Arcserve® Backup for Windows

Dashboard User Guide

r16.5

arcserve®

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve 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 Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE 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 ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

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.

Copyright © 2015 Arcserve (USA), LLC and its affiliates and subsidiaries. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective owners.

Arcserve Product References

This document references the following Arcserve products:

- Arcserve® Backup
- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent for Windows
- Arcserve® Unified Data Protection Agent for Linux
- Arcserve® Replication and High Availability

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

https://www.arcserve.com/support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Providing Feedback About Product Documentation

If you have comments or questions about Arcserve product documentation, please contact us.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Updated to include user feedback, enhancements, corrections, and other minor changes to help improve the usability and understanding of the product or the documentation itself.

Contents

Chapter 1: Understanding Dashboard 11

Introduction 11
Dashboard Features 13
Dashboard GUI 14
Display Options 15
Customize Dashboard Reports 18
- Global Options 19
- Configure Email Reports 24
- Report-Specific Options 31
- SRM Prober Settings 33

Chapter 2: Understanding Global Dashboard 35

Introduction 35
Features 36
Terms and Definitions 36
Global Dashboard Services 38
How Global Dashboard Works 40

Chapter 3: Configuring Global Dashboard 43

Configuration Considerations 43
Configure Global Dashboard 44
- Configure the Central Site 46
- Configure a Branch Site 49

Chapter 4: Using Dashboard 55

Use Arcserve Backup Dashboard 55
Dashboard Groups 57
- Add a Dashboard Group 59
- Modify a Dashboard Group 60
- Delete a Dashboard Group 61

Node Tiers 61
Node Information 62
Send a Report by Email 63
Agent Upgrade Alert 64

Chapter 5: Using Global Dashboard 65

Global Dashboard User Interfaces 65
Understanding Central Manager 66
Understanding Branch Manager 81
Manage Branch Groups 85
Add a New Branch Group 86
Delete a Branch Group 87
Modify a Branch Group 87
Synchronize Data 89
Modify Automatic Data Synchronization 89
Manually Synchronize Data 90
Manually Configure a Branch Site 90
Export/Import Global Dashboard Information 92
Export Global Dashboard Information 93
Import Global Dashboard Information 94

Chapter 6: Dashboard Reports 97

Arcserve Backup Dashboard Report Types 98
Backup Environment Type Reports 98
SRM Type Reports 99
Drill Down Reports 99
Agent Distribution Report 100
Report Benefits 101
Report View 102
Drill Down Reports 103
Application Data Trend Report 104
Report Benefits 105
Report View 105
Backup Data Location Report 106
Report Benefits 107
Report View 108
Drill Down Reports 108
Backup Server Load Distribution Report 109
Report Benefits 109
Report View 110
Client Node Software Report 113
Report Benefits 113
Report View 113
Drill Down Report 116
CPU Report 116
Report Benefits 117

Report View....118
Drill Down Reports....119
Data Distribution on Media Report....120
Report Benefits....120
Report View....121
Drill Down Reports....122
Deduplication Benefits Estimate Report....122
Report Benefits....122
Report View....124
Deduplication Status Report....124
Report Benefits....125
Report View....126
Drill Down Reports....127
Disk Report....128
Report Benefits....128
Report View....128
Drill Down Report....130
Job Archive Status Report....131
Report Benefits....131
Report View....132
Drill Down Reports....133
Job Backup Status Report....135
Report Benefits....136
Report View....136
Drill Down Reports....139
License Report....141
Report Benefits....141
Report View....142
Media Assurance Report....143
Report Benefits....143
Report View....143
Drill Down Reports....145
Memory Report....145
Report Benefits....146
Report View....147
Drill Down Reports....148
Network Report....149
Report Benefits....149
Report View....149
Drill Down Reports....151
Node Archive Status Report....151
Report Benefits....152

Report View....152
Drill Down Reports....154
Node Backup Status Report....155
Report Benefits....156
Report View....156
Drill Down Reports....159
Node Disaster Recovery Status Report....160
Report Benefits....161
Report View....162
Drill Down Reports....163
Node Encryption Status Report....164
Report Benefits....165
Report View....165
Drill Down Reports....166
Node Recovery Points Report....168
Report Benefits....169
Report View....170
Drill Down Reports....171
Node Summary Report....172
Report Benefits....173
Report View....174
Node Tiers Report....175
Report Benefits....175
Report View....176
Drill Down Reports....176
Node Whose Most Recent Backup Failed Report....178
Report Benefits....178
Report View....178
Drill Down Reports....180
OS Report....181
Report Benefits....181
Report View....182
Recovery Point Objective Report....183
Report Benefits....183
Report View....185
Drill Down Reports....185
SCSI/Fiber Card Report....186
Report Benefits....187
Report View....187
Drill Down Reports....189
SRM PKI Utilization Reports....189
SRM PKI Report Benefits....190

CPU Utilization Report 191
Disk Performance Report 192
Memory Utilization Report 193
Network Utilization Report 195
Tape Encryption Status Report 196
Report Benefits 197
Report View 197
Drill Down Reports 198
Top Nodes with Failed Backups Report 200
Report Benefits 201
Report View 202
Drill Down Reports 203
Top Nodes with Fastest/Slowest Backup Throughputs Report 204
Report Benefits 204
Report View 205
Top Nodes with Most Unchanged Files Report 206
Report Benefits 206
Report View 206
Total Archive Size Report 207
Report Benefits 208
Report View 209
Total Protection Size Report 209
Report Benefits 210
Report View 211
Virtual Machine Recovery Points Report 211
Report Benefits 212
Report View 213
Drill Down Reports 214
Virtualization Most Recent Backup Status Report 215
Report Benefits 215
Report View 216
Drill Down Report 218
Volume Report 218
Report Benefits 219
Report View 219
Drill Down Reports 222
Volume Trend Report 222
Report Benefits 223
Report View 223

Chapter 7: Troubleshooting Dashboard 225

Troubleshooting Overview 225
Dashboard Troubleshooting 225

Chapter 8: Troubleshooting Global Dashboard 233

Troubleshooting Overview 233
Global Dashboard Troubleshooting 233
Synchronization Fails Due to Insufficient Free Disk Space 238

Glossary 241

Index 243

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 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 provides snapshot displays that provide an overall status of the specified 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 Arcserve Backup Dashboard from the Monitor & Reports Menu on the Navigation Bar of the Arcserve Backup Manager Console or from the Quick Start menu.

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

Global Dashboard is a part of Arcserve Backup Dashboard and expands on these Dashboard capabilities to let you quickly and easily view dashboard information for multiple Arcserve Backup primary servers, both in your main office and in remote offices, all from a central location. This centralized monitoring capability through Global Dashboard means better information being reported on the performance and operation of your entire Arcserve Backup and SRM environment.

Note: For more information about Global Dashboard, see Understanding Global Dashboard (see page 35).

The reports displayed on the Arcserve Backup Dashboard are:

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

- Agent Distribution Report
- Application Data Trend Report *
- Backup Data Location Report
- Backup Server Load Distribution Report
- Client Node Software Report *
- CPU Report *
- CPU Utilization Report *
- Data Distribution on Media Report
- Deduplication Benefits Estimate Report
- Deduplication Status Report
- Disk Report *
- Disk Performance Report *
- Job Archive Status Report
- Job Backup Status Report
- License Report
- Media Assurance Report
- Memory Report *
- Memory Utilization Report *
- Network Report *
- Network Utilization Report *
- Node Archive Status 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
- OS (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
- Top Nodes with Most Unchanged Files Report *
- Total Archive Size Report
- Total Protection Size Report
- Virtual Machine Recovery Points Report
- Virtualization Most Recent Backup Status Report
- Volume Report *
- Volume Trend Report *

Dashboard Features

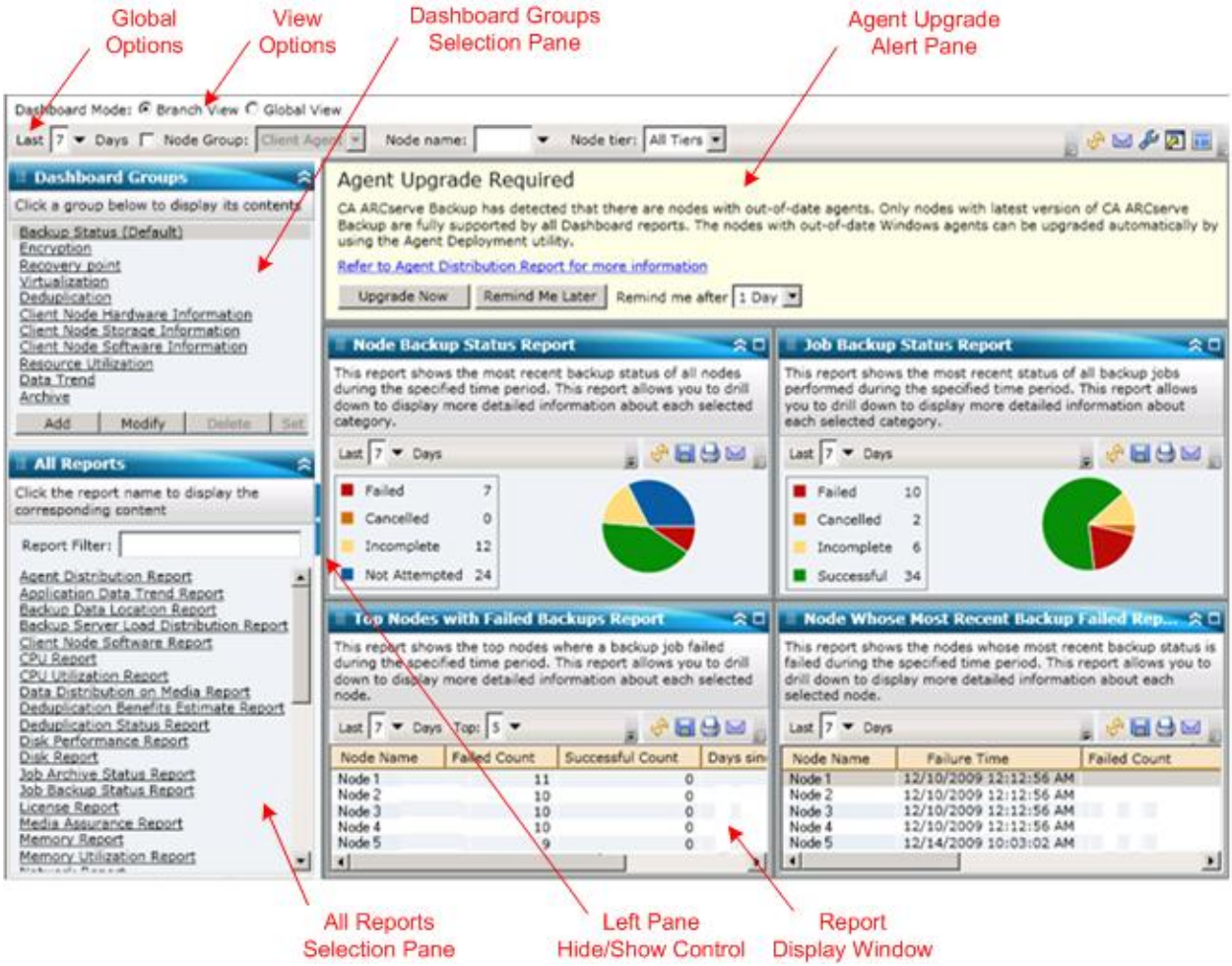
Dashboard contains the following features:

- Provides a central snapshot overview of your backup infrastructure and your storage resource management (SRM) environment.
- Provides 41 individual reports, focusing on such items as jobs, nodes, tapes, encryption, resources of agent machines etc.
- Provides the capability to customize the look of 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.
- Provides Global Dashboard capability to view dashboard-related information for multiple primary servers from a central location.

