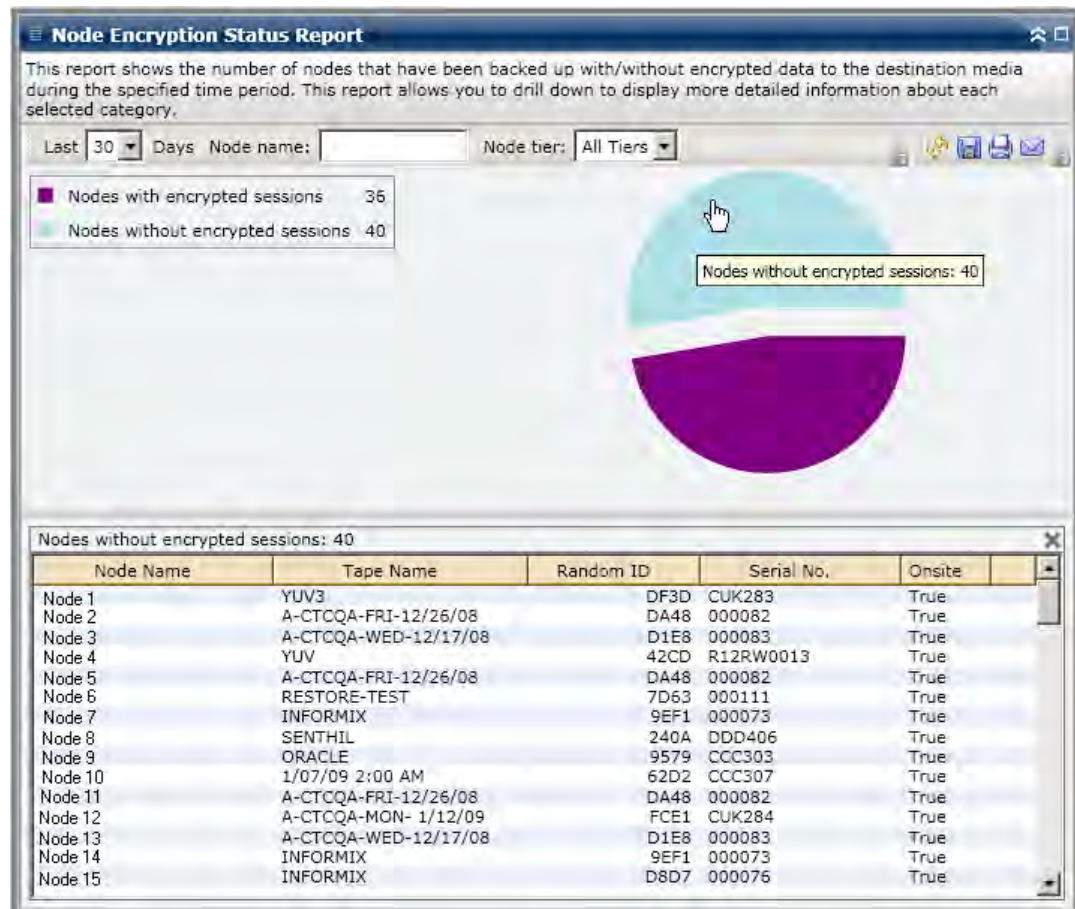
Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

- If you drilled down in the Nodes with Encrypted Sessions category the corresponding table would also display the type of encryption (hardware, software, or none) and the where the encryption occurred (at the agent, at the server during backup, or at the server during migration). In addition this report displays whether or not all backup sessions were encrypted and if an encryption password has been recorded and stored in the CA ARCserve Backup Database.

Note: For more information about the types of data encryption, see the *Administration Guide* or the online help.



- If you drilled down in the Nodes without Encrypted Sessions category the corresponding table also displays the tape name, along with the random ID of the tape and whether or not the tape is located onsite.



Node Recovery Points Report

The Node Recovery Point Report lists the recovery points for each node during the specified time period. A node recovery point means that a node backup was successful or incomplete. For this report, an eligible recovery point is determined by the node status, and not the job status. You can filter this report based on the specified number of recovery points (greater than or less than) for all the nodes.

Report Benefits

The Node Recovery Point Report is helpful in analyzing and determining which nodes are adequately protected for a recovery, and which ones could be potential problem areas. If you find a problem with the number of recovery points for a specific node, look for patterns to determine why not enough or why too many backup recovery points have been taken. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Generally if a specific node contains high-priority data (Tier 1), you would want to ensure that you have enough backup points to enable a quick and complete recovery if necessary.

For example, a node that contains high-priority data should have five recovery points taken to be adequately protected. If from this report, you discover that this specific high-priority node only contains two recovery points, you should investigate the reason, and modify your backup schedule as necessary to ensure proper recovery protection. You can also identify the latest possible time up to which your data can be recovered for each node and whether it is possible to recover each node through the DR option.

Likewise, if a specific node contains low-priority data (Tier 3), you would want to ensure that you do not have too many unnecessary backup points.

For example, a node that contains low-priority data should generally have two recovery points taken to be adequately protected. If from this report, you discover that this specific low-priority node contains five recovery points, you should investigate the reason, and modify your backup schedule to ensure you are not wasting valuable resources and time.

A good practice is to review this report in conjunction with the Media Assurance Report to make sure you not only have adequate recovery points, but also assure the data is guaranteed good to restore.

Report View

The Node Recovery Point Report is displayed in a table format, listing all nodes with more or less than the specified number of recovery points that are available from the specified time period. The report lists the Node names, along with the corresponding number of recovery points, the time of the most recent recovery point, the type of recovery protected (full or partial), and whether or not disaster recovery (DR) is available.

The availability of Disaster Recovery is based upon whether or not the CA ARCserve Backup Disaster Recovery Option is installed and licensed on the Primary Server and if so, whether or not the option is selected for use during backup. To determine if a specific node is properly protected with the CA ARCserve Backup Disaster Recovery Option, you can use the [Node Disaster Recovery Status Report](#) (see page 89).

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Node Name	Num of Recovery Point	Most Recent Recovery Point	Full or Partial Protected	Disaster Recovery Availa
Node 1	2	12/25/2008 12:32:28 AM	Full	YES
Node 2	4	1/8/2009 5:37:16 AM	Full	NO
Node 3	2	1/9/2009 1:10:32 AM	Partial	NO
Node 4	2	12/29/2008 4:18:00 AM	Partial	NO
Node 5	3	12/22/2008 1:03:30 AM	Partial	NO
Node 6	3	12/29/2008 12:53:26 AM	Partial	NO
Node 7	1	1/13/2009 3:09:04 AM	Full	YES
Node 8	4	1/9/2009 10:01:10 PM	Full	YES
Node 9	3	1/9/2009 10:01:10 PM	Full	YES
Node 10	3	1/9/2009 10:01:10 PM	Full	YES
Node 11	3	1/9/2009 10:01:10 PM	Full	YES
Node 12	1	1/9/2009 10:59:02 AM	Full	NO
Node 13	1	12/17/2008 12:30:58 PM	Full	YES
Node 14	4	1/9/2009 10:01:10 PM	Partial	NO
Node 15	1	1/13/2009 12:01:42 AM	Partial	NO
Node 16	1	1/9/2009 10:01:10 PM	Full	NO
Node 17	3	1/2/2009 9:40:16 AM	Full	YES
Node 18	1	12/30/2008 9:42:36 AM	Full	YES
Node 19	1	1/2/2009 9:40:16 AM	Full	YES
Node 20	1	12/30/2008 9:42:36 AM	Full	YES
Node 21	2	1/2/2009 9:40:16 AM	Full	YES
Node 22	2	1/2/2009 9:40:16 AM	Full	YES
Node 23	1	1/2/2009 9:40:16 AM	Full	YES
Node 24	1	12/30/2008 9:42:36 AM	Full	YES
Node 25	2	1/2/2009 9:40:16 AM	Full	YES
Node 26	4	12/18/2008 1:34:54 PM	Partial	NO
Node 27	3	12/18/2008 1:34:54 PM	Partial	NO
Node 28	3	12/29/2008 12:53:26 AM	Partial	NO
Node 29	1	1/12/2009 7:07:52 PM	Partial	NO
Node 30	3	1/8/2009 5:37:16 AM	Partial	NO

Drill Down Reports

The Node Recovery Point Report can be further expanded to display more detailed information. You can click on any of the listed nodes to display a detailed listing of all available recovery points for the corresponding node during the specified time period. You can then click on any of the listed recovery points to display an additional detailed listing of all sessions corresponding to that recovery point.

Note: A recovery point is determined based on the last successful execution start time of the backup job for a node.

Note: For a specific node, if the Node Recovery Points Report indicates that disaster recovery is not available, but the Node Disaster Recovery Status Report indicates that disaster recovery is available for this same node, this is because of a difference in how the information is reported. The Node Recovery Points Report displays the DR information corresponding to the most recent recovery point, while the Node Disaster Recovery Status Report displays the information if there is at least one DR session available within the specified time period.

Node Recovery Points Report

This report shows the recovery/restore information for nodes that were backed up during the specified time period. This report allows you to drill down to display more detailed information about each selected node.

Last: 30 Days Recovery Point Num: 5 Node name:

Node Name	Num of Recovery Point	Most Recent Recovery Point	Full or Partial Protected	Disaster Recovery Available
Node 1	2	12/25/2008 12:32:28 AM	Full	YES
Node 2	4	1/8/2009 5:37:16 AM	Full	NO
Node 3	2	1/9/2009 1:10:32 AM	Partial	NO
Node 4	2	12/29/2008 4:18:00 AM	Partial	NO
Node 5	3	12/22/2008 1:03:30 AM	Partial	NO
Node 6	3	12/29/2008 12:53:26 AM	Partial	NO
Node 7	1	1/13/2009 3:09:04 AM	Full	YES
Node 8	4	1/9/2009 10:01:10 PM	Full	YES
Node 9	3	1/9/2009 10:01:10 PM	Full	YES
Node 10	3	1/9/2009 10:01:10 PM	Full	YES
Node 11	3	1/9/2009 10:01:10 PM	Full	YES
Node 12	1	1/9/2009 10:59:02 AM	Full	NO
Node 13	1	12/17/2008 12:30:58 PM	Full	YES
Node 14	4	1/9/2009 10:01:10 PM	Partial	NO
Node 15	1	1/13/2009 12:01:42 AM	Partial	NO
Node 16	1	1/9/2009 10:01:10 PM	Full	NO

Recovery Points for Node: Node 1, Count: 2

Recovery Point	Root Path	Status	Data Size (KB)	Execute Time	Session Number
12/25/2008 12:32:28 AM	C:	Incomplete	2920432	12/25/2008 12:33:42 AM	4
12/24/2008 12:32:20 AM	System State	Finished	551210	12/25/2008 12:39:34 AM	5

Node Summary Report

The Node Summary Report is an SRM-type report that displays a summary listing of all Windows nodes that are being backed up. This report provides an overall view of all the nodes in your environment.

Report Benefits

The Node Summary Report displays an overall view of all nodes in your environment. You can use this data to analyze and determine which nodes are more effective than others for backup jobs, and which ones could be potential problem areas.

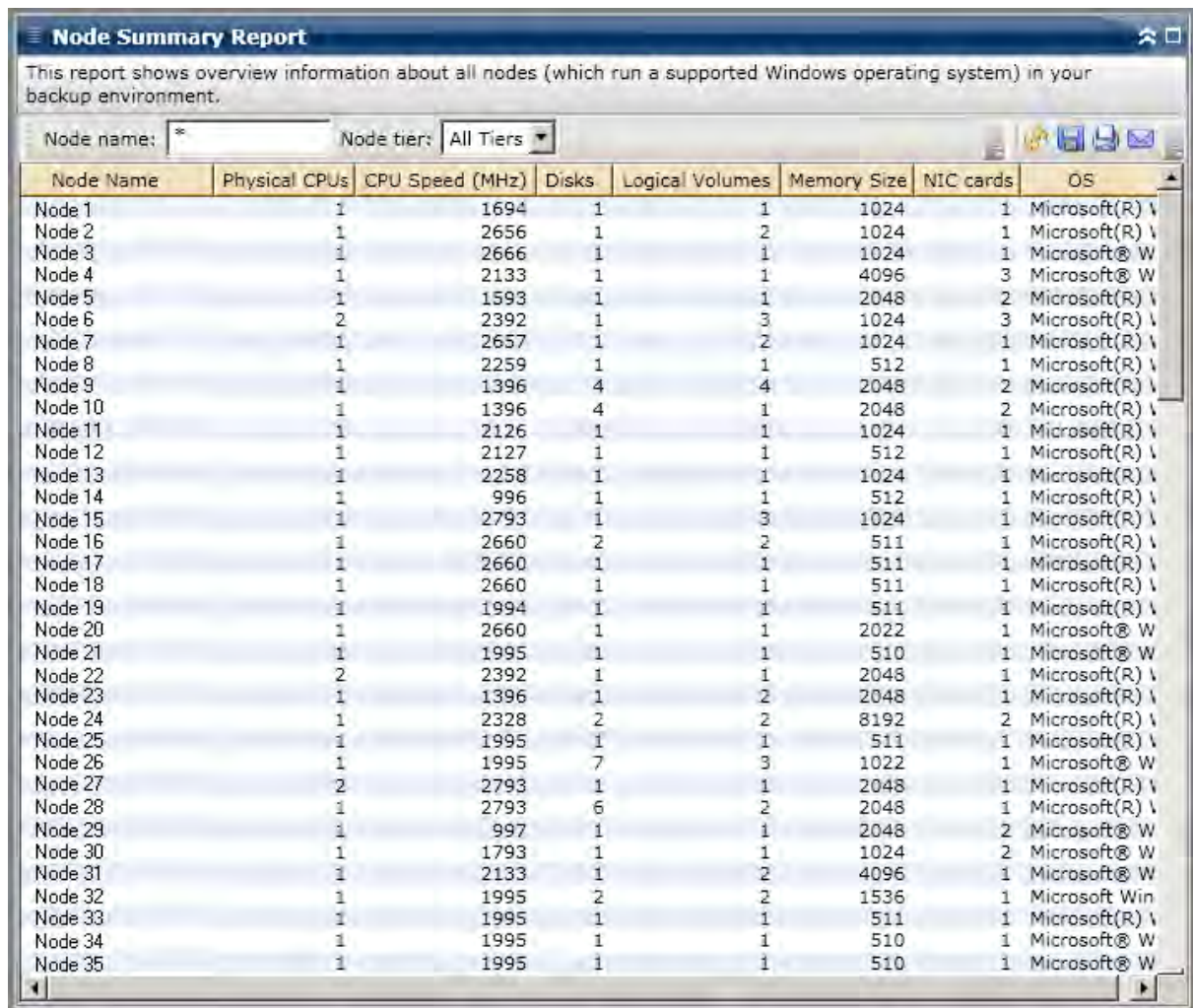
For example, if you find that a particular node has a slower throughput value, you can look in this report for patterns in behavior among the slower nodes. You can use the fastest throughput values as reference points to analyze why these nodes are performing well. You can compare the slower nodes to the faster nodes to determine if you actually have a problem or if both sets of values are similar, maybe the slower nodes are not performing poorly.