Dashboard GUI

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



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 57).

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 19).

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 Arcserve Backup agents that are at a version older than r12.5. For more information, see Agent Upgrade Alert (see page 64).

Dashboard Mode

This option lets you specify the Dashboard Mode to be displayed.

- The Branch View mode displays the dashboard-related information for only the local server, without any other branch site details or global dashboard options.
- The Global View mode displays the dashboard-related information for the local server and also for any or all branch sites. From the Global View mode additional global dashboard options become available.

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.

Line Chart Display

Line charts are used to show trends over time by connecting a series of data points together with a line.

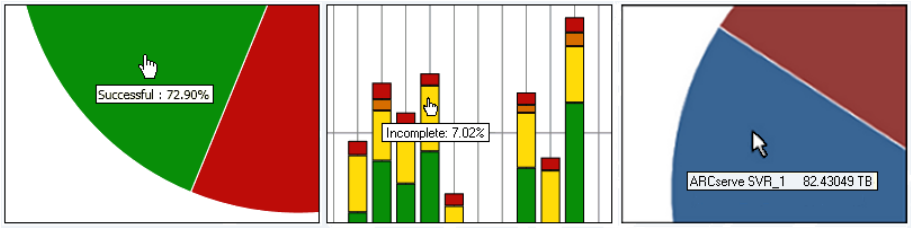
Tabular View

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

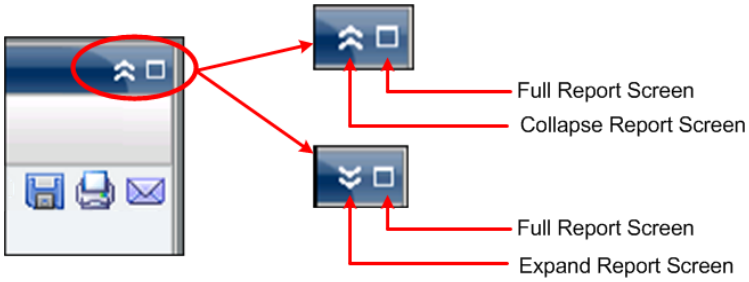
For any of these graphical displays, when you hover the mouse cursor over a particular category of a report, a small box appears under the cursor displaying the category and its corresponding value.

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.



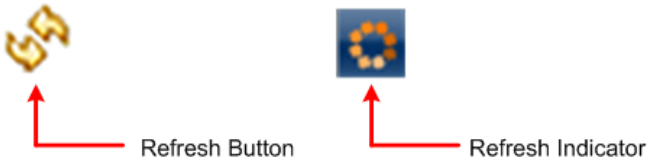
Report Displaying

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.



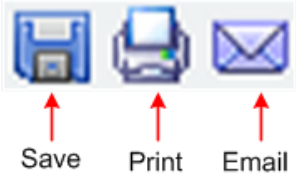
Data Exporting

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*.

Note: Microsoft Excel does not always render multi-byte characters properly.



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

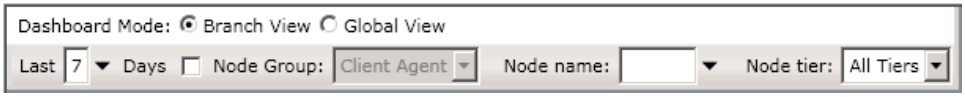
Each report contains various configuration options that let you customize the look and performance of Arcserve Backup Dashboard to meet your specific needs and preferences. For many of the reports, you can select such features as how the graphical information is displayed, the time period for the report, 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.

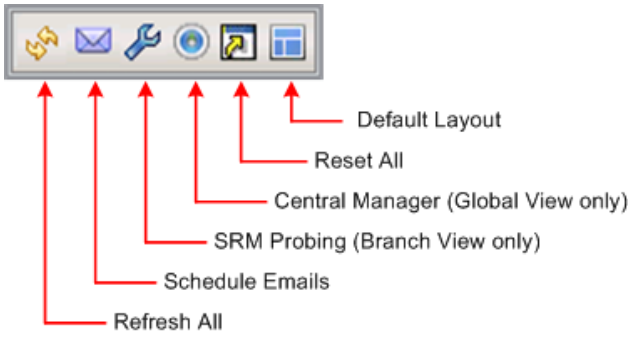
Any parameter or configuration settings that you make to the individual reports remain with the same settings when you close and re-open Dashboard. It does not automatically return to the default settings. In addition, to further enable customized reports, the configuration settings that you make to 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

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.





Dashboard Mode

Specifies the Dashboard Mode to be displayed.

- The Branch View mode displays the dashboard-related information for only the local server, without any other branch site details or global dashboard options.
- The Global View mode displays the dashboard-related information for the local server and also for any or all branch sites. From the Global View mode additional global dashboard options become available.

  Note: For all Dashboard reports, when you access a report using the Global View option, an additional filter is available to let you limit the data displayed by specifying the Branch name (or selecting the Branch name from the drop-down menu). In addition, all table format reports will be expanded to include an additional column to list the Branch Name.

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 Group

You can specify to filter the displayed data that is included in all reports based upon the Node Group.

Each dashboard report that contains a Node Name filter also has the capability to include a Node Group filter. The Node Group filter is only displayed on a report if a Node Group already exists. If a Node Group exists, the group name will be displayed in the Node Group filter drop-down menu and lets you specify how to filter the information being displayed on that report. This selection will only be applied to the corresponding dashboard report and allows you to further filter the displayed information by a specific node within the specified node group.

For Global Dashboard, if you select the Global View and also select multiple branches to monitor, only the Node Groups which exist in all the selected branches will be displayed in the Node Group drop-down menu.

For example, if you have a Branch Group which has three branch sites (Branch 1, Branch 2, and Branch 3) and within each branch site you have the following Node Groups.

- Branch 1: Node Group A, Node Group B
- Branch 2: Node Group B, Node Group C
- Branch 3: Node Group B, Node Group D

When you select this Branch Group in the Branch filter, only Group B will be displayed in the Node Group filter because this is the only Node Group that exists in all selected branches.

Note: Node Groups (or Server Groups) are created in Arcserve Backup from the Backup Manager (or from the Job Status Manager). For more information about creating Node Groups, see the *Administration Guide*.

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 62).

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: High Priority, Medium Priority, and Low Priority. The Node tier field contains a drop-down menu listing each tier category to select from.

For more information, see Node Tiers (see page 61).

Default: All Tiers

Refresh All

Refreshes all reports to display the most current data.

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 24).

SRM Probing

This option is only available when you select the Branch View mode.

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 33).

Central Manager

This option is only available when you select the Global View mode.

Lets you access the Central Manager. The Central Manager provides a snapshot overview of your entire Global Dashboard environment. This user interface lets you quickly and easily monitor the status of any or all registered branch sites from a single location.

For more information, see Understanding Central Manager (see page 66).

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.

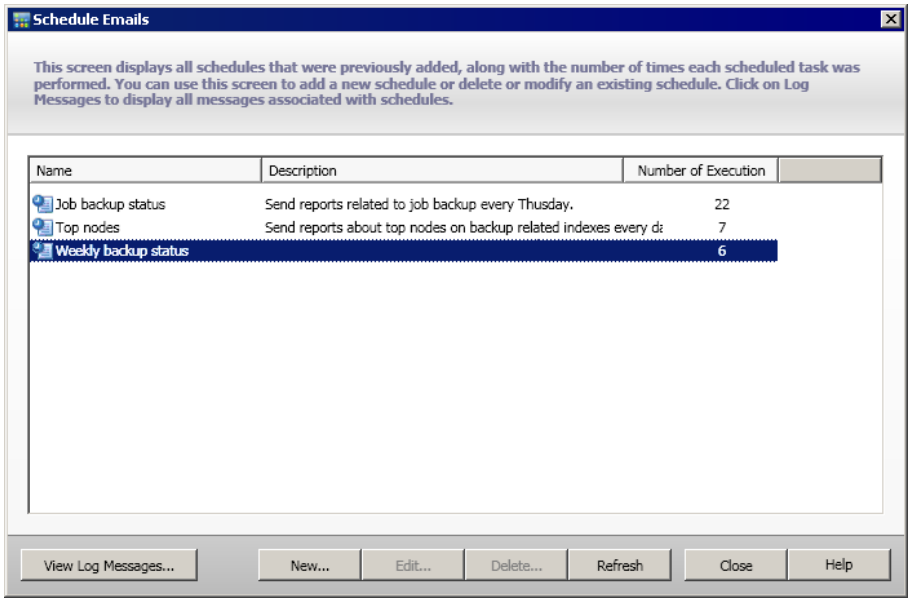
Configure Email Reports

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 30).

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*.

Add a new Email Report

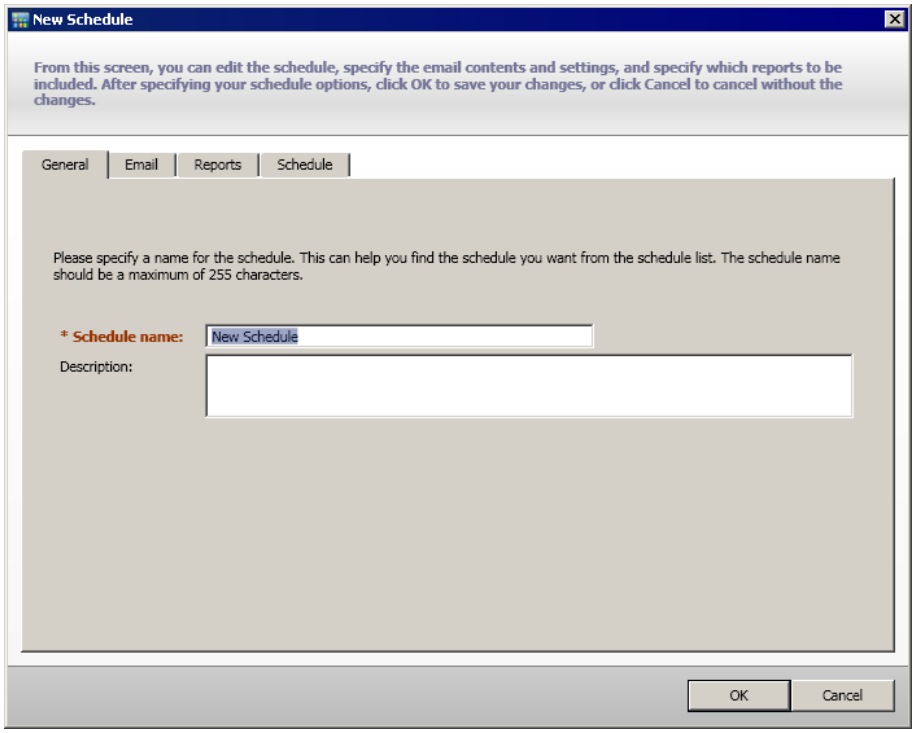
1. From the global options toolbar, click the Schedule Email icon.

   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.

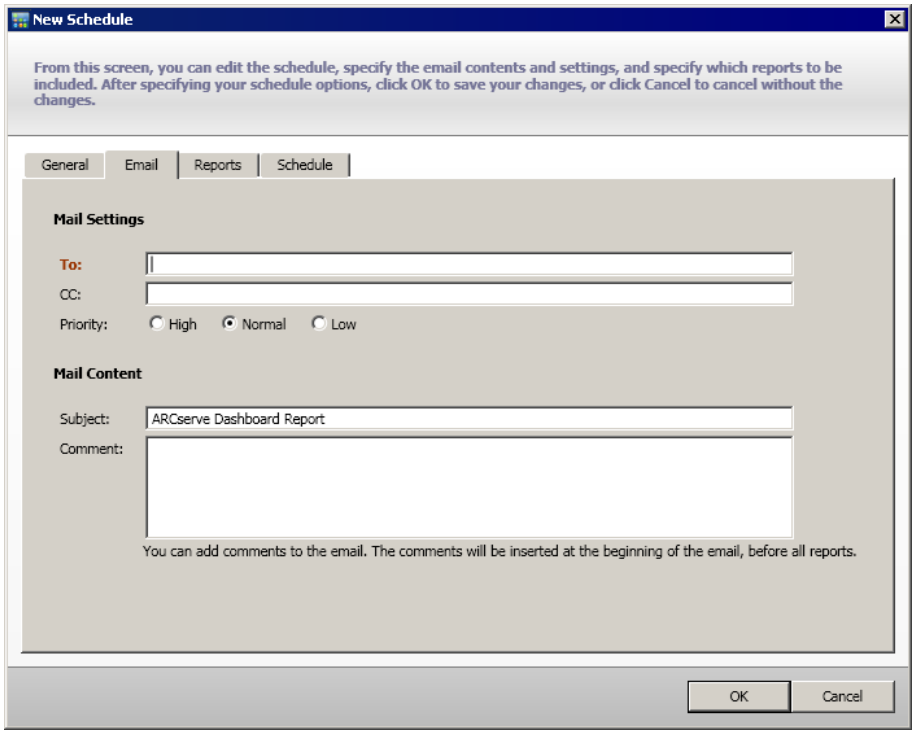


3. Enter a schedule name and a brief description for the new schedule.

   The new report name and corresponding description are saved.

4. Click the Email tab.

   The email settings dialog opens.



5. 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.

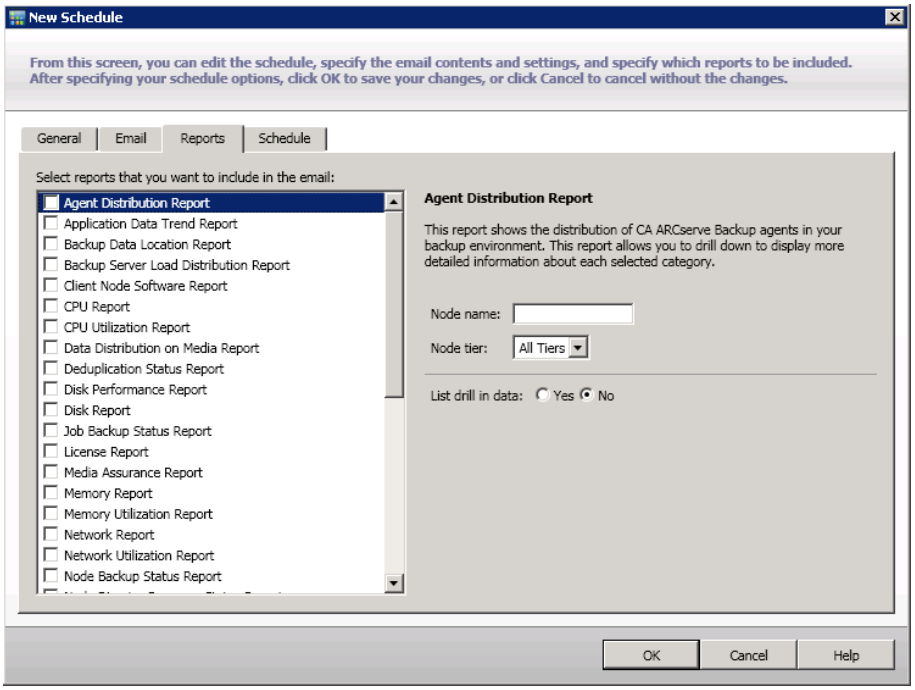
   Note: To enter multiple email addresses, each address must be separated by a semi-colon character.

   You can also specify the priority of the scheduled email (High, Normal, 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.

6. Click the Reports tab.

   The reports settings dialog opens.



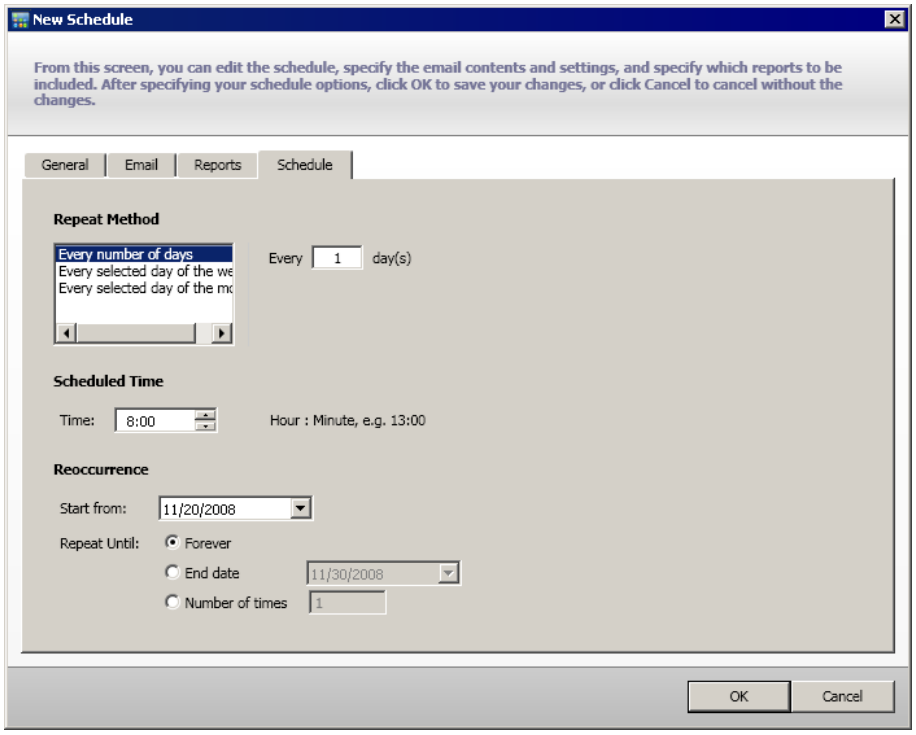
7. Select the report(s) to be included in the email and the parameters for each report.

   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.



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 number of 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 day of the week**

     If you select Every selected day of the week, 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).

   - **Every selected day of the month**

     If you select Every selected day of the 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.

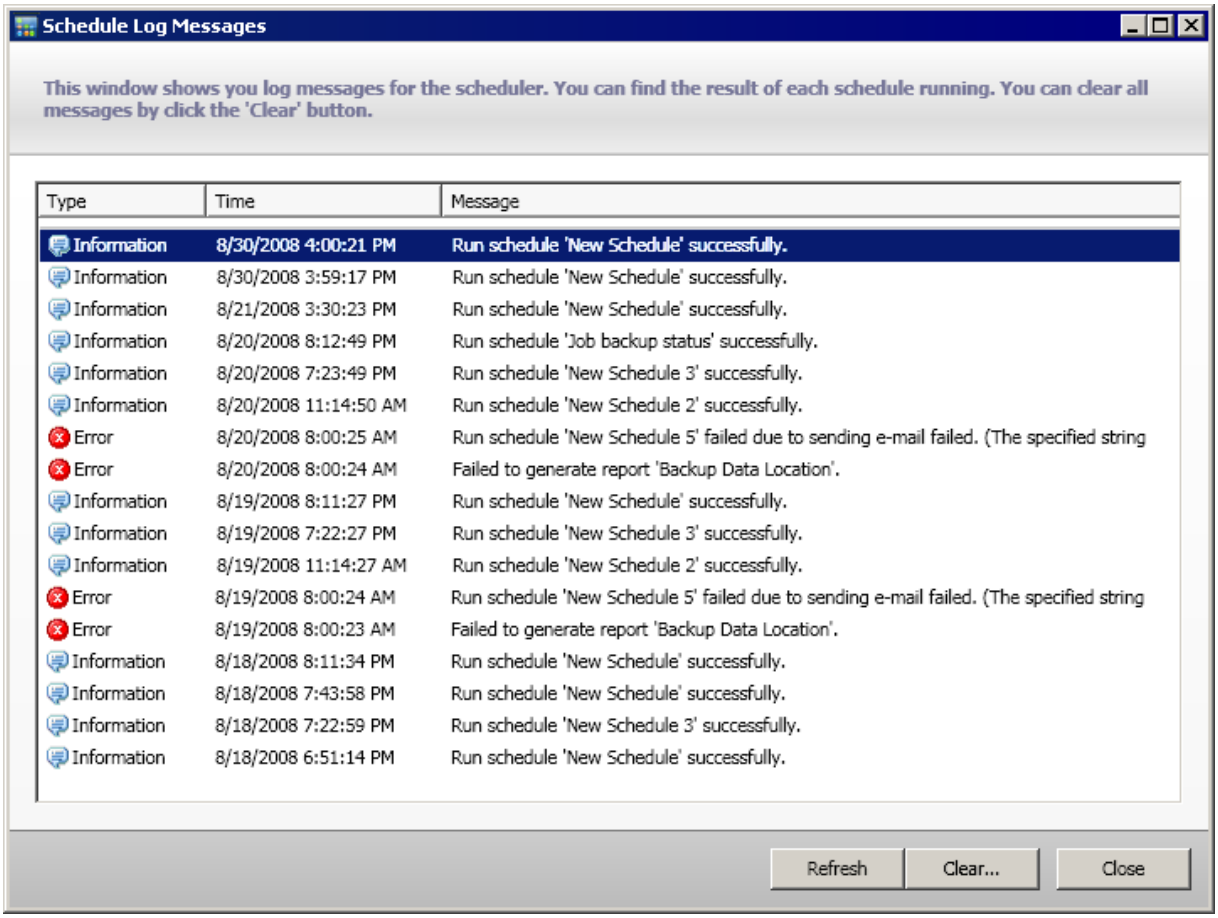
10. Click OK.