Always look for patterns in behavior to isolate potential problem nodes and determine if the same nodes are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Node Summary Report is displayed in table format listing Node Name, Physical CPUs, CPU Speed, Disks, Logical Volumes, Memory Size, NIC Cards and OS. You can filter the data displayed by specifying the Node name or selecting the Node tier from the drop-down menu.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



The screenshot shows a window titled "Node Summary Report" with a description: "This report shows overview information about all nodes (which run a supported Windows operating system) in your backup environment." Below the description are filters for "Node name" (set to "*") and "Node tier" (set to "All Tiers"). The main content is a table with 8 columns: Node Name, Physical CPUs, CPU Speed (MHz), Disks, Logical Volumes, Memory Size, NIC cards, and OS. The table lists 35 nodes, each with its respective hardware and software details.

Node Name	Physical CPUs	CPU Speed (MHz)	Disks	Logical Volumes	Memory Size	NIC cards	OS
Node 1	1	1694	1	1	1024	1	Microsoft(R) W
Node 2	1	2656	1	2	1024	1	Microsoft(R) W
Node 3	1	2666	1	1	1024	1	Microsoft® W
Node 4	1	2133	1	1	4096	3	Microsoft® W
Node 5	1	1593	1	1	2048	2	Microsoft(R) W
Node 6	2	2392	1	3	1024	3	Microsoft(R) W
Node 7	1	2657	1	2	1024	1	Microsoft(R) W
Node 8	1	2259	1	1	512	1	Microsoft(R) W
Node 9	1	1396	4	4	2048	2	Microsoft(R) W
Node 10	1	1396	4	1	2048	2	Microsoft(R) W
Node 11	1	2126	1	1	1024	1	Microsoft(R) W
Node 12	1	2127	1	1	512	1	Microsoft(R) W
Node 13	1	2258	1	1	1024	1	Microsoft(R) W
Node 14	1	996	1	1	512	1	Microsoft(R) W
Node 15	1	2793	1	3	1024	1	Microsoft(R) W
Node 16	1	2660	2	2	511	1	Microsoft(R) W
Node 17	1	2660	1	1	511	1	Microsoft(R) W
Node 18	1	2660	1	1	511	1	Microsoft(R) W
Node 19	1	1994	1	1	511	1	Microsoft(R) W
Node 20	1	2660	1	1	2022	1	Microsoft® W
Node 21	1	1995	1	1	510	1	Microsoft® W
Node 22	2	2392	1	1	2048	1	Microsoft(R) W
Node 23	1	1396	1	2	2048	1	Microsoft(R) W
Node 24	1	2328	2	2	8192	2	Microsoft(R) W
Node 25	1	1995	1	1	511	1	Microsoft(R) W
Node 26	1	1995	7	3	1022	1	Microsoft® W
Node 27	2	2793	1	1	2048	1	Microsoft(R) W
Node 28	1	2793	6	2	2048	1	Microsoft(R) W
Node 29	1	997	1	1	2048	2	Microsoft® W
Node 30	1	1793	1	1	1024	2	Microsoft® W
Node 31	1	2133	1	2	4096	1	Microsoft® W
Node 32	1	1995	2	2	1536	1	Microsoft Win
Node 33	1	1995	1	1	511	1	Microsoft(R) W
Node 34	1	1995	1	1	510	1	Microsoft® W
Node 35	1	1995	1	1	510	1	Microsoft® W

Node Tiers Report

The Node Tiers Report displays the number of nodes for each priority tier. The node tiers are configured with Tier 1 representing high-priority nodes and Tier 3 representing low-priority tiers. By default, Tier 1 is automatically configured to include all CA ARCserve Backup servers (Primary and Member) and any nodes with CA ARCserve Backup application agents installed (such as Oracle, Microsoft Exchange, Microsoft SQL Server, Microsoft Sharepoint, etc.), and Tier 3 is configured to include all other nodes (having file system agents). (By default, Tier 2 is not configured to include any nodes, and is available for customized use).

The node assignments for each tier can be reconfigured and customized to meet your individual needs by using the Node Tier Configuration dialog, which is accessed from the CA ARCserve Backup Server Admin or from the Backup Manager

Note: For more information about Node Tier Configuration, see the *Administration Guide* or the online help.

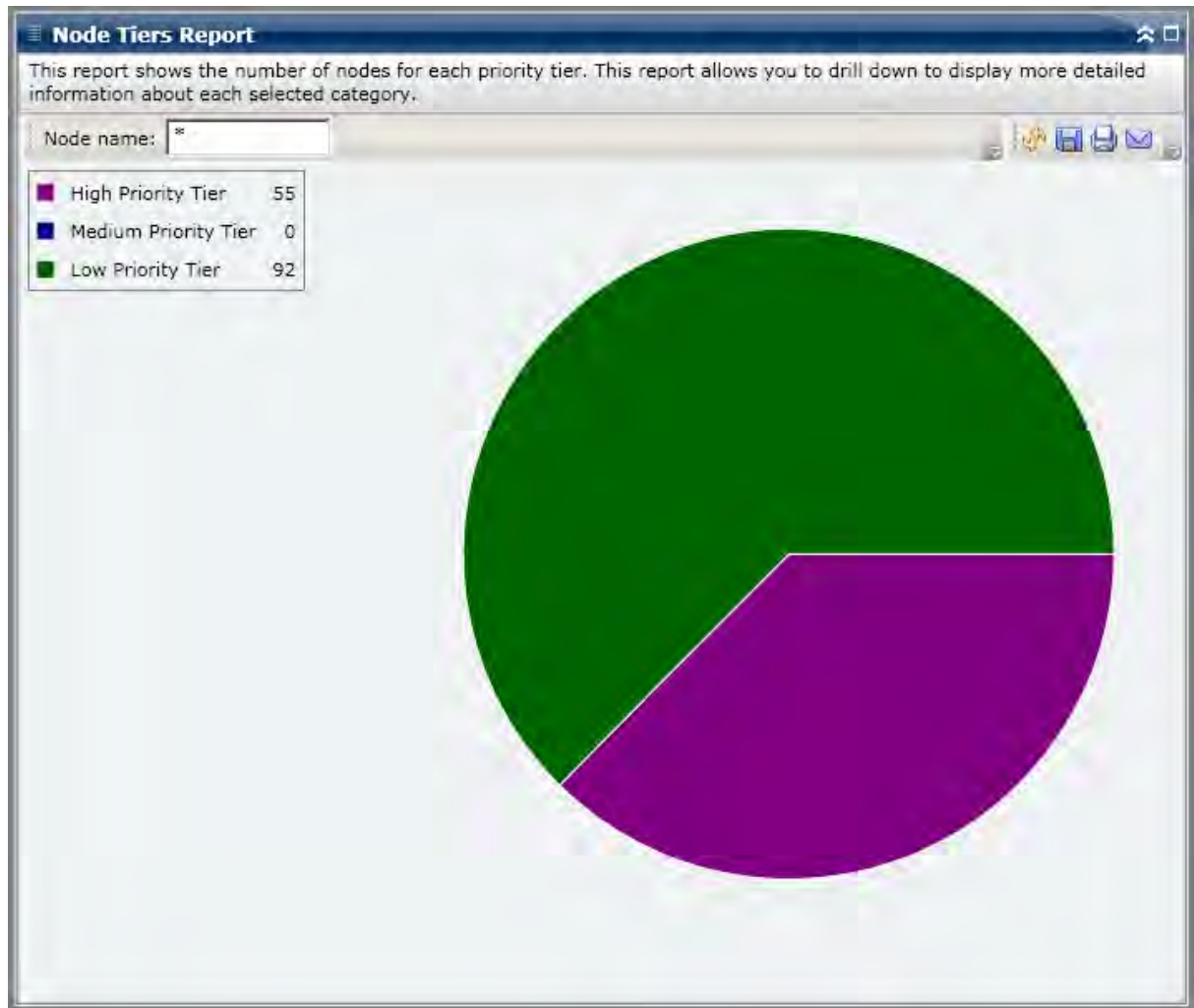
Report Benefits

The Node Tiers Report can be used to quickly identify which nodes are included in each priority tier and help you to ensure that all your nodes are adequately protected.

For example, if you know that a specific node contains high-priority data, but from this report you see that the node is included in the Tier 3 category, you should then use the CA ARCserve Backup Server Admin or CA ARCserve Backup Manager to reassign that node into the Tier 1 category.

Report View

The Node Tiers Report is displayed in a pie chart format, showing the node count for each priority tier.



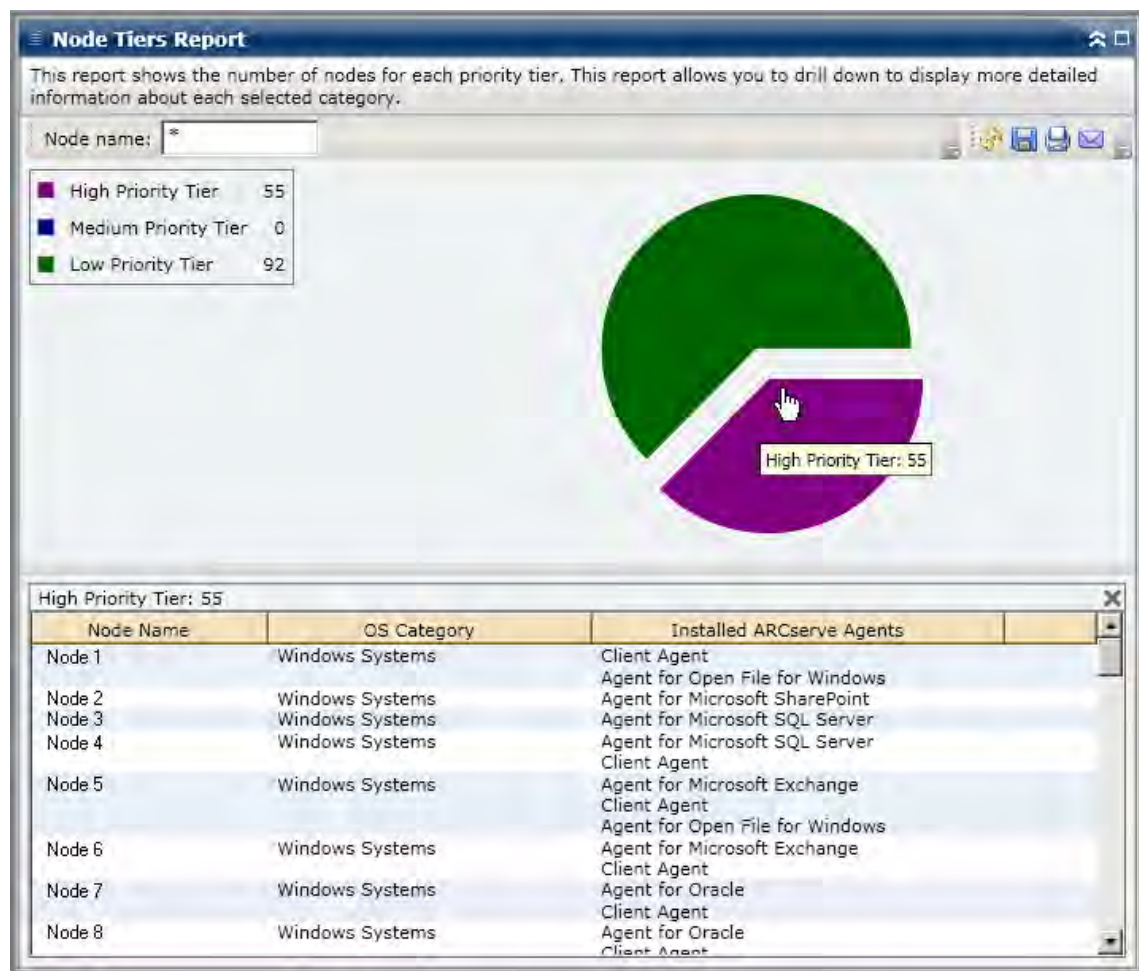
Drill Down Reports

The Node Tiers Report can be further expanded from the Pie chart view to display more detailed information. You can click the pie chart to drill down in the node list for a specific tier as a table with the following columns: Node Name, OS Category, and Installed ARCserve Agents.

The OS Category column would include only the supported node categories that are displayed in the source tree for the Backup Manager. The OS categories that will be displayed in this column are NAS Servers, Mac OS X Systems, UNIX/Linux Systems, Windows Systems, CA XOssoft Scenarios, VMware VCB Systems, and Microsoft Hyper-V Systems.

The Installed ARCserve Agents column would include all the CA ARCserve Backup Agents installed on that node.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



Node Whose Most Recent Backup Failed Report

The Node Whose Most Recent Backup Failed Report contains a listing of the nodes for which the last or most recent backup attempt failed during the specified time period. This report can be used to determine if your data is being properly protected and provide a means to quickly identify and resolve potential problem areas with your backups. Ideally, there should be no nodes listed at all to indicate that all backup attempts were successful.

Report Benefits

The Node Whose Most Recent Backup Failed Report is helpful in analyzing and determining which nodes that are configured for scheduled backups are adequately protected, and which ones could be potential problem areas. If you find a problem with recent backup failures for a specific node, look to determine if the date of the most recent backup failure indicates that protection of your data is at risk.

For example, if you have a node with scheduled backup jobs set for Daily incremental, Weekly full, and Monthly full backups and from this report you see that the most recent Weekly or Monthly backup job failed, then this is an indication that your data is not properly protected since you do not have a currently successful backup. However, if you see that the most recent failure occurred for a Daily backup and the number of days since your last successful backup is low, then it is an indication that your data is not protected on a daily basis, but you probably still have last week's full backup available to recover your data up to that point of time.

If necessary, you can drill down to view the Activity Log and scroll through the pages to obtain more information about each node and each job. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Node Whose Most Recent Backup Failed Report is displayed in a table format, listing all nodes whose most recent backup attempt failed during the specified time period. The report displays the Node names, along with the time of the most recent failed backup attempt, the throughput (speed) of the node, the number of failed attempts during the specified time period, the number of days since the last successful backup, and the related job information (name, ID, and status).

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

In addition, this report also displays the status of any associated makeup job. The makeup job status can be Created, Not Created, Active, and Finished.

- **Created** - A makeup job has been created and is ready in the job queue, but has not been run yet.
- **Not Created** - After the initial backup job failed, there was no attempt to create a makeup job. You should verify that the job was properly configured to create a makeup job in case of failure.
- **Active** - A makeup job has been created and is running. The status of the makeup job is unknown yet.
- **Finished** - After the initial backup job failed, the makeup job has been completed and is finished running.