    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*.



Type	Time	Message
Information	8/30/2008 4:00:21 PM	Run schedule 'New Schedule' successfully.
Information	8/30/2008 3:59:17 PM	Run schedule 'New Schedule' successfully.
Information	8/21/2008 3:30:23 PM	Run schedule 'New Schedule' successfully.
Information	8/20/2008 8:12:49 PM	Run schedule 'Job backup status' successfully.
Information	8/20/2008 7:23:49 PM	Run schedule 'New Schedule 3' successfully.
Information	8/20/2008 11:14:50 AM	Run schedule 'New Schedule 2' successfully.
Error	8/20/2008 8:00:25 AM	Run schedule 'New Schedule 5' failed due to sending e-mail failed. (The specified string
Error	8/20/2008 8:00:24 AM	Failed to generate report 'Backup Data Location'.
Information	8/19/2008 8:11:27 PM	Run schedule 'New Schedule' successfully.
Information	8/19/2008 7:22:27 PM	Run schedule 'New Schedule 3' successfully.
Information	8/19/2008 11:14:27 AM	Run schedule 'New Schedule 2' successfully.
Error	8/19/2008 8:00:24 AM	Run schedule 'New Schedule 5' failed due to sending e-mail failed. (The specified string
Error	8/19/2008 8:00:23 AM	Failed to generate report 'Backup Data Location'.
Information	8/18/2008 8:11:34 PM	Run schedule 'New Schedule' successfully.
Information	8/18/2008 7:43:58 PM	Run schedule 'New Schedule' successfully.
Information	8/18/2008 7:22:59 PM	Run schedule 'New Schedule 3' successfully.
Information	8/18/2008 6:51:14 PM	Run schedule 'New Schedule' successfully.

Report-Specific Options

The following report-specific options can be individually set to customize each 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

Backup Types

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

- **Normal Backup** - A normal backup lets you back up a data source to a target destination, using a custom schedule, repeat method, or rotation scheme.
- **Synthetic Backup** - A synthetic full backup (SFB) is a synthesized backup. It is created by consolidating the most recent full backup and subsequent incremental/differential backups. (The resulting synthetic full backup is identical to what would have been created had the last backup had been a full backup).

Default: All

Server

You can specify to filter the displayed information that is included in the report based upon the corresponding Arcserve Backup server. The Server is a drop-down menu and lets you select all Arcserve Backup servers or an individual Arcserve Backup server (Primary or Member) that is part of the 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: High Priority, Medium Priority, and Low Priority. The Node Tier field contains a drop-down menu listing each tier category to select from.

For more information, see Node Tiers (see page 61).

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

Branch Drop-Down Menu

The Branch drop-down menu lets you specify how to filter the information being displayed on the Global Dashboard Console. The selection from this menu will be applied to all displayed dashboard reports. From this menu you can select to display dashboard-related information for all branch sites or filtered for just the branch sites that are not assigned to a branch group, a specified branch group, or a specified single branch site. The Ungrouped filter will display all branch sites that are not part of any branch group.

Default: All Branch Sites

Branch Filter

Each dashboard report also contains a Branch filter drop-down menu to let you specify how to filter the information being displayed on that report. This selection will only be applied to the corresponding dashboard report and allows you to further filter the displayed information by a specific branch site within the specified branch group.

Default: All

Node Group Filter

Each dashboard report that contains a Node Name filter also has the capability to include a Node Group filter. The Node Group filter is only displayed on a report if a Node Group already exists. If a Node Group exists, the group name will be displayed in the Node Group filter drop-down menu and lets you specify how to filter the information being displayed on that report. This selection will only be applied to the corresponding dashboard report and allows you to further filter the displayed information by a specific node within the specified node group.

For Global Dashboard, if you select the Global View and also select multiple branches to monitor, only the Node Groups which exist in all the selected branches will be displayed in the Node Group drop-down menu.

For example, if you have a Branch Group which has three branch sites (Branch 1, Branch 2, and Branch 3) and within each branch site you have the following Node Groups.

- Branch 1: Node Group A, Node Group B
- Branch 2: Node Group B, Node Group C
- Branch 3: Node Group B, Node Group D

When you select this Branch Group in the Branch filter, only Group B will be displayed in the Node Group filter because this is the only Node Group that exists in all selected branches.

Note: Node Groups (or Server Groups) are created in Arcserve Backup from the Backup Manager (or from the Job Status Manager). For more information about creating Node Groups, see the *Administration Guide*.

SRM Prober Settings

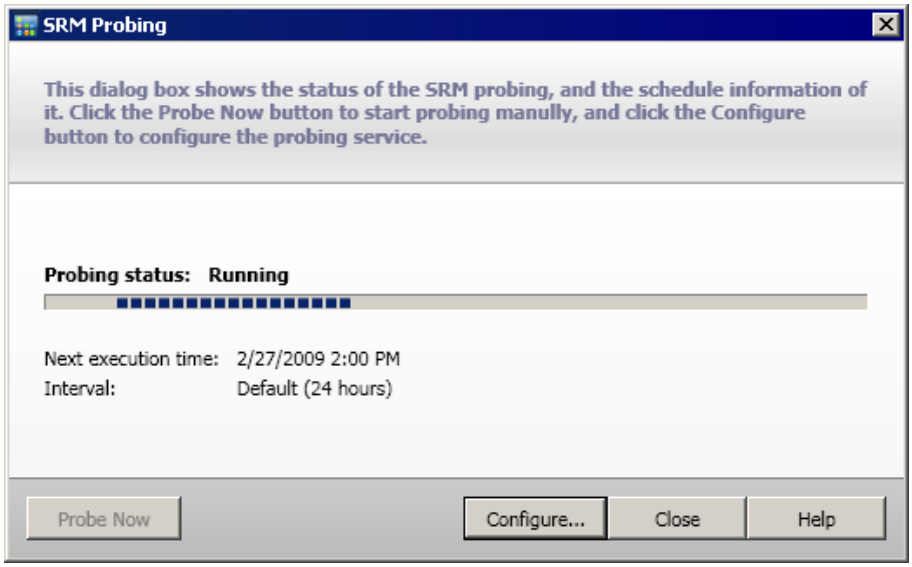
The SRM prober is a data-collection utility that when invoked, probes or communicates with all machines in your storage environment that have Arcserve Backup agents r12.5, r15, and r16 running on a supported Microsoft Windows Operating System. These machines send back an updated response containing all related information to be included in the SRM-type reports.

This option is only available when you select the Branch View mode.

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

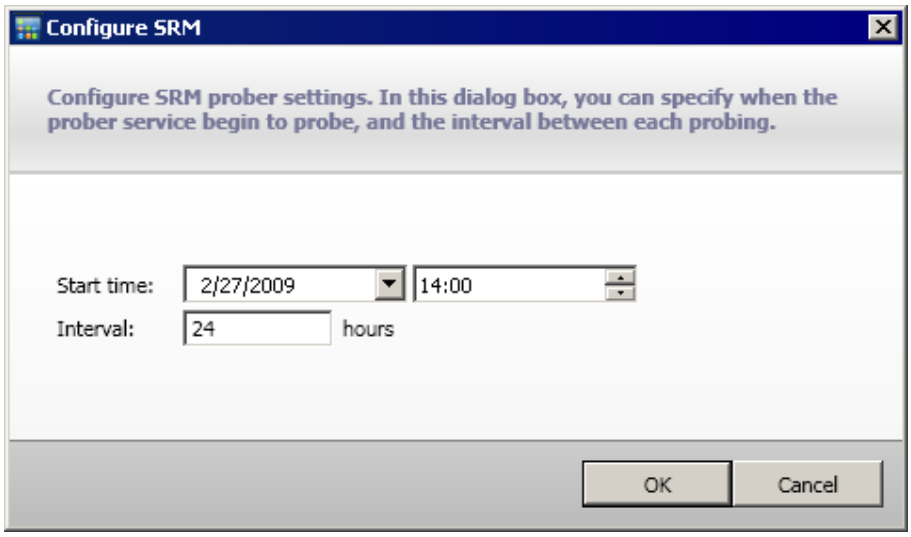
From the global options toolbar, you can click the SRM Prober button to open the SRM Probing dialog. From this dialog you can select to immediately initiate an SRM probe or configure the SRM prober settings to perform this probe at a scheduled time.

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



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

  By default, 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 230) to enhance this performance to meet your needs.

Chapter 2: Understanding Global Dashboard

This section contains the following topics:

Introduction (see page 35)
Features (see page 36)
Terms and Definitions (see page 36)
Global Dashboard Services (see page 38)
How Global Dashboard Works (see page 40)

Introduction

Global Dashboard is a user interface tool that provides you with a single network-based console from which you can monitor and report dashboard information for multiple Arcserve Backup domains across your enterprise. Arcserve Backup Dashboard displays a snapshot overview of the backup infrastructure and storage resource management (SRM) environment for just the Arcserve Backup primary server that you are connected to. Global Dashboard expands on this capability to let you quickly and easily view this dashboard information for multiple Arcserve Backup primary servers, both in your main office and in remote offices, all from a central location. This centralized monitoring capability through Global Dashboard means better information being reported on the performance and operation of your entire Arcserve Backup and SRM environment.

Remote office and branch office (ROBO) contain dashboard-related information for the individual branch primary server. Because such remote offices often have relatively limited on-site resources, ROBO may need to integrate the on-site dashboard information with those of the entire organization. Rather than attempting to monitor data at each site, Global Dashboard can synchronize this on-site data to let you remotely view dashboard information for any individual primary server (or group of primary servers) from a central location or provide a consolidated dashboard display of several primary servers. Global Dashboard can display consolidated reports for all branches, a customized group of branches, or a single branch.

Features

Global Dashboard contains the following features:

- Provides the capability to view Dashboard reports for multiple primary servers within your enterprise (local or remote) to help monitor and evaluate each individual server from one central location.
- Provides the capability to view dashboard reports for all branches, a customized group of branches, or a single branch.
- Provides the capability to manage all associated branches from one central location. Operations that can be performed include suspending a branch, deleting a branch, viewing message logs, changing configuration settings, and so on.
- Automatically synchronizes the dashboard data from all Branch Primary Servers to the Central Primary Server to provide current and refreshed central monitoring.
- Provides the capability to customize the individual or group of Branch Primary Servers being monitored to meet your specific needs and preferences. (A Branch Primary Server can be part of multiple branch groups).
- Provides the capability to filter the data being displayed on any dashboard report based upon specified branch parameters.
- Provides the capability to export the collected data for the reports as a CSV file for use in a spreadsheet. You can also print or email these reports.
- Provides the capability to track the status of individual Branch Primary Servers through a newly added Branch Manager GUI. From this GUI, you can view logs, check the status of last synchronization, and perform a full synchronization.

Terms and Definitions

Before you can understand the details of Global Dashboard, you must be familiar with some of the terms and definitions used by this utility.

Global Dashboard uses the following terms and definitions:

Central Primary Server

The Central Primary Server (and its associated Arcserve Backup database) is the central hub interface for storing synchronized dashboard-related information received from Branch Primary Servers. Within your Arcserve Backup environment, there can only be one primary server configured as the Central Primary Server, and a Branch Primary Server can only report to one Central Primary Server. All associated Branch Primary Servers need to be registered with this Central Primary Server to enable network communication. Communication is always one way, from a branch site to the central site. The terms Central Primary Server and Central Site are used interchangeably in this document.

Branch Primary Server

Any primary server (or stand-alone server) within your Arcserve Backup environment can be configured to be a Branch Primary Server. A Branch Primary Server synchronizes dashboard-related information to the designated Central Primary Server. All data is transmitted from the Branch Primary Server to the associated Central Primary Server. Within your Arcserve Backup environment, there can be multiple Branch Primary Servers, but only one Central Primary Server. In addition, a Branch Primary Server can only report to one Central Primary Server. After a primary server is configured as a Branch Primary Server and registered with the associated Central Primary Server, the corresponding dashboard data can be automatically synchronized with the Central Primary Server. The terms Branch Primary Server and Branch Site are used interchangeably in this document.

Global Dashboard Console

The Global Dashboard Console is the user interface for displaying the synchronized dashboard information (reports). The Global Dashboard Console is basically an expanded version of the Arcserve Backup Dashboard GUI, with some additional capabilities and options. All dashboard reports that can be displayed from the Arcserve Backup Dashboard can also be displayed from the Global Dashboard Console. However, the Global Dashboard Console lets you view these dashboard reports for any one or group of registered branch sites.

Central Manager

The Central Manager provides a snapshot overview of your entire Global Dashboard environment. This user interface lets you quickly and easily monitor the status of any or all registered branch sites from a single location. The Central Manager also displays any log messages associated with the branch sites. The Central Manager is accessible from the Global Dashboard Console (when the Global View mode is selected) by clicking the icon button on the Global Dashboard toolbar.

For more information, see Understanding Central Manager (see page 66).

Data Synchronization

Data synchronization is the process of transmitting dashboard-related information from a branch site database to the central site database so that the central database contains (and reports) the same information as each of the registered branch databases. For Global Dashboard, the initial data synchronization will always be a full data synchronization. All subsequent data synchronizations will be incremental. Incremental synchronization is synchronizing the data that was modified, deleted, or added since the last synchronization was performed. The synchronized data is compressed to minimize size prior to transmittal.

During a full synchronization process, the Arcserve Backup database engine will be shut down for a few minutes. During an incremental data synchronization, no Arcserve Backup services will be shut down.

The full data synchronization process is basically a three-step process:

- Export the dashboard-related data from the branch database to files.
- Transfer the exported files from the branch site to the central site.
- Import the dashboard-related data from the files to the central database.

The incremental data synchronization process is basically a three-step process:

- Read data from Arcserve Backup database event log table on the branch site.
- Transfer the changed dashboard-related data from the branch site to the central site.
- Import the changed dashboard-related data to the central database.

Global Dashboard Services

When Global Dashboard is installed on your primary server, there are also corresponding services that are installed and registered with the Windows Service Control Manager (SCM). The SCM maintains a database of installed services in the registry.

Note: These services will only be enabled in Arcserve Backup after Global Dashboard has been configured.

The following Global Dashboard services are installed:

Central Site:

- **Arcserve Central Remoting Server**

  Allows communication between a branch site and the central site.

- **Arcserve Communication Foundation (Global)**

  Provides data used by Arcserve Backup Global Dashboard.

- **Arcserve Dashboard Sync Service**

  Allows a branch site to synchronize data to the central site database. This is required because the central site itself acts a local branch site.

- **Arcserve Communication Foundation**

  Provides data used by Arcserve Backup Dashboard.

Branch Site:

- **Arcserve Dashboard Sync Service**

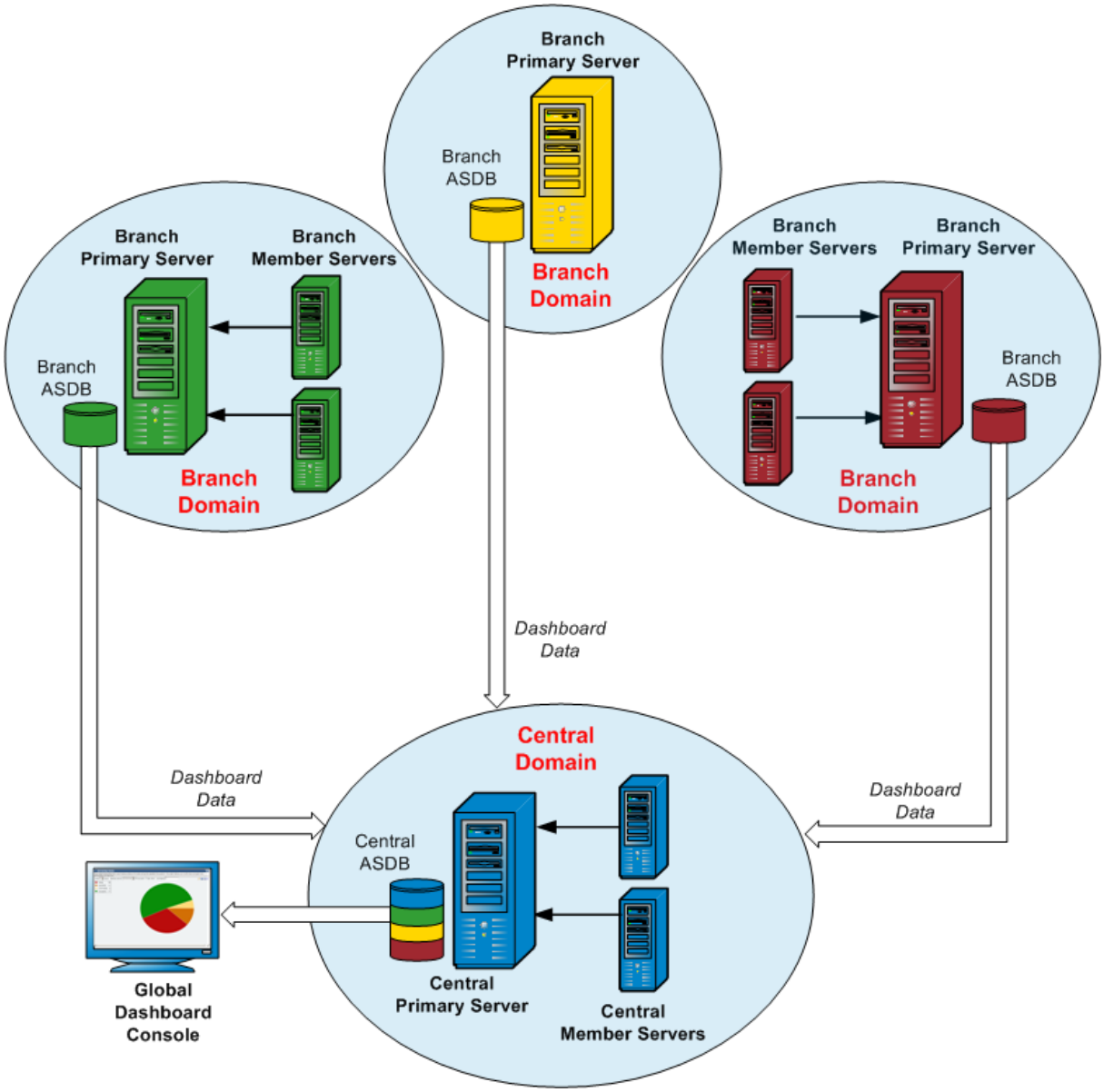
  Allows a branch site to synchronize data to the central site database.

- **Arcserve Communication Foundation**

  Provides data used by Arcserve Backup Dashboard.

How Global Dashboard Works

A Global Dashboard environment consists of a designated Central Domain and its associated Branch Domains. Within each domain is a Arcserve Backup server and a corresponding Arcserve Backup database (ASDB). The Arcserve Backup server can be either a stand-alone server or a primary server with its associated member servers.



When the Global Dashboard environment is first setup, you must specify which server will be configured as the Central Primary Server and which server(s) will be registered as the connected Branch Primary Servers. Generally, the Central Primary Server should be capable of receiving, processing, and storing large amounts of transmitted data. There can only be one Central Primary Server within each Global Dashboard environment. However, there can be any number of Branch Primary Servers (depending upon the performance limitations of the Central Primary Server), and they can be located either locally or remotely. In addition, a Branch Primary Server can only report to one Central Primary Server.

Dashboard Data (Arcserve Backup data and SRM-related data) from the individual Branch Primary Servers is stored in each corresponding ASDB. The Global Dashboard utility provides the interface between each Branch Domain and the Central Domain. When invoked (either automatically as scheduled or manually), the collected dashboard data from each Branch ASDB is synchronized to the Central Domain, where it is processed by the Central Primary Server and stored in the Central ASDB. (All communication is always one way, from the Branch Domain to the Central Domain). The initial transfer of this synchronized data from the Branch Domain is a full upload, and each subsequent transfer after that will be an incremental upload of only the data that has been modified, deleted, or added since the last synchronization was performed. During a full synchronization process, the Arcserve Backup database engine will be shut down for a few minutes. During an incremental data synchronization, no Arcserve Backup services will be shut down. For any data synchronization, file details (file name, size, path, and so on) will not be sent to the Central Domain. Any database pruning that is performed at a Branch ASDB will be reflected in the Central ASDB the next time data synchronization is performed.

The Global Dashboard Console is the user interface connected to the Central ASDB. From this Global Dashboard Console, you can monitor the synchronized dashboard data collected from any or all of the associated branches. You can specify which individual dashboard reports (or group of reports) will be displayed for which server. From the Global Dashboard Console you can also view consolidated dashboard data from a group of Branch Domains or from all Branch Domains within your Global Dashboard environment.

Chapter 3: Configuring Global Dashboard

This section contains the following topics:

Configuration Considerations (see page 43)
Configure Global Dashboard (see page 44)

Configuration Considerations

Configuration of Global Dashboard can be performed during or after installation of Arcserve Backup. However, before you configure Global Dashboard, consider the following:

- Which server within your Global Dashboard environment will be configured as the Central Primary Server?

  There can only be one Central Primary Server in a Global Dashboard environment.

  - When selecting the Central Primary Server, the main consideration should be database size. Ensure the selected Central Primary Server is capable of storing dashboard data received from all registered Branch Primary Servers.
  - Server performance should also be considered when selecting the Central Primary Server to help ensure fast, efficient, and reliable data interface between the Central Primary Server and all associated Branch Primary Servers.
  - Database type should also be considered when selecting the Central Primary Server.

    For Global Dashboard, the Central Primary Server only supports Microsoft SQL Server 2005/2008/2008 R2/2012. It does not support Microsoft SQL Server 2005/2008 Express and Microsoft SQL Server 2000.

- Which servers within your Global Dashboard environment will be configured as Branch Primary Servers?

  At each server location, the Branch Primary Server must be a primary/stand-alone server within the Arcserve Backup domain (not a domain member server).

- During the configuration process, the Arcserve Backup database engine will be shut down for a few minutes. Plan your installation at a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled.