Node Whose Most Recent Backup Failed Report						
This report shows the nodes whose most recent backup status is failed during the specified time period. This report allows you to drill down to display more detailed information about each selected node.						
Last	30	Days	Node name:		Node tier:	All Tiers
Node Name	Failure Time	Failed Count	Days since last successf	Job Name	Job ID	Makeup Job
Node 1	1/8/2009 5:37:16 AM	4	No successful backup	Job 01	1827	Created
Node 2	1/12/2009 12:53:32 AM	7	15	Job 02	2753	Created
Node 3	1/7/2009 1:16:10 PM	6	12	Job 03	1677	Created
Node 4	1/13/2009 4:34:06 AM	20	1	Job 04	2969	Created
Node 5	1/13/2009 4:34:06 AM	3	1	Job 05	2969	Created
Node 6	1/9/2009 10:01:10 PM	1	4	Job 06	2379	Created
Node 7	1/9/2009 10:01:10 PM	4	5	Job 07	2379	Created
Node 8	1/12/2009 5:33:52 PM	4	4	Job 08	1385	Done
Node 9	1/12/2009 5:33:52 PM	7	14	Job 09	1385	Done
Node 10	1/12/2009 5:33:52 PM	8	4	Job 10	1385	Done
Node 11	1/12/2009 5:33:52 PM	5	9	Job 11	1385	Done
Node 12	1/12/2009 5:33:52 PM	2	9	Job 12	1385	Done
Node 13	1/12/2009 5:33:52 PM	7	14	Job 13	1385	Done
Node 14	1/12/2009 5:33:52 PM	5	No successful backup	Job 14	1385	Done
Node 15	1/12/2009 5:33:52 PM	13	14	Job 15	1385	Done
Node 16	1/12/2009 5:33:52 PM	6	11	Job 16	1385	Done

Drill Down Reports

The Node Whose Most Recent Backup Failed Report can be further expanded to display more detailed information. You can click on any of the listed nodes to display a detailed listing of all jobs for that selected node. You can filter the displayed information by the severity level. This drill-down report includes the information about the failed node (backup server, agent host, job ID, and session number) and the condition associated with the failure (time of failure and corresponding message).

Note: Dashboard uses pagination to display the first 100 log messages. You can click on the Next page button to view further messages.

Note: From this drill down report, you can click on any listed error or warning message to display the related troubleshooting help topic with the corresponding reason and corrective action.

Node Whose Most Recent Backup Failed Report

This report shows the nodes whose most recent backup status is failed during the specified time period. This report allows you to drill down to display more detailed information about each selected node.

Last: 30 Days Node name: Node tier: All Tiers

Node Name	Failure Time	Failed Count	Days since last success	Job Name	Job ID	Makeup J
Node 1	1/8/2009 5:37:16 AM	4	No successful backup	Job 01	1827	Created
Node 2	1/12/2009 12:53:32 AM	7	15	Job 02	2753	Created
Node 3	1/7/2009 1:16:10 PM	6	12	Job 03	1677	Created
Node 4	1/13/2009 4:34:06 AM	20	1	Job 04	2969	Created
Node 5	1/13/2009 4:34:06 AM	3	1	Job 05	2969	Created
Node 6	1/9/2009 10:01:10 PM	1	4	Job 06	2379	Created
Node 7	1/9/2009 10:01:10 PM	4	5	Job 07	2379	Created
Node 8	1/12/2009 5:33:52 PM	4	4	Job 08	1385	Done
Node 9	1/12/2009 5:33:52 PM	7	14	Job 09	1385	Done
Node 10	1/12/2009 5:33:52 PM	8	4	Job 10	1385	Done
Node 11	1/12/2009 5:33:52 PM	5	9	Job 11	1385	Done
Node 12	1/12/2009 5:33:52 PM	2	9	Job 12	1385	Done
Node 13	1/12/2009 5:33:52 PM	7	14	Job 13	1385	Done
Node 14	1/12/2009 5:33:52 PM	5	No successful backup	Job 14	1385	Done
Node 15	1/12/2009 5:33:52 PM	13	14	Job 15	1385	Done
Node 16	1/12/2009 5:33:52 PM	6	11	Job 16	1385	Done

Node 1

Severity Filter: Errors and Warnings 1 / 1

Severity	Time	Message
Error	1/8/2009 6:12:15 AM	AE9971 Get the Backup Component Farm\SharedServices1 Information Failed. Plei
Warning	1/8/2009 5:57:39 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft
Warning	1/8/2009 5:57:38 AM	AW0004 <100-362-2K8X64> Failed to open file <C:\Program Files (x86)\Microsoft

OS Report

The OS Report is an SRM-type report that displays the supported Operating System information for all Windows nodes within your CA ARCserve Backup Domain. You can filter this report to display which selected Operating System information you want to classify the nodes by.

Report Benefits

The OS Report is helpful in quickly classifying machines based on the operating system. You can get an overall view to analyze and determine which operating system is most effective for backup jobs, and which ones could be potential problem areas.

For example, you can correlate this report with the Top Nodes with Fastest/Slowest Backup Throughput Report and identify if a node has slow throughput possibly because of a recent Service Pack applied on the node's operating system. You can also use this report to identify the version and Service Pack level of the operating systems for the nodes in your environment. You can then use this information to apply the latest patches or upgrades to the operating system for the nodes in your environment. You can also use this report to obtain information about the installation directory of your operating system as well as the language of operating systems in a localized backup environment.

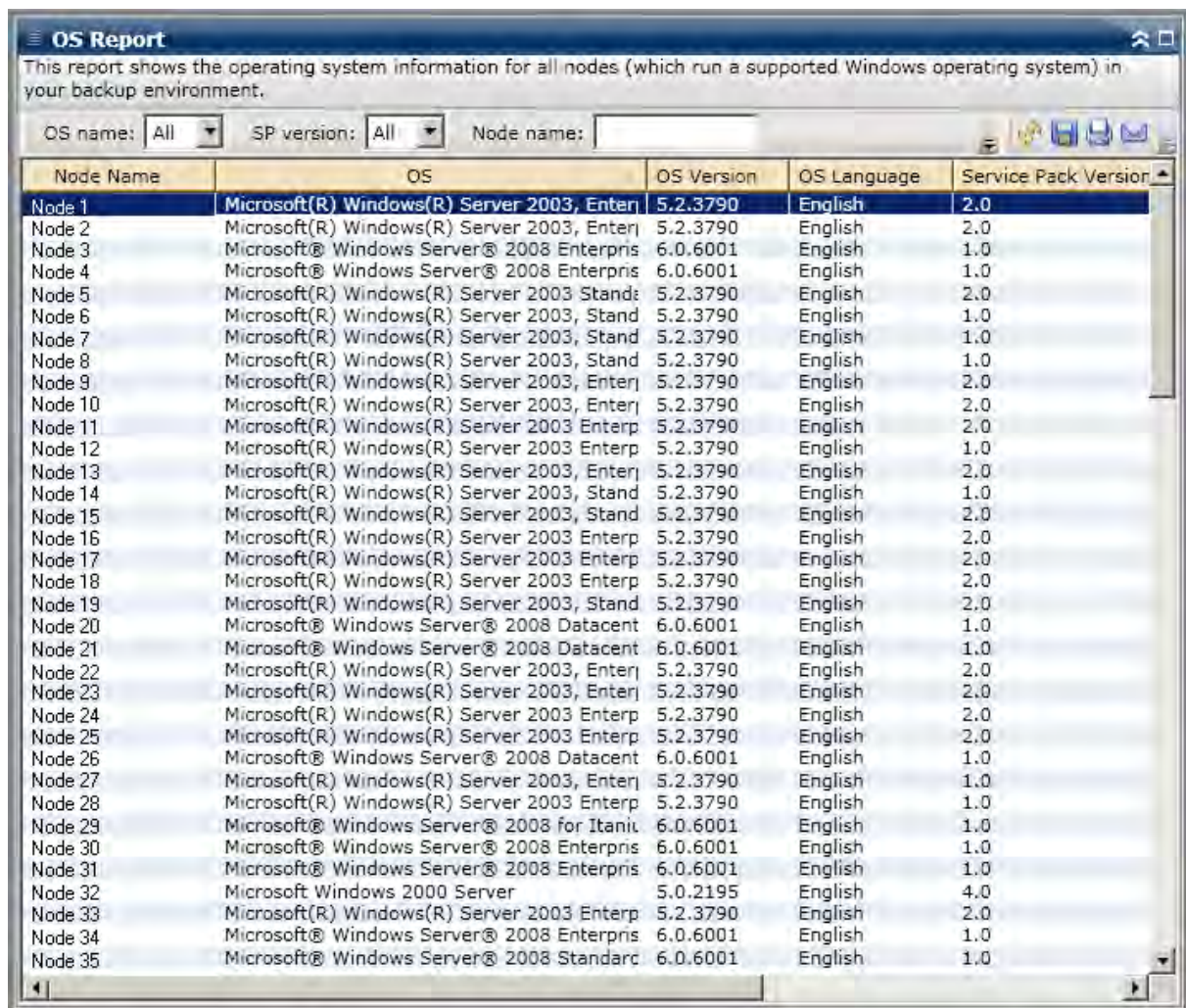
Always look for patterns in behavior to isolate potential problem operating systems and determine if nodes with the same operating system are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The OS Report is displayed in table format listing the Node Name, and the associated operating system, OS Version, OS Language, Service Pack Version, System Directory, System Device, and OS Manufacturer for each node.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

To filter the table display, you can either specify the Node name or use drop-down menus for OS name, SP Version (Service Pack), or Node tier.



The screenshot shows a window titled "OS Report" with a description: "This report shows the operating system information for all nodes (which run a supported Windows operating system) in your backup environment." Below the description are filters for "OS name" (set to "All"), "SP version" (set to "All"), and "Node name" (empty). The main table lists 35 nodes with columns for Node Name, OS, OS Version, OS Language, and Service Pack Version.

Node Name	OS	OS Version	OS Language	Service Pack Version
Node 1	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 2	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 3	Microsoft® Windows Server® 2008 Enterpris	6.0.6001	English	1.0
Node 4	Microsoft® Windows Server® 2008 Enterpris	6.0.6001	English	1.0
Node 5	Microsoft(R) Windows(R) Server 2003 Stande	5.2.3790	English	2.0
Node 6	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	1.0
Node 7	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	1.0
Node 8	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	1.0
Node 9	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 10	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 11	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 12	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	1.0
Node 13	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 14	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	1.0
Node 15	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	2.0
Node 16	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 17	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 18	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 19	Microsoft(R) Windows(R) Server 2003, Stand	5.2.3790	English	2.0
Node 20	Microsoft® Windows Server® 2008 Datacent	6.0.6001	English	1.0
Node 21	Microsoft® Windows Server® 2008 Datacent	6.0.6001	English	1.0
Node 22	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 23	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	2.0
Node 24	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 25	Microsoft® Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 26	Microsoft® Windows Server® 2008 Datacent	6.0.6001	English	1.0
Node 27	Microsoft(R) Windows(R) Server 2003, Enterp	5.2.3790	English	1.0
Node 28	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	1.0
Node 29	Microsoft® Windows Server® 2008 for Itaniu	6.0.6001	English	1.0
Node 30	Microsoft® Windows Server® 2008 Enterpris	6.0.6001	English	1.0
Node 31	Microsoft® Windows Server® 2008 Enterpris	6.0.6001	English	1.0
Node 32	Microsoft Windows 2000 Server	5.0.2195	English	4.0
Node 33	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 34	Microsoft® Windows Server® 2008 Enterpris	6.0.6001	English	1.0
Node 35	Microsoft® Windows Server® 2008 Standar	6.0.6001	English	1.0

Recovery Point Objective Report

The Recovery Point Objective Report is a bar chart format and displays the backup node count at each location for each day. This report can be used to analyze the location of your node backups for any given day and help you determine the best means for recovery if necessary.

The Recovery Point Objective Report separates the node backups into four categories: Replicated, Disk, tape On-Site, and tape Off-Site. You can click on the bar chart to view the recovery points available for the selected node within corresponding category.

Replicated

Nodes that were replicated using CA XOssoft and backed up using CA ARCserve Backup as XOssoft scenarios. Replicated backups can usually be recovered within minutes.

Disk

Nodes that were backed up to disk (including FSD, VTL, and deduplication devices). Disk backups can usually be recovered within hours.

On-Site:

Nodes that were backed up to tape and the tape is located on-site. On-site tape backups can usually be recovered within a day.

Off-Site:

Nodes that were backed up to tape and the tape is located off-site. Off-site tape backups can usually be recovered within a few days.

Report Benefits

The Recovery Point Objective Report is similar to the Backup Data Location Report; however, this report has the extra benefit of being able to display the number of recovery points and location of your backup data for any specified day. This report is helpful for planning and demonstrating (if necessary) the speed and effectiveness of your recovery strategy.

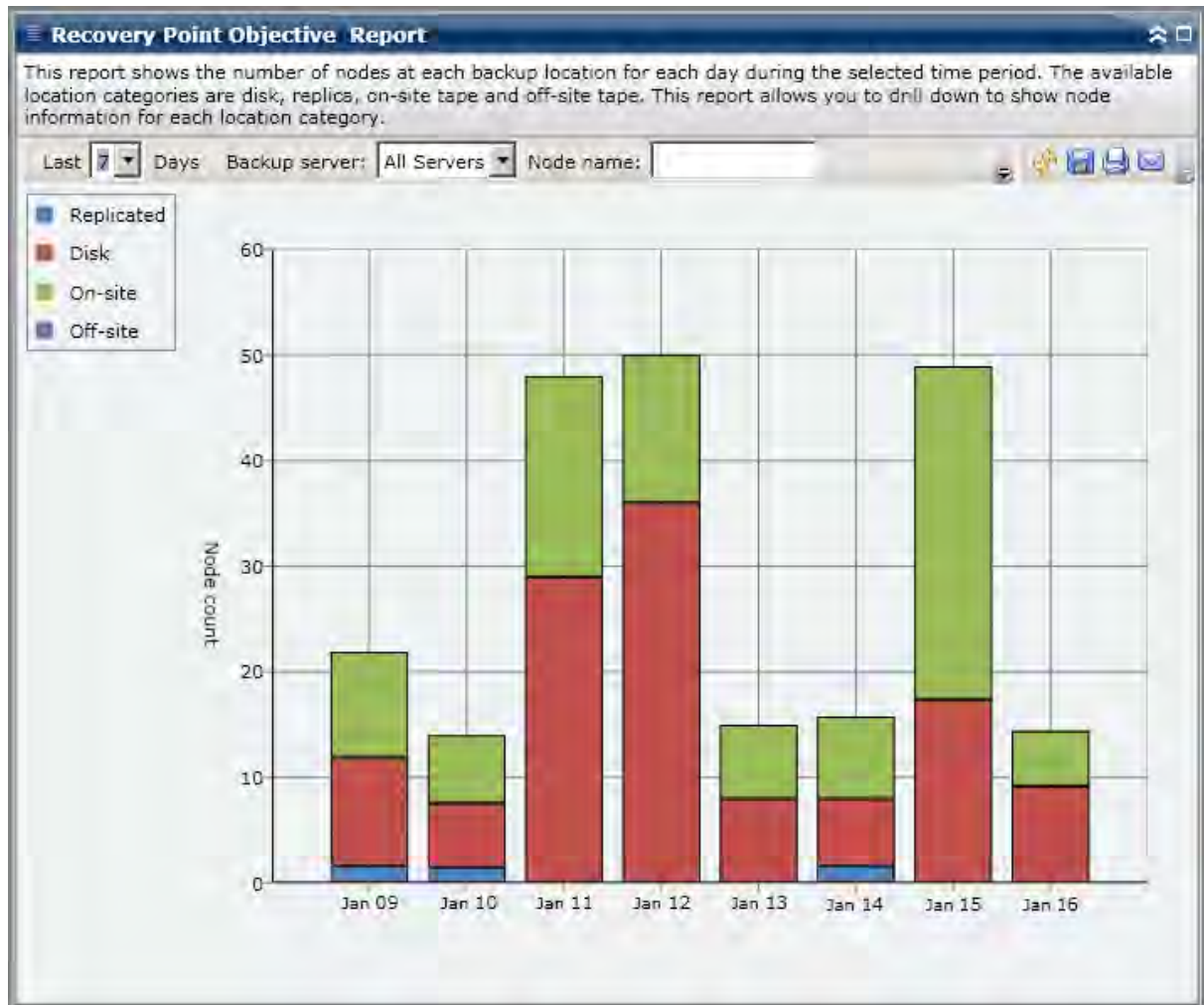
Generally you can use this report to determine how fast you can restore data and how many recovery points (backups) you have taken.

For example, if within your company, Department A has backed up data that is critical or high-priority and would need to recover this data within minutes if necessary. Also, Department B may have different backed up data that is less critical and would need to recover within a day if necessary. Based on these needs, the Department A data would have to be replicated to enable almost immediate recovery, while Department B data could be backed up on a daily basis and stored on an on-site tape to satisfy the recovery requirements.

As a result, you can use this report to view the number of recovery points and locations of the stored data to determine if you have satisfied these various needs. You can then demonstrate to each department how you have met their individual requirements, or if necessary modify your backup strategy (by either changing the amount of recovery points/backups taken or change the location/speed to recover of the stored data) to satisfy the various requirements.

Report View

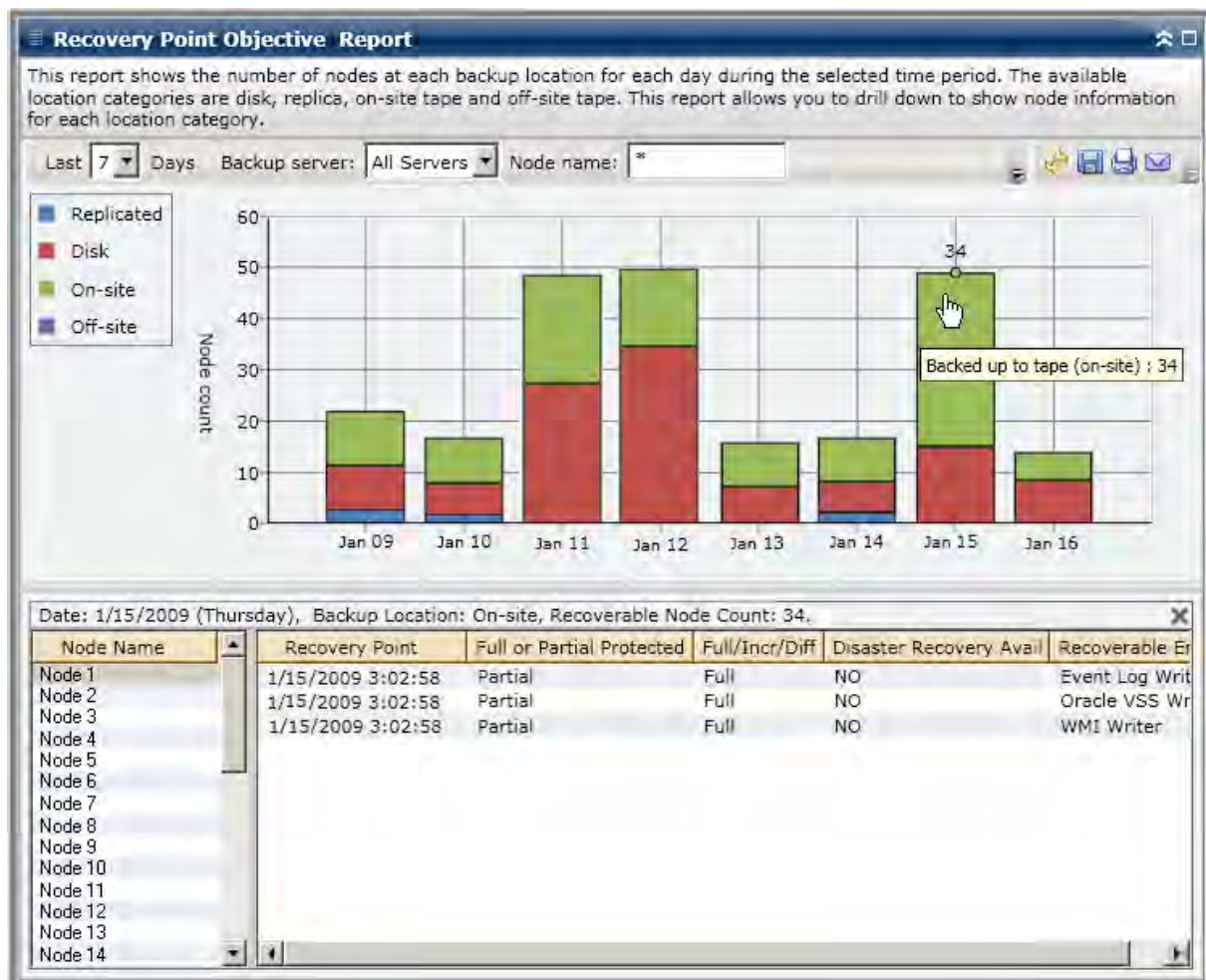
The Recovery Point Objective Report is displayed in a bar chart format, showing the number of nodes that were backed up to the various recovery point locations during the specified time period. The bar chart provides a detailed level view of the nodes that were backed up for the selected server during each day of the time period. The status categories shown in the bar chart represent the daily number of nodes backed up at each recovery location (replicated, disk, tape on-site, and tape off-site).



Drill Down Reports

The Recovery Point Objective Report can be further expanded to display more detailed information. You can click on any of the bar chart category to display a detailed listing of all nodes that were backed up for the corresponding recovery location on that selected day. This drill-down report includes the Node names, along with the corresponding most recent recovery point (backup time), the number of recovery points, the type of recovery protected (full or partial), the backup method used (full, incremental, or differential), whether or not disaster recovery (DR) is available, and the recoverable entity name (root session path for the recovery points).

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



SCSI/Fiber Card Report

The SCSI/Fiber Card Report is an SRM-type report that shows the Small Computer System Interface (SCSI) and fiber card information for all Windows nodes within your environment, categorized by the manufacturer.

Report Benefits

The SCSI/Fiber Card Report is helpful in quickly classifying machines based on the SCSI or fiber card. You can get an overall view to analyze and determine which SCSI or fiber cards are more effective than others for backup jobs, and which ones could be potential problem areas.

For example, if from this report you see that a particular SCSI or fiber card node has a slow throughput value, you can try to determine why this is occurring. Look for patterns in behavior among the slower SCSI or fiber cards or among the same manufacturer. You can also use the fastest throughput values as reference points to analyze why these SCSI or fiber cards are performing well. You can compare the slower SCSI or fiber cards to the faster SCSI or fiber cards to determine if you actually have a problem or if both sets of values are similar, maybe the slower SCSI or fiber cards are not performing poorly.

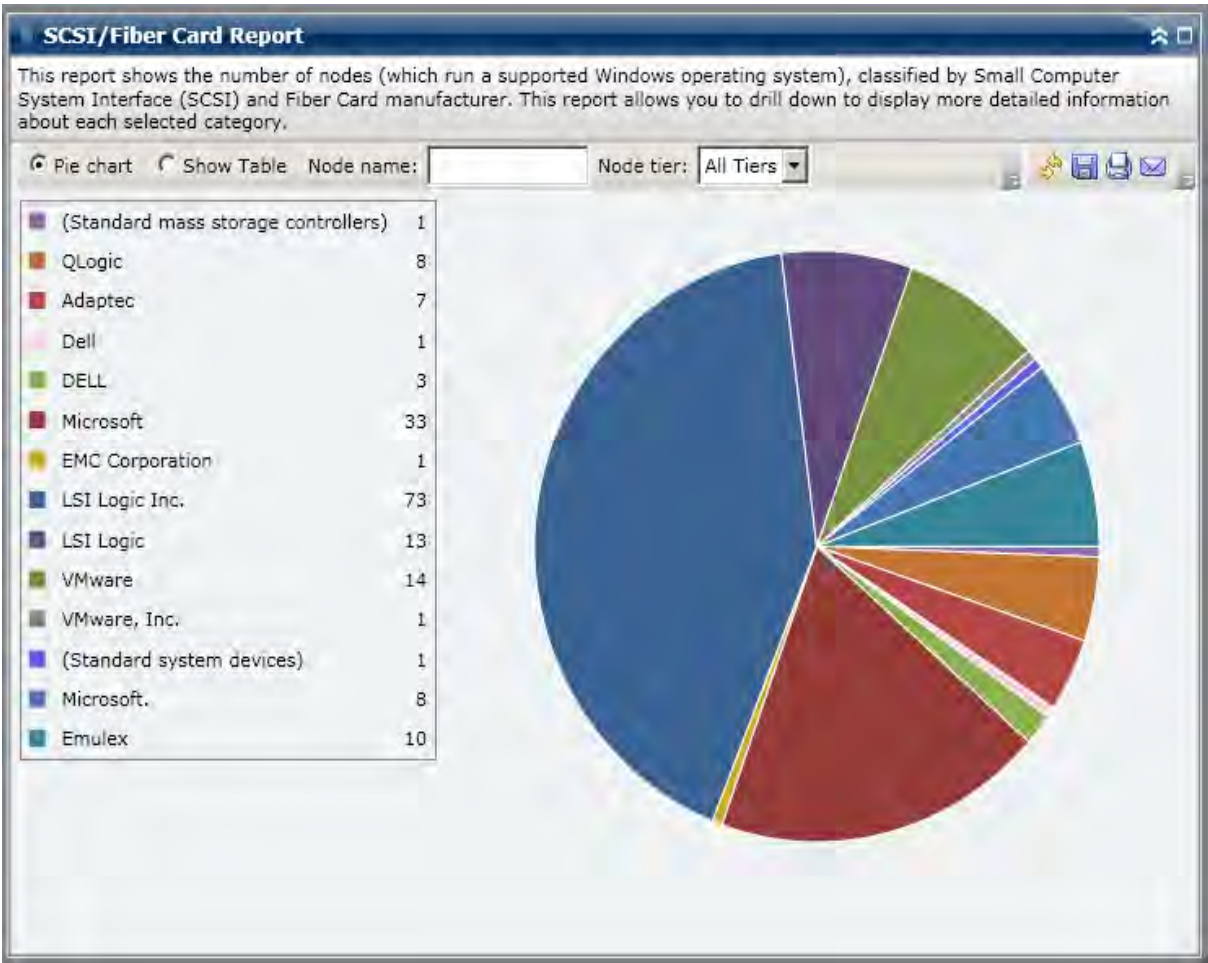
Always look for patterns in behavior to isolate potential problem SCSI or fiber cards and determine if the same SCSI or fiber cards are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The SCSI/Fiber Card Report is displayed in a pie chart or table format.

Pie Chart

The pie chart shows the SCSI and fiber card information for all known nodes.



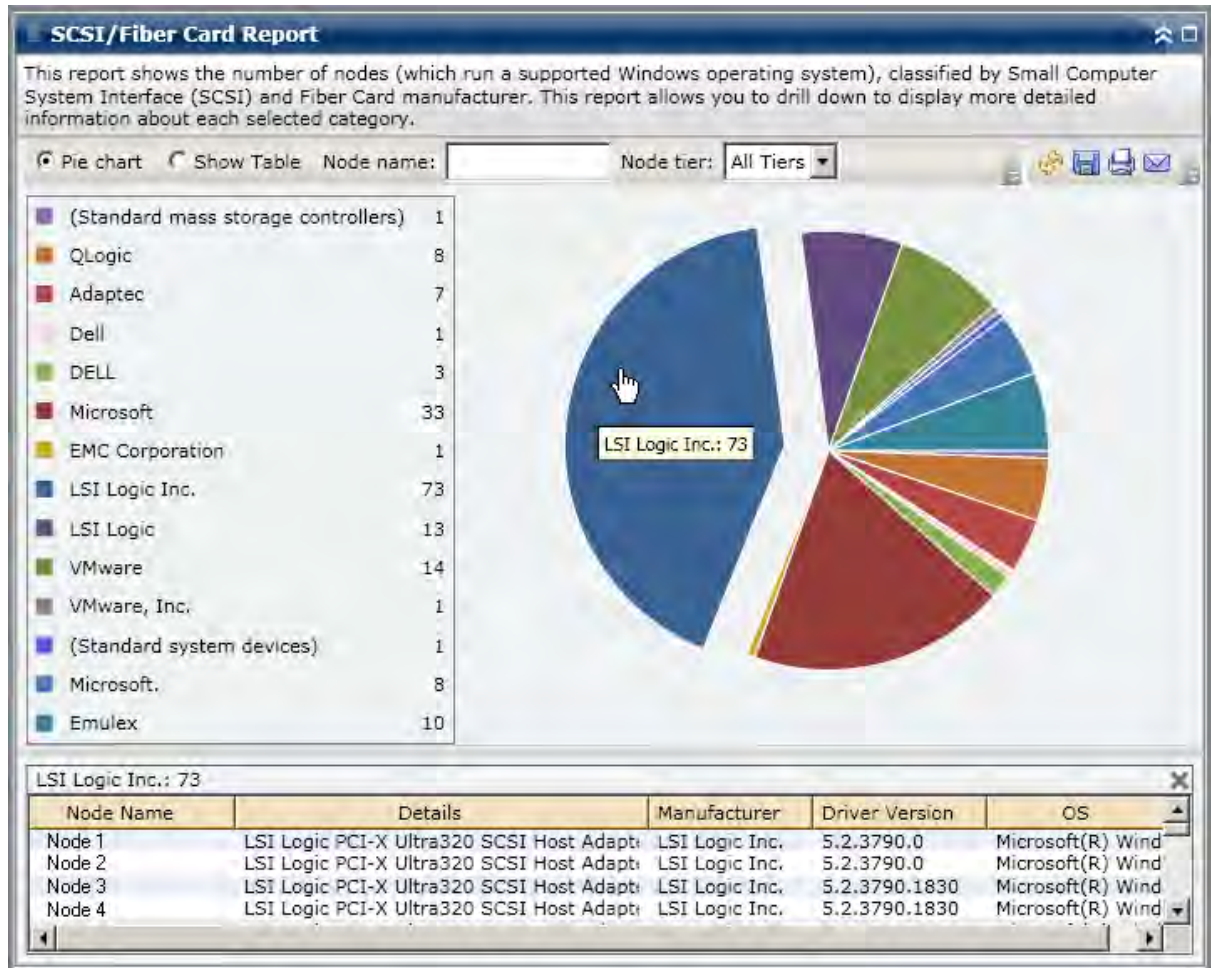
Show Table

If you select Show Table, the SCSI/Fiber Card Report displays more detailed information in table format listing the Node Name, OS, Details, Manufacturer, and Driver Version for all of the allocated space categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The SCSI/Fiber Card Report can be further expanded from the Pie chart view to display more detailed information. You can click a row to drill down from a report of summary information to a more focused and detailed report about that particular SCSI or fiber card.