- In a Global Dashboard domain, if you are demoting a Branch Primary Server to a member server or changing which primary server will be configured as the Central Primary Server, you may want to continue to use the collected information from the old primary server. Global Dashboard lets you export (and save) this information from the old primary server and import it into the new primary server.

License Requirements:

- To enable Global Dashboard capabilities, you must have a valid Arcserve Backup Global Dashboard license at the Central Primary Server, with multiple license counts to include all registered Branch Primary Servers. (Branch Primary Servers do not need to install a Global Dashboard license).
- Each registered Branch Primary Server will then occupy one count of the Global Dashboard license. If the registered branch count exceeds the maximum limit of the license, new branch sites will not be allowed to register to that Central Primary Server.
- A license status check will then be performed for each of the following scenarios
  - When registering a branch site
  - When re-registering a branch site
  - When performing full data synchronization
  - When performing incremental synchronization
- If the license status check fails, you will need to obtain additional licenses or re-allocate your existing licenses, to enable data synchronization to the Central Primary Server. (The status of each branch site license is displayed on the Central Manager dialog).

  Note: Deleting a branch server from the Central Manager will release the license count occupied by that branch and allow you to re-assign that license count to a different branch server.

Configure Global Dashboard

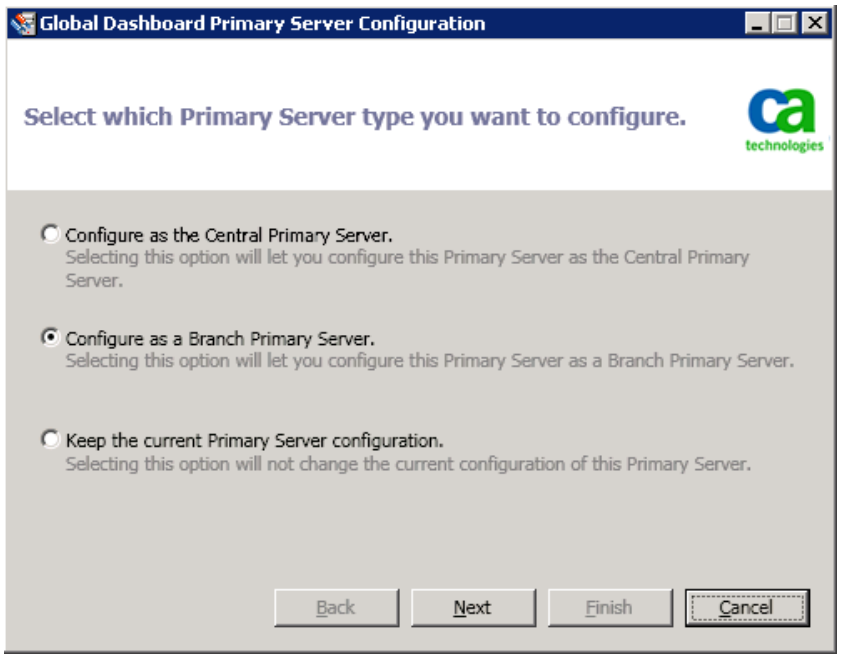
For Global Dashboard to work properly, it is important that the configuration process be performed at the central site and at each associated branch site to enable the necessary communication and synchronization of dashboard-related data from the branch site to the central site. You can configure the server immediately after installation or you can manually launch the configuration at a more convenient time from the Server Configuration Wizard.

Important! During the configuration process, the Arcserve Backup database engine will be shut down for a few minutes. Plan your configuration at a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled.

When you start the Global Dashboard configuration process, you must first select the type of primary server you want to configure. When making this selection, it is important to remember the following:

- Within your Arcserve Backup environment, there can only be one primary server configured as the Central Primary Server and a Branch Primary Server can only report to one Central Primary Server. When selecting the Central Primary Server, the main consideration should be database type and size. Make sure the selected Central Primary Server is Microsoft SQL Server 2005/2008/2008 R2/2012 and capable of storing dashboard data received from all registered Branch Primary Servers.
- Any primary server (or stand-alone server) within your Arcserve Backup environment can be configured to be a Branch Primary Server. A domain member server cannot be configured as a Branch Primary Server.
- All associated Branch Primary Servers must be registered with the Central Primary Server to enable synchronization.
- There are three roles for Global Dashboard: Central Primary Server, Branch Primary Server, and Global Dashboard Console.
  - The Global Dashboard Console role does not need configuration. After a Primary Server has selected the Global Dashboard option during installation, it automatically has Global Dashboard Console functionality.
  - A Primary Server with the Global Dashboard Console role can still be configured as the Central Primary Server or a Branch Primary Server.
  - After a Primary Server has been configured as the Central Primary Server or a Branch Primary Server, its role cannot be changed anymore.
  - The relationship of three roles is as follows:
    - A Branch Primary Server also has the functionality of a Global Dashboard Console.
    - The Central Primary Server also has the functionality of both a Branch Primary Server (there is a local branch) and a Global Dashboard Console.

- At the end of Arcserve Backup installation, setup will launch the Global Dashboard configuration utility. You can use this utility to configure your server as the Central Primary Server or a Branch Primary Server. If you only want to use the Global Dashboard Console functionality or you want to configure your server as the Central Primary Server or a Branch Primary Server at a later time, you can select the "Keep the current Primary Server configuration" option.



Configure the Central Site

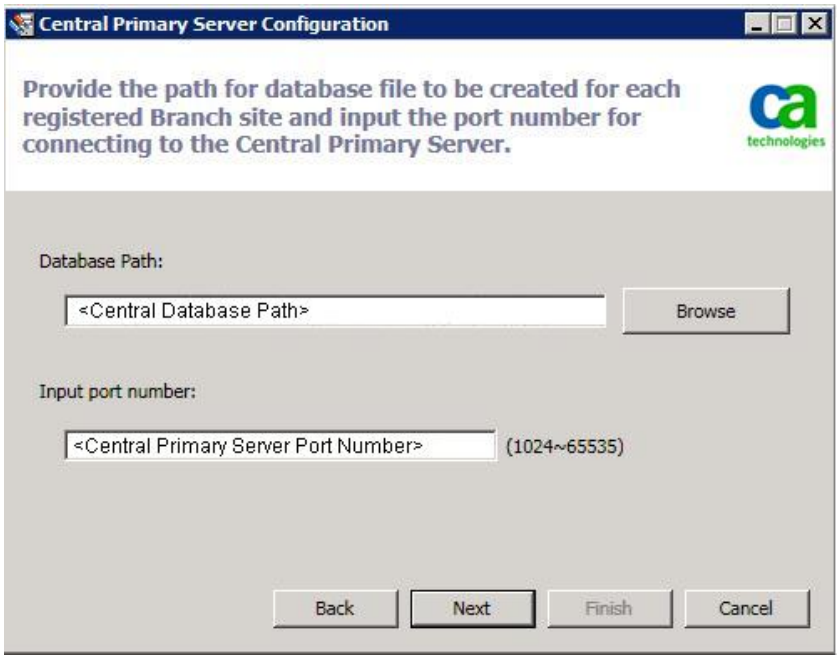
The parameters specified during the configuration of the central site must be used by each registered branch site to enable synchronization of dashboard-related data to the central site.

Note: The local Arcserve Backup database for the Central Primary Server will be treated the same as a normal branch site. However, you do not need to configure it manually because this was completed during setup of the Central Primary Server.

To configure the central site

1. Launch the Central Configuration wizard and click Next to start.

   The screen to provide the path and port information for the central site appears.



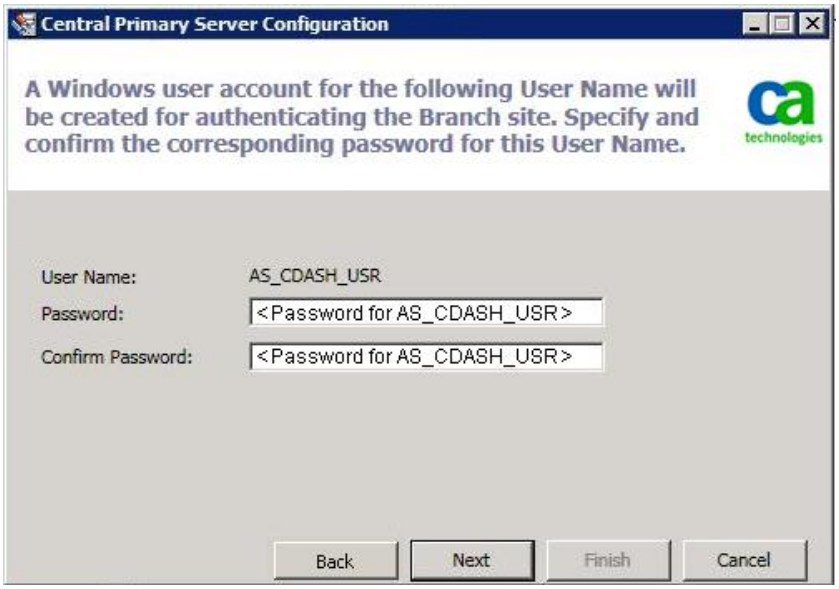
2. Specify the path for the central site database. (This will be the database location where the dashboard-related data from each branch site will be uploaded to and stored).

   Note: If a remote database is used as the ASDB of the Central Primary Server, the database path must be an existing path at the remote machine or else the configuration may fail.

3. Specify the input port number. This will be the port number for each Branch Primary Server to access the Central Primary Server. By default, the Port number is 18001, but can be changed from this screen.

4. Click Next.

   The screen to provide user authentication information appears.



5. Specify and confirm the password for the AS_CDASH_USR user name. A local Windows User with this account name and password will be created on the Central Primary Server. When a branch site connects to the central site, the connection will use this authentication information to allow access to the central site.

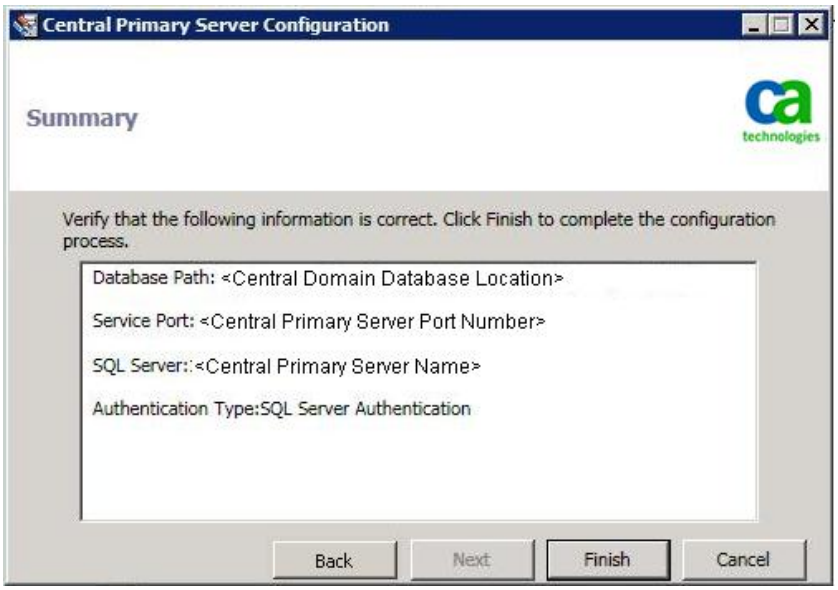
   This password is needed when each branch site wants to register to the Central Primary Server. If necessary, this password can be reset using the Windows User Management. However, if the password is changed, the new information must be manually reset at every branch site that is registered to this Central Primary Server.