Tape Encryption Status Report

The Tape Encryption Status Report displays the number of tapes with and without encrypted backup sessions during the specified time period. Encryption of data is important, not only to remain compliant, but also to maintain to data security. Many companies transport their backup tapes to offsite locations for disaster recovery purposes. This transport poses a security risk because there is always the chance that when the data leaves the secured facility, it is often exposed to the public and could be lost or stolen in transit. Using backup tape encryption can help protect your data no matter where it is.

This report can be used to determine if your sensitive data is properly protected and provides a means to quickly identify and resolve potential problem areas with your backups.

Report Benefits

The Tape Encryption Status Report is helpful in analyzing and determining which tapes are adequately protected, and which ones could be potential problem areas. Encryption of data is critical for both security purposes and for your company to remain compliant.

From this report you can quickly determine if you have sensitive data on tapes that is not encrypted and therefore subject to a security risk.

For example, you can easily view which of your tapes contain encrypted data and which ones do not. In addition, you can also view from this report the location of these encrypted and non-encrypted tapes (onsite or offsite). If you see that you have non-encrypted tapes that contain sensitive data on them and they are stored at an offsite location, you immediately know that your data is not being properly protected. You need to re-evaluate your backup strategy before a problem occurs.

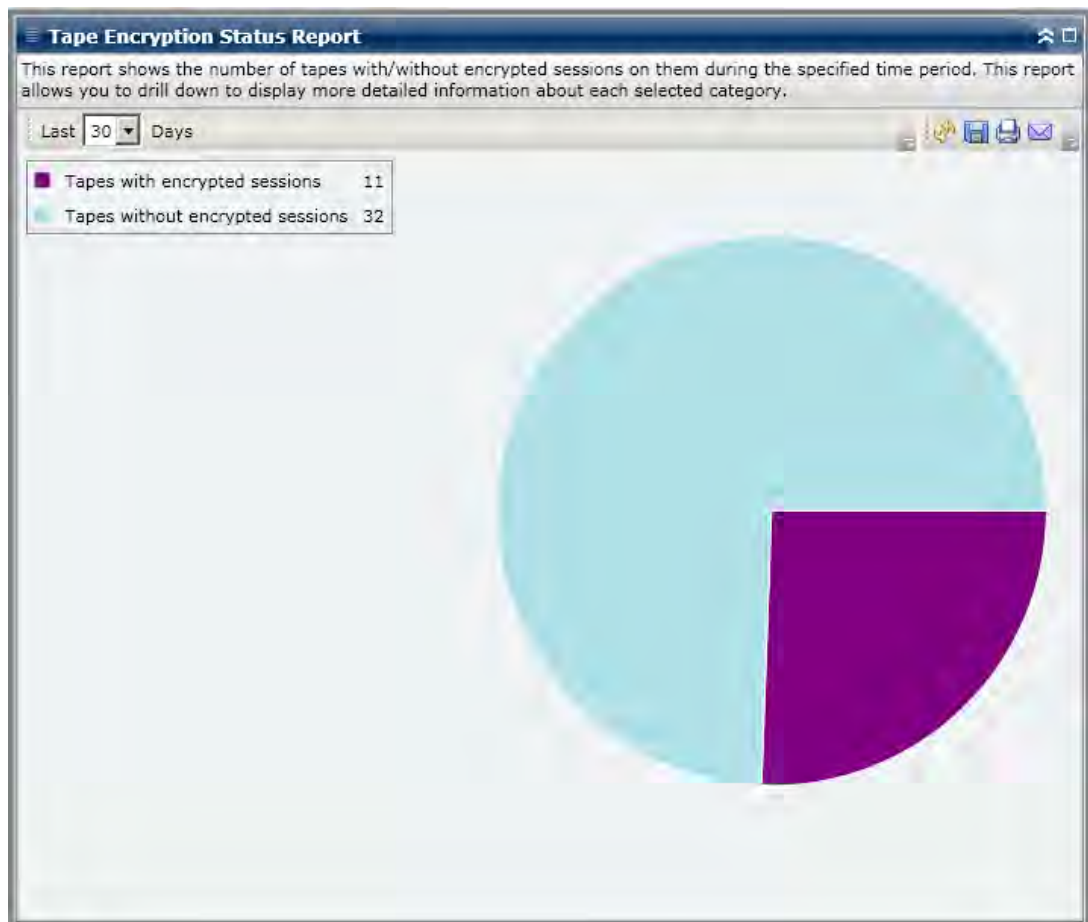
Likewise, from this report you can see if you have non-sensitive data that is being encrypted and therefore not only wasting valuable resources (time and money), but also slowing down your backup efforts.

For example, if from this report you see that you have tapes that do not contain critical data but the data is still encrypted, you should re-evaluate your backup strategy to ensure proper use of resources and time.

Report View

The Tape Encryption Status Report is displayed in a pie chart format, showing the number (and percentage) of tapes that were backed up and contain encrypted sessions and the number of tapes that were backed up and do not contain encrypted sessions.

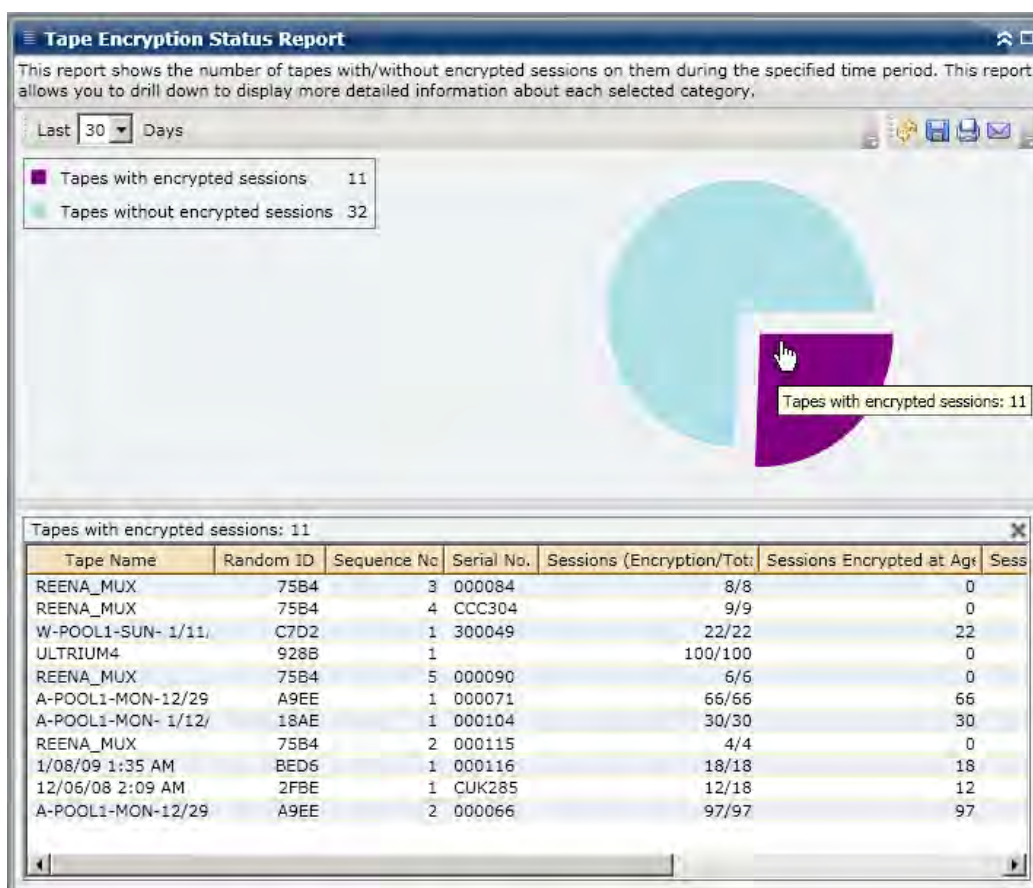
- Tapes with encrypted sessions are defined as tapes that have one or more encrypted backup sessions during the specified time period.
- Tapes without encrypted sessions are defined as tapes that do not have any encrypted backup sessions during the specified time period.



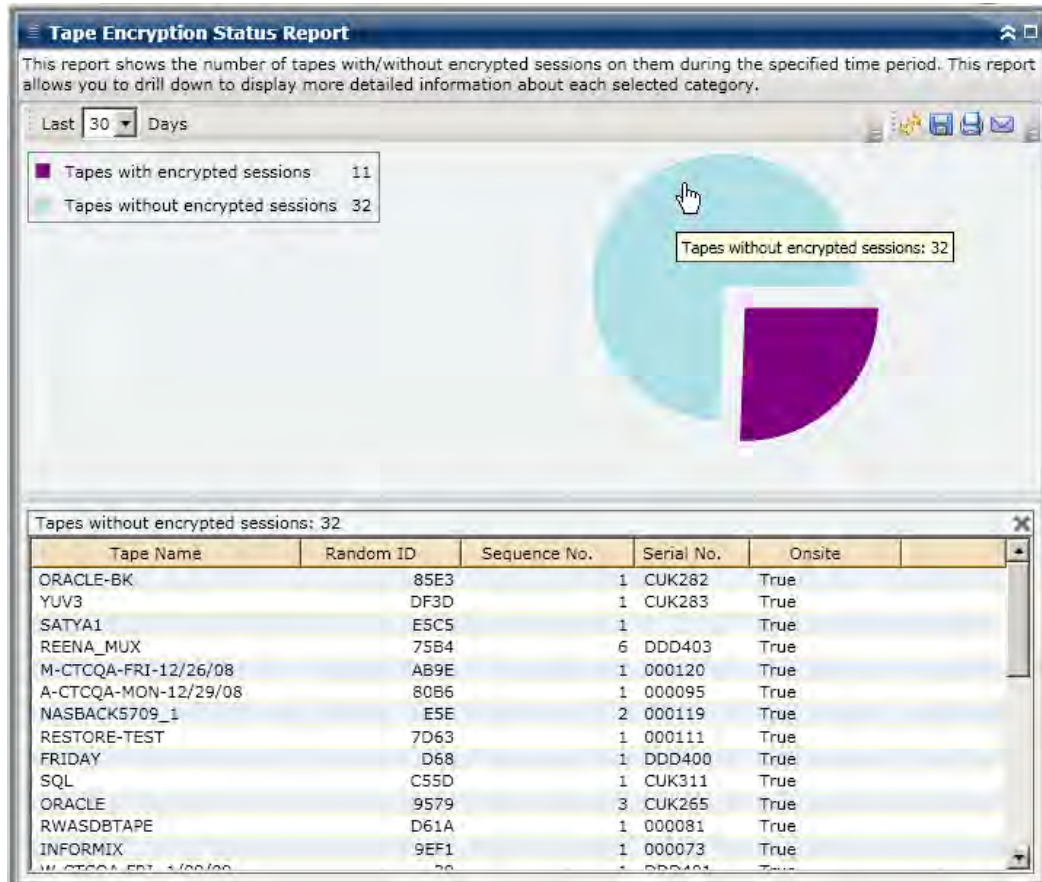
Drill Down Reports

The Tape Encryption Status Report can be further expanded to display more detailed information. You can click on either of the two categories to display a detailed listing of all tapes associated with that category during the specified time period. This drill-down report includes the tape names, along with the associated encryption-related information for each category.

- If you drilled down in the Tapes with Encrypted Sessions category this report also displays the session counts of each tape. The session count consists of four sequential categories:
 - **Sessions (Encryption/Total)** - Count of encrypted and total number of sessions on tape.
 - **Sessions Encrypted at Agent** - Count of sessions encrypted at agent side on tape.
 - **Sessions Encrypted at Server (SW/HW)** - Count of sessions encrypted at the CA ARCserve Backup server (using software encryption and hardware encryption).
 - **Password only** - Session information is protected by a session password on the tape



- If you drilled down in the Tapes without Encrypted Sessions category the corresponding table also displays information about the corresponding tape.



Top Nodes with Failed Backups Report

The Top Nodes with Failed Backups Report lists the top specified number of nodes where a backup job (Full, Incremental, or Differential) failed during the last specified number of days.

Report Benefits

You can use this report to focus on the nodes with the most Failed Count and try to determine why this is occurring. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

For example, if you just focus on number of failures, it may be a false indication of a problem area because if a node failed 3 times, but was successful 30 times (a 10% failure rate), it may be less of a problem than a node that failed only 2 times but was successful just 3 times (a 40% failure rate).

In addition, the number of days since the last successful backup could provide an indication of problem areas if it shows a pattern of recent failures.

For example, if a node failed 10 times, but the last successful backup was only 1 day ago, it may be less of a problem than a node that failed 5 times, but the last successful backup was 7 days ago.

Note: An "N/A" displayed in this field indicates that the data is Not Applicable and means that there has not been a successful backup of this node during the specified time period.

Report View

The Top Nodes with Failed Backups Report is displayed in a table format, listing the nodes with the highest number of failed backups.

Note: By default, CA ARCserve Backup only retains Activity Log information for 14 days. If you want CA ARCserve Backup Dashboard to display Activity Log information for more than 14 days, you must modify the "Prune activity logs older than" option to increase the log retention period. For more information about modifying Activity Log settings, see the Administration Guide.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

This report shows the top nodes where a backup job failed during the specified time period. This report allows you to drill down to display more detailed information about each selected node.			
Last: 30 Days	Top: 5	Node name:	Node tier: All Tiers
Node Name	Failed Count	Successful Count	Days since last successful backup
Node 1	33	92	0
Node 2	20	27	1
Node 3	13	1	14
Node 4	12	14	1
Node 5	12	0	No successful backup

Drill Down Reports

The Top Nodes with Failed Backups Report can be further expanded to display more detailed information. You can click on any of the node to display a detailed listing of all log messages associated with that node. You can also filter the list by specifying the severity of the messages displayed (Errors and Warnings, Errors, Warnings, Information, or All).

Note: Dashboard uses pagination to display the first 100 log messages. You can click on the Next page button to view further messages.

Note: From this drill down report, you can click on any listed error or warning message to display the related troubleshooting help topic with the corresponding reason and corrective action.

Top Nodes with Failed Backups Report

This report shows the top nodes where a backup job failed during the specified time period. This report allows you to drill down to display more detailed information about each selected node.

Last: 30 Days Top: 5 Node name: Node tier: All Tiers

Node Name	Failed Count	Successful Count	Days since last successful backup
Node 1	33	92	0
Node 2	20	27	1
Node 3	13	1	14
Node 4	12	14	1
Node 5	12	0	No successful backup.