   The "Set Password for AS_CDASH_USR" dialog for the Windows User Management is accessed from the Central Primary Server Start menu (Programs\Administrative Tools\Computer Management\Local Users and Groups\Users\AS_CDASH_USR\Set Password).

   Note: The pre-assigned user "AS_CDASH_USR" is for authentication purposes only. No other Arcserve Backup permissions are associated with this user name.

6. Click Next.

   The central site Summary screen appears.



7. The Summary screen displays all configuration-related information for the central Arcserve Backup database and the Central Primary Server. Verify that all displayed information is correct before continuing. If the information is correct, click Finish.

   An alert message appears reminding you that during the configuration process, the Arcserve Backup database engine will be shut down for a few minutes.

8. If it is a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled, click OK to continue.

   The configuration Progress screen appears displaying the status.

9. When the configuration process is finished, a confirmation screen appears. Click OK.

   The central site configuration process is completed.

Configure a Branch Site

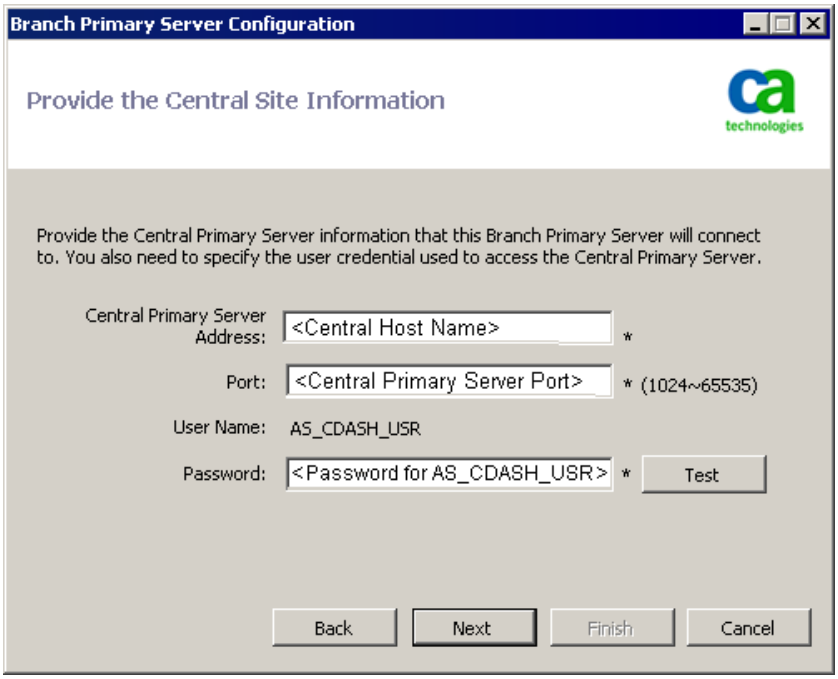
A branch site must be registered to the central site to enable synchronization of dashboard-related data to that central site. A branch site can only report to one Central Primary Server. To register your branch site, you must first configure it to communicate with the central site.

To configure a branch site

1. Launch the Branch Configuration wizard and click Next to start.

   The Provide Central Site Information screen appears.

   Important! For a branch site to properly communicate to the central site, you must provide three access and location parameters: the name (or IP address) of the Central Primary Server, the Port number to access the Central Primary Server, and the authentication Password for the AS_CDASH_USR user. You need to obtain this information before attempting to register your branch site.



2. Specify the name of the Central Primary Server, the Port number to the Central Primary Server, and the authentication Password.

   When the branch site connects to the central site, the connection will use this information to access the central site.

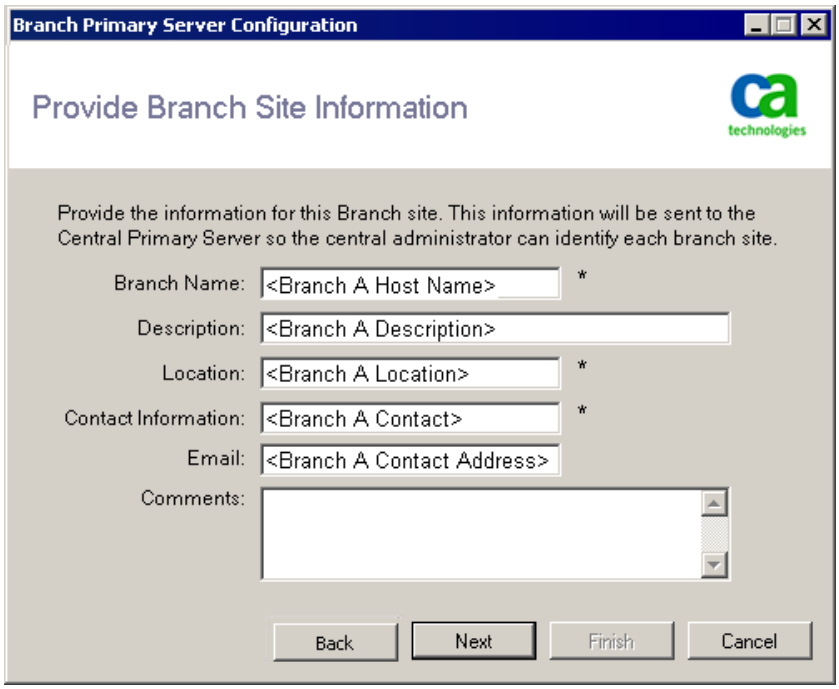
   By default, the Port number is 18001, but can be changed from the central site. For more information about changing the port number from the central site, see Configure the Central Site (see page 46).

3. Click Test to verify proper connection to the central site.

   A test connection status message appears.

4. If the test connection status is successful, click OK to continue. If the test connection status is not successful, verify you have the proper central site information specified before continuing.

   The Provide Branch Site Information screen appears.



5. You must specify the name of the Branch Primary Server, a location, and the name of the contact at that branch. In addition, you can also specify some additional branch-related information to further help the central site administrator to identify the branch site. Information such as the email address for the branch contact and any useful comments that you want the central site administrator to know can all be helpful in effectively maintaining your Global Dashboard environment.

   This information specified for the branch site user will be sent to the Central Primary Server and kept in the Central Primary Server database.

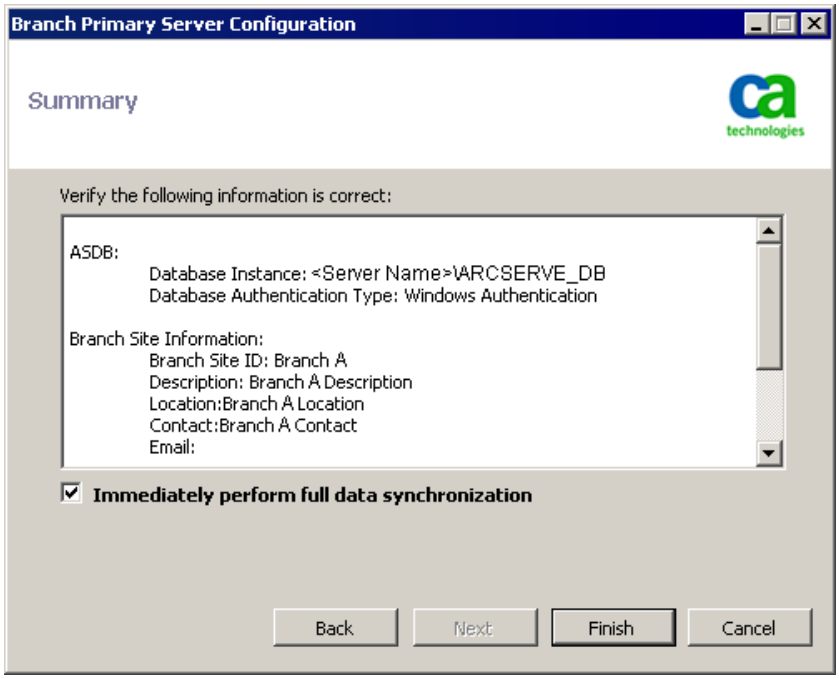
   Click Next to continue.

   a. If the name of the Branch Primary Server already exists, a message alert will appear informing you of this condition and requesting that you either specify a different branch name or have Arcserve Backup Global Dashboard automatically assign a new branch name (by appending a numerical suffix to your existing branch name).

      Click Yes to create an automatically appended branch name or click No to return to the Provide Branch Site Information screen and specify a different branch name.

b. If the name of the Branch Primary Server does not already exist, the branch configuration Summary screen appears.

The Summary screen displays all configuration-related information for the Central Arcserve Backup database, your branch site, and the Central Primary Server.



6. From the branch configuration Summary screen, you have the option to immediately perform a full data synchronization at this time.

Important! Data synchronization will temporarily interrupt and shut down the Arcserve Backup database engine and database for this branch site until the configuration and register process is complete. When the configuration and register process is finished, the Arcserve Backup database engine and all database functions will resume normally.

If you do not want to perform full data synchronization at this time, you can perform it after the configuration process is finished. For more information, see Manually Synchronize Data (see page 90).

Note: The initial data synchronization will always be a full data synchronization. All subsequent data synchronizations will be incremental.

7. From the branch configuration Summary screen, verify that all displayed information is correct before continuing. If the information is correct, click Finish.

The Configuration Progress screen appears displaying the status.

8. When the configuration and register process is finished, a confirmation screen appears. Click OK.

   The branch configuration process is completed and the branch site is now registered to the central site.

Chapter 4: Using Dashboard

This section contains the following topics:

Use Arcserve Backup Dashboard (see page 55)
Dashboard Groups (see page 57)
Node Tiers (see page 61)
Node Information (see page 62)
Send a Report by Email (see page 63)
Agent Upgrade Alert (see page 64)

Use Arcserve Backup Dashboard

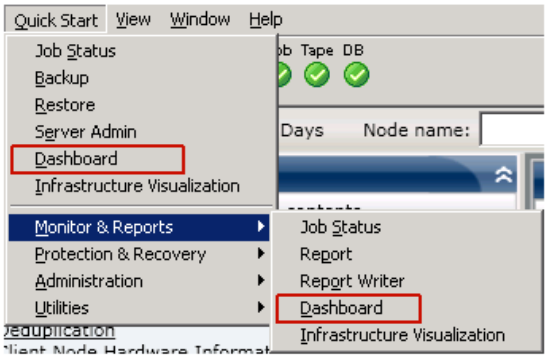
The Arcserve Backup Dashboard is a user interface tool that provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment. This dashboard view lets you quickly and easily monitor relevant information to help you manage the performance and operation 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 Arcserve Backup services are up and running prior to using Arcserve Backup Dashboard. For more information about starting Arcserve Backup services, see the Administration Guide.