Node 1

Severity Filter: Errors and Warnings 1 / 1

Severity	Time	Message	Backup Server	Agent Host	Job ID	Session
Error	1/13/2009 4:52:33 AM	E3712 Unable to close s	Server 1	Host 1	2970	
Error	1/13/2009 4:50:06 AM	E3719 Unable to write t	Server 1	Host 1	2970	
Error	1/12/2009 4:04:54 PM	E8533 The request is dr	Server 2	Host 1	2952	
Warning	1/12/2009 4:37:29 AM	W12612 The number of	Server 1	Host 1	2800	
Error	1/12/2009 1:12:30 AM	E3834 Unable to find ar	Server 1		2758	
Warning	1/12/2009 1:07:58 AM	W3825 Unable to find t	Server 1		2758	
Warning	1/11/2009 4:36:42 AM	W12612 The number of	Server 2	Host 1	2617	
Error	1/11/2009 1:12:25 AM	E3834 Unable to find ar	Server 1		2587	
Warning	1/11/2009 1:07:54 AM	W3825 Unable to find t	Server 1		2587	
Error	1/10/2009 1:57:45 PM	E3834 Unable to find ar	Server 2		2405	
Error	1/10/2009 1:51:46 PM	E6300 A Windows NT S	Server 2		2405	
Error	1/10/2009 1:21:47 PM	E3705 Unable to format	Server 2		2405	

Top Nodes with Fastest/Slowest Backup Throughputs Report

The Top Nodes with Fastest/Slowest Backup Throughputs Report lists the top specified number of nodes with the highest/lowest throughput values during the last specified number of days. For each node, throughput is computed as the ratio of total data backed up and total time taken (MB/minute) by all backup jobs (Full, Incremental, or Differential) for that node, during the last specified number of days.

Report Benefits

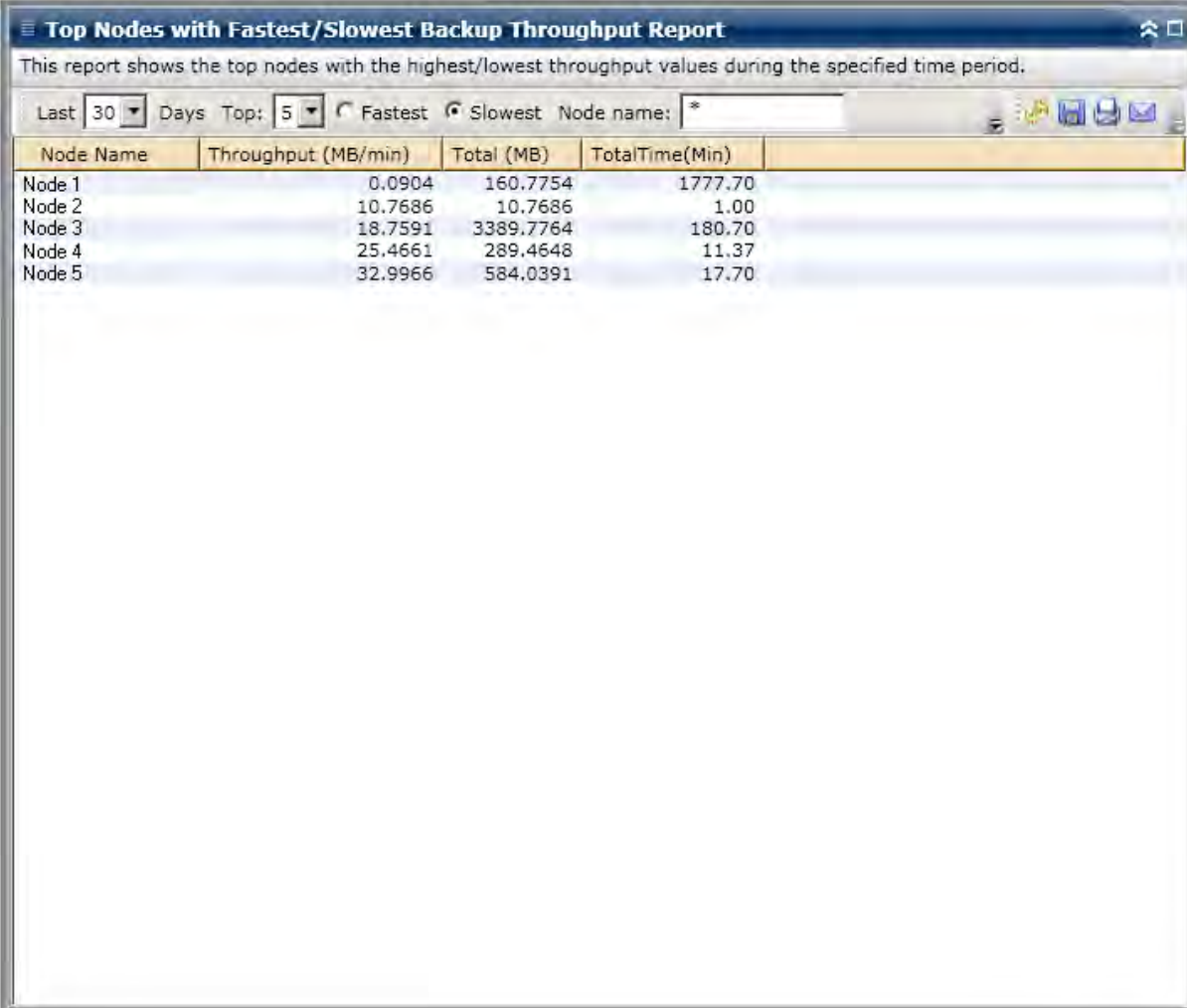
The Top Nodes with Fastest/Slowest Backup Throughputs Report is helpful in analyzing and determining which nodes are more effective than others for backup jobs, and which ones could be potential problem areas. Generally from this report, you would focus your attention on the nodes with the slowest throughput values and try to determine why this is occurring. Perhaps it is a network problem, or a slow drive, or the type of backup job being performed. Look for patterns in behavior among the slower nodes. You can also use the fastest throughput values as reference points to analyze why these nodes are performing well. You can compare the slower nodes to the faster nodes to determine if you actually have a problem or if both sets of values are similar, maybe the slower nodes are not performing poorly. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

For example, if you only focus on the slowest performing nodes (lowest throughput value), it may be false indication of a problem area because you also need to analyze the amount of data being moved or the type of backup being performed.

Report View

The Top Nodes with Fastest/Slowest Backup Throughputs Report is displayed in a table format, listing the nodes with the fastest or slowest throughput values (MB/min).

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).



Node Name	Throughput (MB/min)	Total (MB)	TotalTime(Min)
Node 1	0.0904	160.7754	1777.70
Node 2	10.7686	10.7686	1.00
Node 3	18.7591	3389.7764	180.70
Node 4	25.4661	289.4648	11.37
Node 5	32.9966	584.0391	17.70

Virtual Machine Recovery Points Report

The Virtual Machine Recovery Point Report lists details about the recovery points available for each virtual machine (VM) that was backed up using VMware Consolidated Backup (VCB) technology or Microsoft Hyper-V.

Report Benefits

The Virtual Machine Recovery Point Report is helpful in analyzing and determining the effectiveness of your protected VM data environment. From this report you can get a snapshot view of your overall VM backup infrastructure and determine if your data is well-protected. This report also displays the number of recovery points and location of your backup data for any specified day, which is helpful for planning and demonstrating (if necessary) the speed and effectiveness of your recovery strategy of your virtual machines.

Generally if a specific VM contains high priority data, you want to ensure that you have enough recovery points to enable a quick and complete recovery, if necessary.

For example, a VM that contains high-priority data should have five recovery points taken to be adequately protected. If from this report, you discover that this specific high-priority VM only contains two recovery points, you should investigate the reason, and modify your backup schedule as necessary to ensure proper recovery protection. You can determine the most recent recovery point to identify the latest possible time up to which your data can be recovered for each VM and whether it is possible to recover each node as a RAW level recovery, file level or both.

Report View

The Virtual Machine Recovery Point Report is displayed in table format listing detailed information for the selected node.

Note: This report will only display Virtual Machines which have had at least one successful backup.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

This report shows recovery/restore information for virtual machines (VM) that were backed up using VMware Consolidated Backup (VCB) technology or Microsoft Hyper-V during the specified time period. This report allows you to drill down to display more detailed recovery point information about each selected node.						
Last	7	Days	Virtual Machine Type:	All	Node name:	
Node Name	Hosting Machine Name	VMware VirtualCenter	VMware Proxy	Virtual Machine Type	OS	Recovery Type
Node 1	RMDMQAHYPV1	N/A	N/A	Microsoft Hyper-V	Window	Raw/File
Node 2	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Unix/Lin	RAW
Node 3	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 4	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 5	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 6	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 7	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 8	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 9	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 10	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 11	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 12	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 13	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 14	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 15	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 16	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 17	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 18	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 19	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 20	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 21	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 22	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 23	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 24	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 25	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 26	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 27	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 28	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 29	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW

Drill Down Reports

The Virtual Machine Recovery Point Report can be further expanded to display more detailed information. You can click a row to drill down from a report of summary information to a more focused and detailed report about that particular recovery point.

The screenshot shows the 'Virtual Machine Recovery Points Report' window. It includes a summary table of nodes and a detailed view of recovery points for a selected node.

Summary Table:

Node Name	Hosting Machine Name	VMware VirtualCenter	VMware Proxy	Virtual Machine Type	OS	Recovery Type
Node 1	RMDMOAHYPV1	N/A	N/A	Microsoft Hyper-V	Window	Raw/File
Node 2	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Unix/Lin	RAW
Node 3	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 4	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 5	172.24.092.548	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 6	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 7	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 8	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 9	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 10	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 11	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 12	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	RAW
Node 13	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 14	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	File
Node 15	172.24.101.649	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File
Node 16	172.24.112.07	172.24.073.175	100-LL-DELL07	VMware VCB	Window	Raw/File

Recovery Points for Virtual Machine: Node 1, Count: 1

Recovery Point	Volume	Data Size	Execution Time
1/13/2009 3:09:04 AM	RAW	72.38	1/13/2009 3:04:28 AM
	C:	10.48	1/13/2009 3:53:52 AM
	E:	0.05	1/13/2009 3:53:52 AM
	F:	0.09	1/13/2009 3:53:52 AM

The drill down view is made up of two tables: Recovery Point and Volume.

Recovery Point Table

The Recovery Point table displays all recovery points available for the virtual machine selected and lists the dates/times of the recovery points.

Volumes Table

The Volume table displays all the volumes that were backed up as part of the selected recovery point.

Virtualization Most Recent Backup Status Report

The Virtualization Most Recent Backup Status Report shows the most recent backup status for each virtual machine (VM) that was backed up using VMware Consolidated Backup (VCB) technology or Microsoft Hyper-V.

Report Benefits

The Virtualization Most Recent Backup Status Report is helpful in analyzing and determining which VM are more effective than others for backup jobs, and which ones could be potential problem areas.

For example, generally you can use this report to check the status of the most recent backup status of your VM's. If the backup status from the previous day is all green (successful), you know that you had a good backup. However, if the backup status is red (failed), then you can correlate the results with the activity logs that you see in the Node Backup Status drill down Report for this VM to determine the problem area and fix it without delay. You can also identify the kind of recovery (raw, file, or both) that is available for each VM in case of successful VM backups.

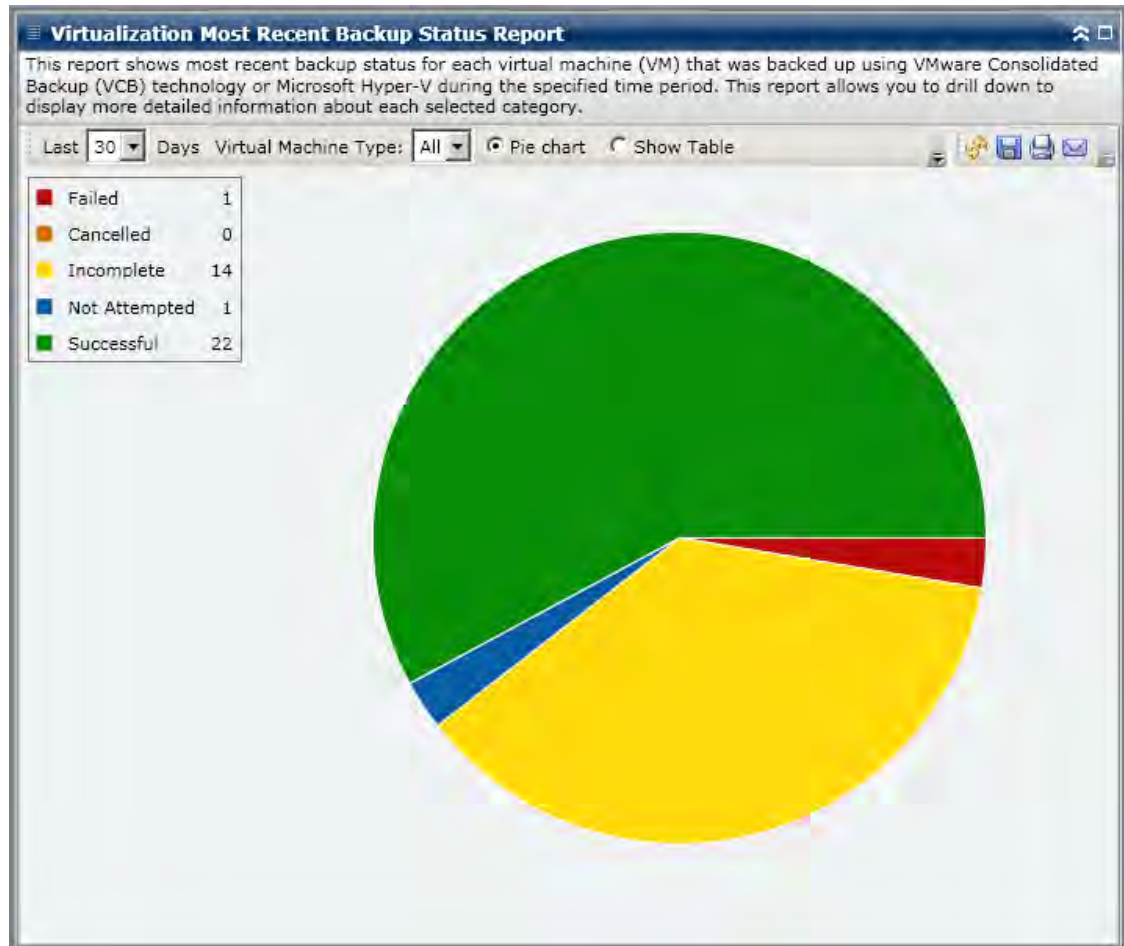
Always look for patterns in behavior to isolate potential problem jobs and determine if the same jobs are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem backup jobs.

Report View

The Virtualization Most Recent Backup Status Report is displayed in a pie chart or table format.

Pie Chart

The pie chart shows the most recent backup status for all virtual machines.



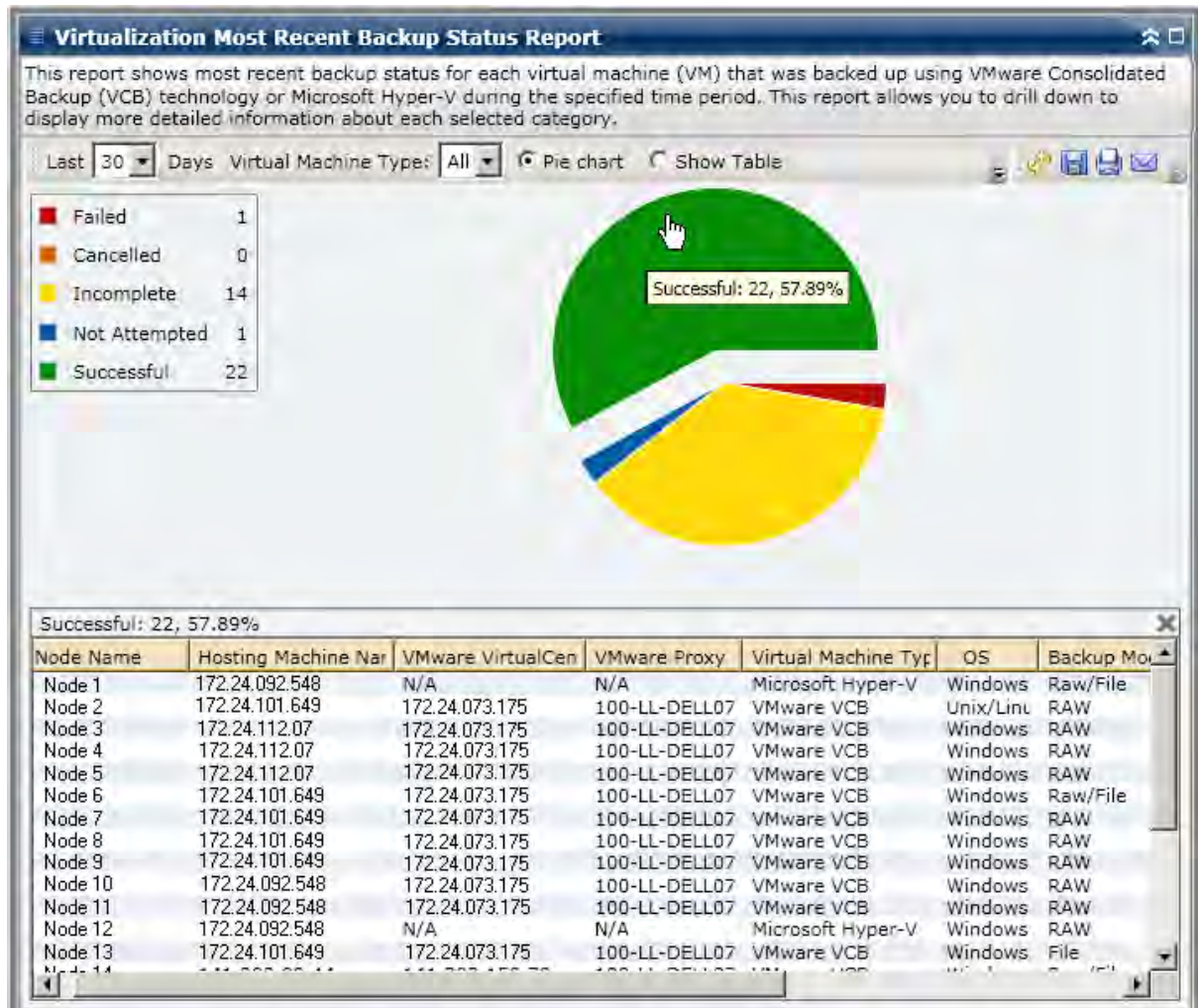
Show Table

If you select Show Table, the Virtualization Most Recent Backup Status Report displays more detailed information in table format listing the Node Name, Hosting Machine Name, VMware Virtual Center, VMware Proxy, and Virtual Machine for all of the backup status categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Report

The Virtualization Most Recent Backup Status Report can be further expanded from the Pie chart view to display a drill-down report with the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



Volume Report

The Volume Report is an SRM-type report that displays volume information for all Windows nodes in your environment. This report categorizes the nodes by the amount (percentage) of used volume space. The amount of allocated space is reported in the Disk Report.

Report Benefits

The Volume Report is helpful in quickly classifying machines based on the amount of free space available. You can get an overall view to analyze and determine which nodes are almost full and potentially can cause a problem. This report identifies nodes in danger of running out of free space or even nodes that are under utilized. It also identifies nodes in which the volume needs to be defragmented.

You can use this report in conjunction with the Disk Report to analyze the amount of allocated space compared to the amount of used space.

For example, if from this report you see that a particular volume has very little free space, you should then check the Disk Report to compare the allocated space to the amount of space being used. If the allocated space is low, but the used space is high, you should investigate the reason for this non-allocated space and if possible, create a new volume to better utilize your available space.

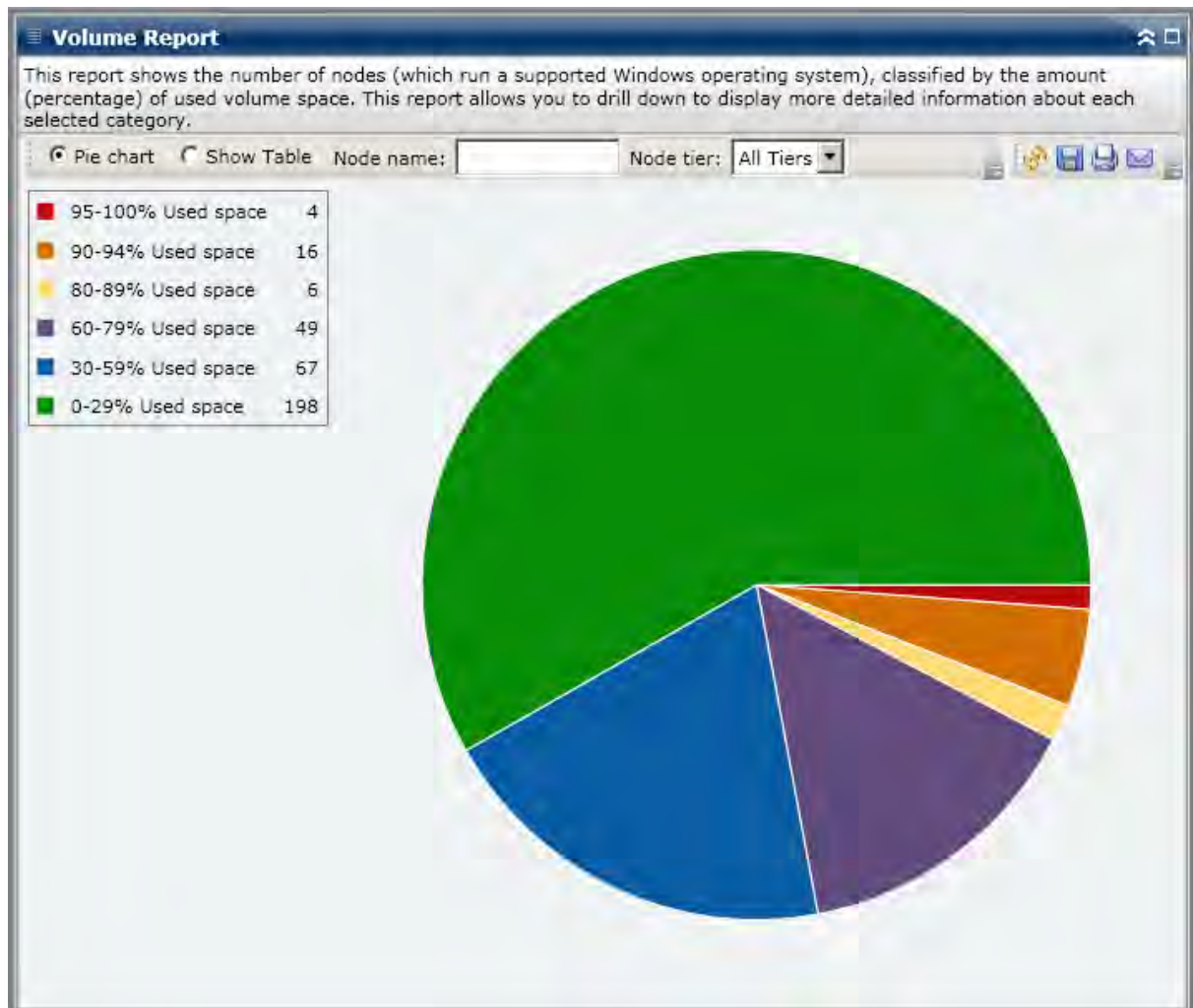
It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Volume Report is displayed in pie chart or table format.

Pie Chart

The pie chart shows the amount of volume space used in pre-configured percentage categories.



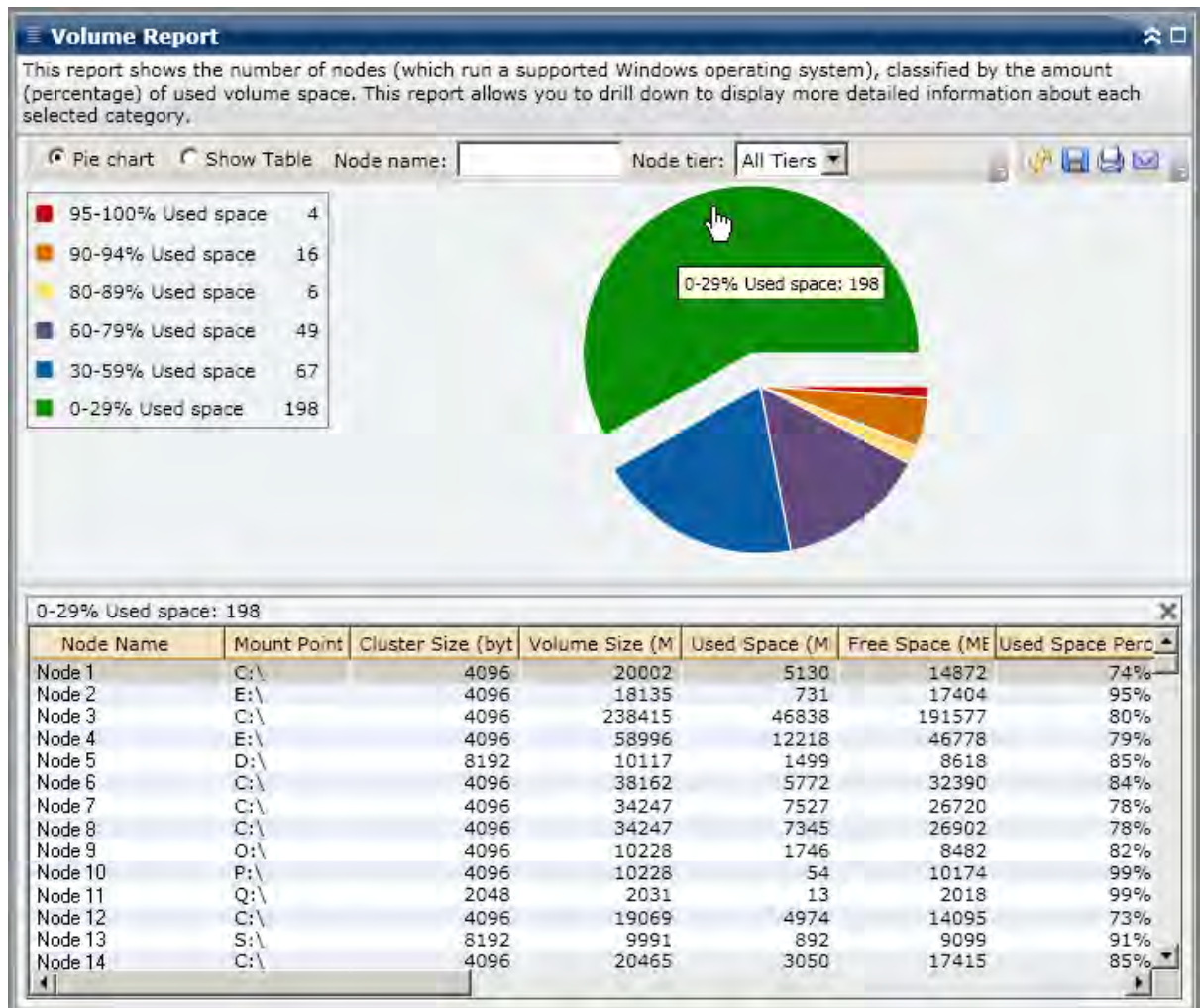
Show Table

If you select Show Table, the Volume Report displays more detailed information in table format, listing the Node Name, OS, Mount Point, Cluster Size, Volume Size, Free Space, Free Space Percentage, Volume Type, Disk Name, Compressed, File System Type, and Total Fragmentation for all of the allocated space categories.

Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see [Node Information](#) (see page 39).

Drill Down Reports

The Volume Report can be further expanded to display a drill-down report with the same detailed information as the Show Table; however, the data displayed in the drill down report is filtered by the selected category.



Chapter 4: Troubleshooting

This section explains the most common CA ARCserve Backup Dashboard troubles, along with the reason or solution.

This section contains the following topics:

[Email notifications not being sent](#) (see page 137)

[Dashboard does not display data](#) (see page 138)

[Dashboard does not display data after a previous CA ARCserve Backup database has been restored](#) (see page 139)

[Dashboard does not display data for node backed up using command line](#) (see page 140)

[Dashboard shows a blank screen upon launch](#) (see page 140)

[Dashboard shows an Unhandled Exception alert upon launch](#) (see page 141)

[SRM data probe not occurring](#) (see page 142)

[SRM data probe performance problem](#) (see page 143)

[SRM probe dialog displays "Service not ready" message](#) (see page 144)

Email notifications not being sent

If the scheduled email notifications have not been sent, perform the following troubleshooting procedure:

1. Verify the CA ARCserve Backup services are running and restart if necessary. For more information about CA ARCserve Backup services, see the *Administration Guide*.
2. Verify you have the proper Dashboard email notification settings applied. For more information, see [Configure Email Reports](#) (see page 20).
3. Check Email schedule log messages as follows:
 - a. From the global options toolbar, click the Schedule Email icon to open the Schedule Manager dialog.
 - b. From this dialog, click the Log Messages button to display the Log Message window and check for any log messages of the schedule runs.
 - If the log indicates that the email server is not reachable, ping the machine in an attempt to establish a connection. If the machine is still not reachable, contact CA Technical Support at <http://ca.com/support> for online technical assistance.
 - If the log indicates that the email settings are not correct, verify you have the proper Alert Manager notification settings applied. For more information about the Alert Manager, see the *Administration Guide*.

Dashboard does not display data

If the CA ARCserve Backup Dashboard does not display any data, perform the following troubleshooting procedure:

Note: Dashboard can only monitor and report on nodes that have CA ARCserve Backup agents with r12.5 or later.

1. Verify that data for Dashboard is being collected.
 - For SRM type reports, browse to and expand each node and perform an SRM probe to collect data.

You can manually initiate an SRM probe by opening the SRM Probing dialog and clicking the Probe Now button or wait until 2:00 PM for the next automatic probe.
 - For Backup Environment type reports, perform a backup of a CA ARCserve Backup r12.5 agent.
2. Verify the CA ARCserve Backup services are running and restart if necessary. For more information about CA ARCserve Backup services, see the *Administration Guide*.
3. Refresh the reports.
4. If the problem persists, access the CA.ARCserve.CommunicationFoundation.WindowsServices.exe.config file to enhance the corresponding CACF.svclog information.

The configuration file is located in the following directory:

X:\Program Files\CA\ARCServe Backup

- a. In the configuration file, locate the following string:

source name="CA.ARCserve.CommunicationFoundation.Trace"
- b. Change the value from "Information" (default value) to "Verbose" to provide more detailed information in the output log files and help CA troubleshoot the problem.
- c. Restart the CA ARCserve Backup services.
- d. Refresh the Dashboard reports.
- e. Locate the CACF.svclog file in the following directory:

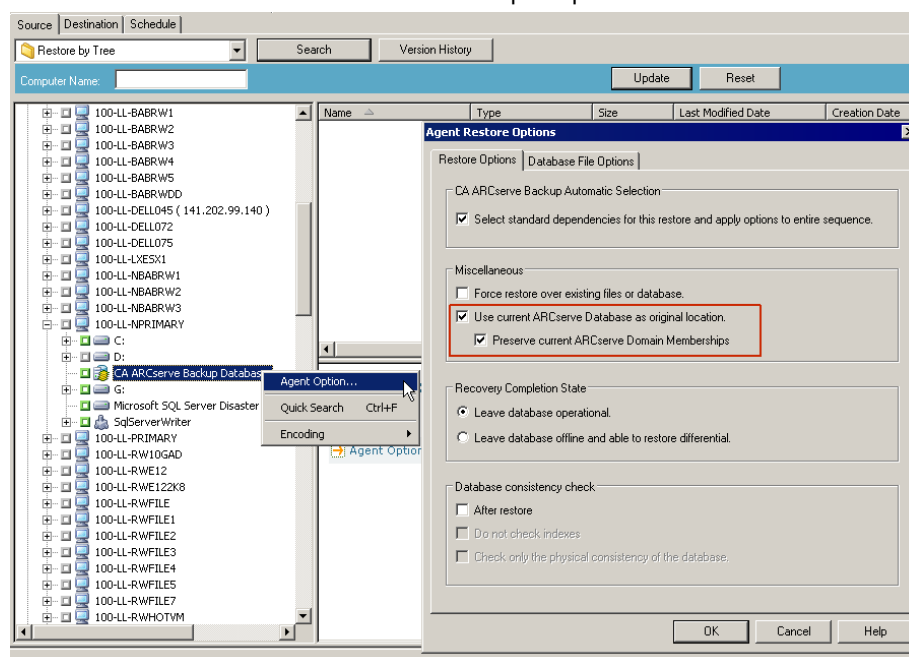
X:\Program Files\CA\ARCServe Backup\LOG
- f. Send the CACF.svclog file to CA Technical Support for investigation.

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at <http://ca.com/support>.

Dashboard does not display data after a previous CA ARCserve Backup database has been restored

If the CA ARCserve Backup Dashboard does not display any data after you have restored an older version of the CA ARCserve Backup Database, perform the following troubleshooting procedure:

1. If you have not restored the CA ARCserve Backup Database, make sure that you specify to include the "Preserve current ARCserve Domain Memberships" option as follows to avoid this problem:
 - a. From the Restore Manager, select the CA ARCserve Backup Database to be restored.
 - b. Right-click and from the pop-up menu, select Agent Option.
 - c. The Agent Restore Options dialog appears.
 - d. Right-click and from the pop-up menu, select Agent Option.
 - e. From the Restore Options tab, select the "Use current ARCserve Database as original location" and also select the associated "Preserve current ARCserve Domain Memberships" option.



2. If you have already restored the CA ARCserve Backup Database (and if the "Preserve current ARCserve Domain Memberships" option is not selected), you need to enter the CA ARCserve Backup Database credentials using Server Configuration Wizard as follows:
 - a. Close CA ARCserve Backup Manager on the new primary server
 - b. Launch the Server Configuration Wizard and choose the Select Database option.
 - c. Provide the necessary information in the subsequent screens until you reach SQL Database System Account screen. If the "DB overwrite" alert message appears, click OK.
 - d. Clear the check mark from the Overwrite the existing "ARCserve_DB" instance option to retain your previous data and click Next.
 - e. After the Server Configuration Wizard completes the updates, click Finish.
 - f. Close the Server Configuration Wizard, open CA ARCserve Backup Manager, and launch Dashboard.

Dashboard does not display data for node backed up using command line

If the CA ARCserve Backup Dashboard does not display any data for a node that was backed up using the command line (ca_backup), perform the following troubleshooting procedure:

1. Add the same node to the Backup Manager GUI by selecting the Windows Systems object, right-clicking, and selecting Add Machine/Object from the pop-up menu.
2. Expand the node in the Source directory tree by giving administrator or equivalent user credentials.

The node will now display data in the Dashboard reports.

Dashboard shows a blank screen upon launch

This is because you may not have rebooted your machine after installing CA ARCserve Backup. During the installation of CA ARCserve Backup the .NET framework 3.5 SP1 is also installed and a machine reboot is a prerequisite for .NET framework. If the dashboard shows a blank screen, perform the following troubleshooting procedure:

1. Reboot the machine.
2. If the problem persists, contact Technical Support at <http://ca.com/support> for online technical assistance and a complete list of locations, primary service hours, and telephone numbers.

Dashboard shows an Unhandled Exception alert upon launch

This is because you may not have rebooted your machine after installing CA ARCserve Backup. During the installation of CA ARCserve Backup the .NET framework 3.5 SP1 is also installed and a machine reboot is a prerequisite for .NET framework. If the dashboard shows the following alert screen, perform the following troubleshooting procedure:



1. Reboot the machine.
2. If the problem persists, contact Technical Support at <http://ca.com/support> for online technical assistance and a complete list of locations, primary service hours, and telephone numbers.

SRM data probe not occurring

If the SRM data probe is not occurring, perform the following troubleshooting procedure:

1. Manually initiate an SRM probe by opening the SRM Probing dialog and clicking the Probe Now button.
2. Refresh the reports.
3. Access the AgIfProb.exe.log file for additional information. The AgIfProb.exe.log file is located in the following directory:

X:\Program Files\CA\ARCServe Backup\LOG

4. Check the AgIfProb.exe.log for the following conditions:
 - a. Check if the node is displayed as a good node name. This will indicate if CA ARCserve Backup is aware that this node exists.
 - b. Check if CA ARCserve Backup has the user information login credentials in the database to gain access to the node.

If the log indicates that no user information about this node exists in the database, access the Backup Manager, browse to and expand the node name, and provide the proper security credentials (User name and Password).

- c. Check if CA ARCserve Backup failed to connect to the node. If the log indicates that the connection to the node has failed, ping the node in an attempt to establish a connection. This will verify if the client agent on the node is working.
5. If the problem persists, send the AgIfProb.exe.log file to CA Technical Support for investigation.

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at <http://ca.com/support>.

SRM data probe performance problem

If the performance of your SRM probe is either taking an excessive amount of time or using an excessive amount of system resources, you can configure the number of simultaneous connections (parallel threads) to enhance this performance. To change the performance of the SRM data collection process you need to add a new registry key and then modify the value for these parallel threads to meet your specific needs.

To configure the SRM probe thread count setting in the Registry Editor

1. Open the Registry Editor.
2. Expand the tree in the browser of the Registry Editor by selecting the following:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\Base\Task\Common
3. Add a new key (if it does not already exist) and name it "SRMReportTime".
4. Add a new DWORD Value and name it "ThreadCount".
5. Double-click the Thread Count option to open the Edit DWORD Value dialog. You can now modify the DWORD setting.

By default CA ARCserve Backup has this SRM data collection value set to 16 threads until you add this new key. The minimum allowable value is 1 (meaning a single thread will be used to collect the SRM data) and maximum allowable value is 32 threads. Any value entered greater than 32 will be ignored and revert to this maximum value of 32 parallel threads.

- As you increase the number of parallel threads, it will reduce the overall SRM probe time; however, it will also increase the impact on your system resources.
 - As you decrease the number of parallel threads, it will reduce the impact on your backup server; however, it will also increase the overall SRM probe time.
6. When you finish configuring the Thread Count option for the SRM probe, close the Registry Editor and restart the Database engine service on the CA ARCserve Backup server.

SRM probe dialog displays "Service not ready" message

This is because the SRM probing utility is unable to gather SRM-related information from a node. To identify which node is causing this problem, check the AgIfProb.exe.log file for additional information. The AgIfProb.exe.log file is located in the following directory:

X:\Program Files\CA\ARCServe Backup\LOG

If you see the following entry for a node in the log file "Receive xml size tli header failed, error number=183", perform the following troubleshooting procedure:

1. Restart the Database Engine service and run SRM probe again.
2. If the problem persists, contact Technical Support at <http://ca.com/support> for online technical assistance and a complete list of locations, primary service hours, and telephone numbers.

Index

A

- add a Dashboard Group • 35
- add new email schedule • 22
- Agent Distribution Report • 44
 - drill down reports • 46
 - report benefits • 44
 - report view • 45
- agent upgrade alert • 40

B

- Backup Data Location Report • 48
 - drill down reports • 50
 - report benefits • 48
 - report view • 49
- Backup Server Load Distribution Report • 51
 - report view • 51
- bar chart overview • 15

C

- CA ARCserve Backup Dashboard
 - email reports • 20
 - global options • 18
 - graphical displays • 15
 - groups • 33
 - GUI • 14
 - introduction • 11
 - report types • 41
 - reports • 41
 - report-specific options • 28
- collapse report view • 15
- configure email reports • 20
- configure SRM • 29
- CPU Report • 54
 - drill down reports • 56
 - report benefits • 54
 - report view • 55
- cursor overview • 15
- customize reports • 18

D

- Dashboard Groups • 33
 - add • 35
 - delete • 37
 - modify • 36

- Data Distribution on Media Report • 57
 - drill down reports • 59
 - report benefits • 57
 - report view • 58
- data exporting • 123
- data sorting • 123
- Deduplication Benefits Estimatie Report • 60
 - report benefits • 60
 - report view • 61
- Deduplication Status Report • 62
 - drill down reports • 64
 - report benefits • 62
 - report view • 63
- delete a Dashboard Group • 37
- Disk Report • 65
 - drill down reports • 67
 - report benefits • 65
 - report view • 65
- drill down reports • 43
 - Agent Distribution Report • 46
 - Backup Data Location Report • 50
 - CPU Report • 56
 - Data Distribution on Media Report • 59
 - Deduplication Status Report • 64
 - Disk Report • 67
 - Job Backup Status Report • 71
 - Media Assurance Report • 77
 - Memory Report • 80
 - NIC Report • 83
 - Node Backup Status Report • 87
 - Node Disaster Recovery Report • 92
 - Node Encryption Status Report • 96
 - Node Recovery Point Report • 100
 - Node Tiers Report • 105
 - Node Whose Most Recent Backup Failed Report • 108
 - Recovery Point Objective Report • 114
 - SCSI/Fiber Card Report • 117
 - Tape Encryption Status Report • 119
 - Top Nodes with Failed Backups Report • 124
 - Virtual Machine Recovery Point Report • 129
 - Virtualization Most Recent Backup Status Report • 132
 - Volume Report • 135

E

email scheduling • 18, 20
email scheduling status • 27
expand report view • 15

F

failed node backups • 123
fastest backup nodes • 126
features • 13

G

global options • 18
graphical displays • 15
GUI • 14

I

Introduction • 11

J

Job Backup Status Report • 68
 drill down reports • 71
 report benefits • 68
 report view • 69

L

License Report • 73
 report benefits • 73
 report view • 74
log messages • 20

M

Media Assurance Report • 75
 drill down reports • 77
 report benefits • 75
 report view • 76
Memory Report • 78
 drill down reports • 80
 report benefits • 78
 report view • 79
modify a Dashboard Group • 36

N

NIC Report • 81
 drill down reports • 83
 report benefits • 81
 report view • 82
Node Backup Status Report • 84

 drill down reports • 87
 report benefits • 84
 report view • 84
Node Encryption Status Report • 94
 drill down reports • 96
 report benefits • 94
 report view • 95
node information window • 39
Node Recovery Point Report • 98
 drill down reports • 100
 report benefits • 98
 report view • 99
Node Summary Report • 101
 report benefits • 101
 report view • 102
node tiers • 38
Node Tiers Report • 103
 drill down reports • 105
 report benefits • 103
 report view • 104
Node Whose Last Backup Failed Report • 106
 drill down reports • 108
 report benefits • 106
 report view • 106

O

options • 28
OS Report • 109
 report benefits • 109
 report view • 110
overall • 11

P

pie chart overview • 15

R

Recovery Point Objective Report • 111
 drill down reports • 114
 report benefits • 112
 report view • 113
report types • 41
 backup environment • 42
 drill down • 43
 SRM • 42
reports • 41
 Agent Distribution Report • 44
 Backup Data Location Report • 48
 Backup Server Load Distribution Report • 51
 collapse view • 13

- CPU Report • 54
- Data Distribution on Media Report • 57
- Deduplication Benefits Estimate Report • 60
- Deduplication Status Report • 62
- expand view • 13
- Fiber Card Report • 115
- Job Backup Status Report • 68
- License Report • 73
- Media Assurance Report • 75
- Memory Report • 78
- NIC Report • 81
- Node Backup Status Report • 84
- Node Encryption Status Report • 94
- Node Recovery Point Report • 98
- Node Summary Report • 101
- Node Tiers Report • 103
- Node Whose Most Recent Backup Failed Report • 106
- OS Report • 109
- Recovery Point Objective Report • 111
- reports, Disk Report • 65
- Tape Encryption Status Report • 118
- Top Nodes with Failed Backups Report • 122
- Top Nodes with Fastest/Slowest Backup Throughputs Report • 125
- types • 41
- Virtual Machine Recovery Point Report • 127
- Virtualization Most Recent Backup Status Report • 130
- Volume Report • 133

S

- scheduling emails • 18, 20
- SCSI/Fiber Card Report • 115
 - drill down reports • 117
 - report benefits • 115
 - report view • 116
- slowest backup nodes • 126
- SRM configure • 29
- SRM prober • 29
- SRM reports • 42

T

- Tape Encryption Status Report • 119
 - drill down reports • 119
 - report benefits • 118
 - report view • 119
- throughputs • 126
- Top Nodes with Failed Backups Report • 122

- drill down reports • 124
- report benefits • 122
- report view • 123
- Top Nodes with Fastest/Slowest Backup Throughputs Report • 125
 - report benefits • 125
 - report view • 126
- tracking email schedule status • 27

V

- Virtual Machine Recovery Point Report • 127
 - drill down reports • 129
 - report benefits • 127
 - report view • 128
- Virtualization MostRecent Backup Status Report • 130
 - drill down reports • 132
 - report view • 131
 - reports benefit • 130
- Volume Report • 133
 - drill down reports • 135
 - report benefits • 133
 - report view • 133