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

To use Arcserve Backup Dashboard

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



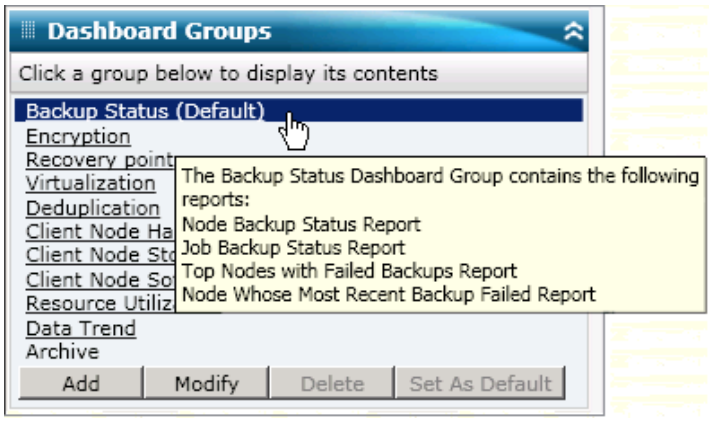
The Arcserve Backup Dashboard main screen appears, displaying a snapshot view that provides status reports of the specified Arcserve Backup environment.

2. The 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.



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.

Arcserve Backup Dashboard contains several pre-configured groups, which if necessary can be modified, but not deleted. In addition to the pre-configured 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.

You can also specify which Dashboard Group will be the default group by selecting the group and clicking the Set As Default button. (Default) will be displayed next to the group name to indicate the current default group. Each time you access Arcserve Backup Dashboard, it will open with the default Dashboard Group displayed.

The pre-configured Dashboard 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: Network 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.

Resource Utilization Dashboard Group

Contains the following reports: CPU Utilization Report, Disk Performance Report, Memory Utilization Report, and Network Utilization Report.

Data Trend Dashboard Group

Contains the following reports: Application Data Trend Report and Volume Trend Report.

Archive Dashboard Group

Contains the following reports: Job Archive Status Report, Node Archive Status Report, and Total Archive Size Report.

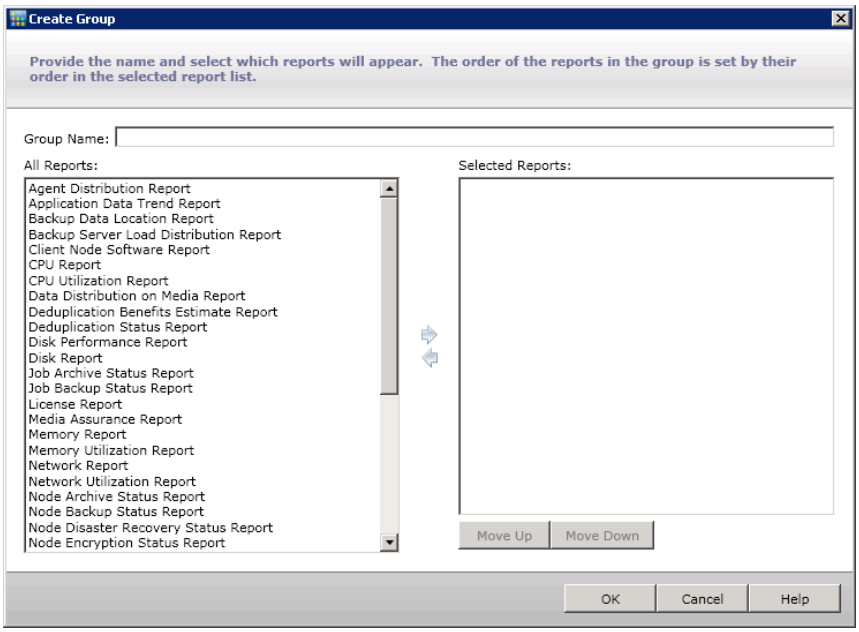
Add a Dashboard Group

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

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

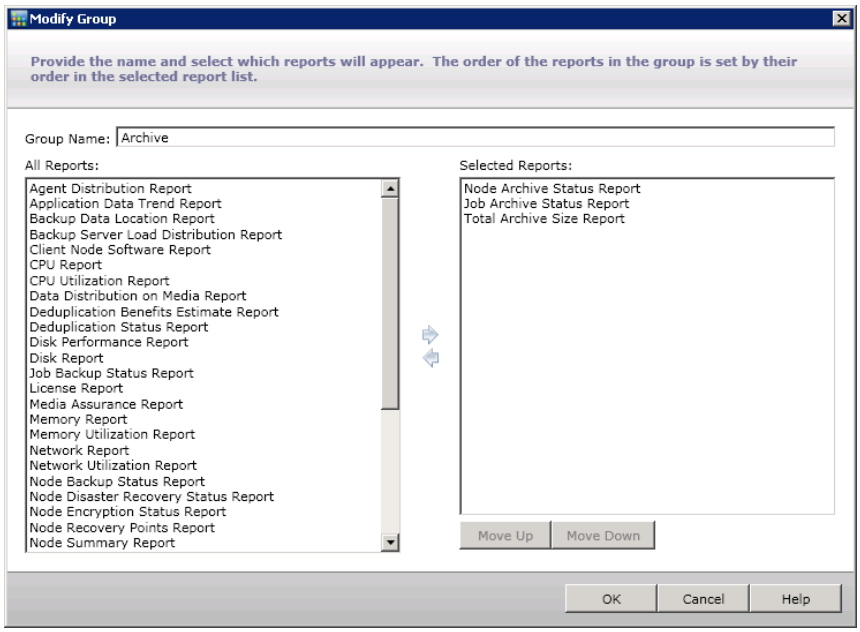
Modify a Dashboard Group

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

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 Arcserve Backup Server Admin or the Central Agent Admin to change the assigned priority classifications of your Arcserve Backup nodes. These tiers are used to filter the information displayed on the Arcserve Backup Dashboard by the priority level of the monitored nodes.

The Node Tier Configuration dialog contains three priority categories (High Priority, Medium Priority, and Low Priority), and is automatically populated when a node is added to your system and browsed. By default, a High Priority tier is configured to include all Arcserve Backup servers (Primary and Member) and any nodes with Arcserve Backup application agents installed (such as Oracle, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Sharepoint Server, and so on), and a Low Priority tier is configured to include all other nodes (having file system agents installed). The Medium Priority tier 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 Arcserve Backup Server Admin or from the Backup Manager (right-click Windows Systems in Source tab) or from the Central Agent Admin (right-click Windows Systems).

Notes:

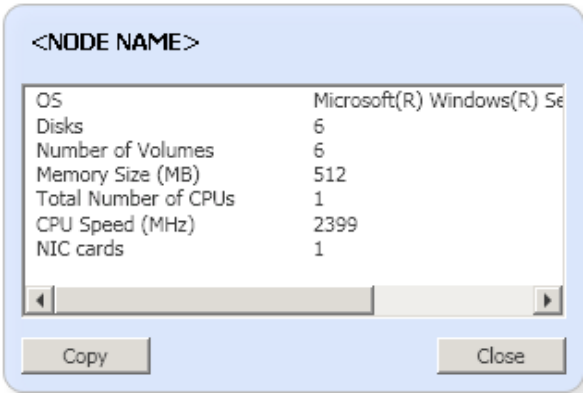
- For more information about Node Tier Configuration, see the *Administration Guide*.
- For more information about monitoring node tiers, see Node Tiers Report (see page 175).

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 memory 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 or later, this window will not display any information for such nodes because SRM information collection is not supported for non-windows nodes.



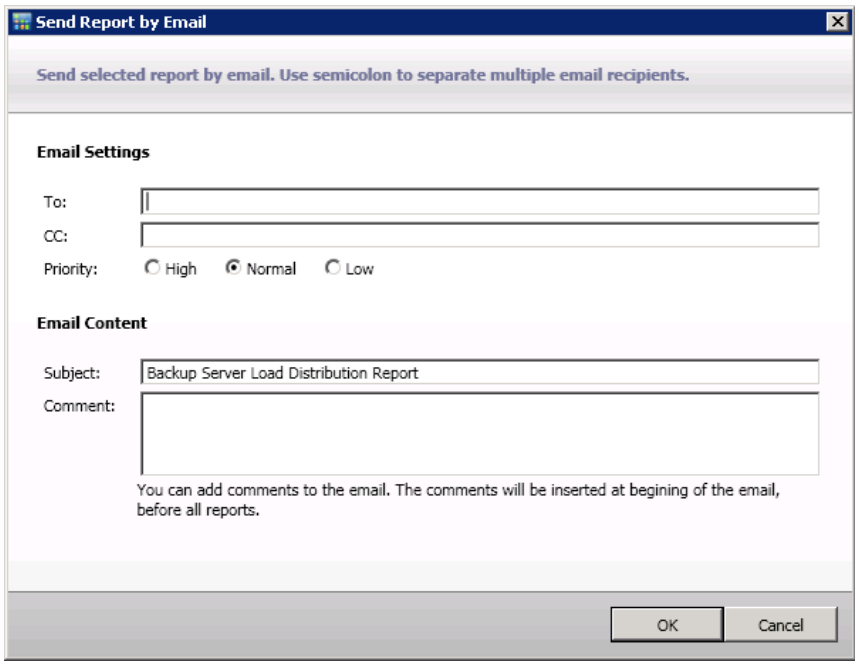
Send a Report by Email

All reports let you export collected data for the corresponding report. For each report you can specify if you want to email the report through a SMTP server. If you send a report by email, the content is the same as the printed content and all graphical charts are sent as embedded images.

To send a report by email

1. Click on the email icon (located at the upper right corner of each individual report).

   The Send Report by Email dialog opens.



2. 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.

3. Specify the priority of the scheduled email (High, Normal, or Low), add a comment to be included in the email, and enter the email subject.

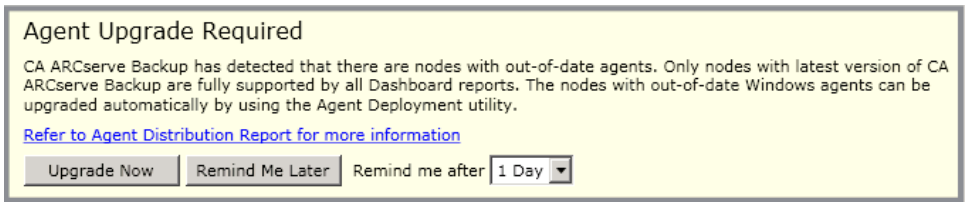
   Note: If you do not enter a subject, a pop-up confirmation window opens when you click the OK button.

4. Click OK.

   The email containing the corresponding report is sent to the recipients.

Agent Upgrade Alert

When you access Dashboard, Arcserve Backup Dashboard probes your backup environment to detect if any installed Arcserve Backup agents are at a version prior to latest version of Arcserve Backup. Dashboard can only monitor and report on nodes that have 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 Arcserve Backup agents prior to the latest version. 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.

Note: If you have not installed the Agent Deployment package during your 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 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 Arcserve Backup.

Chapter 5: Using Global Dashboard

This section contains the following topics:

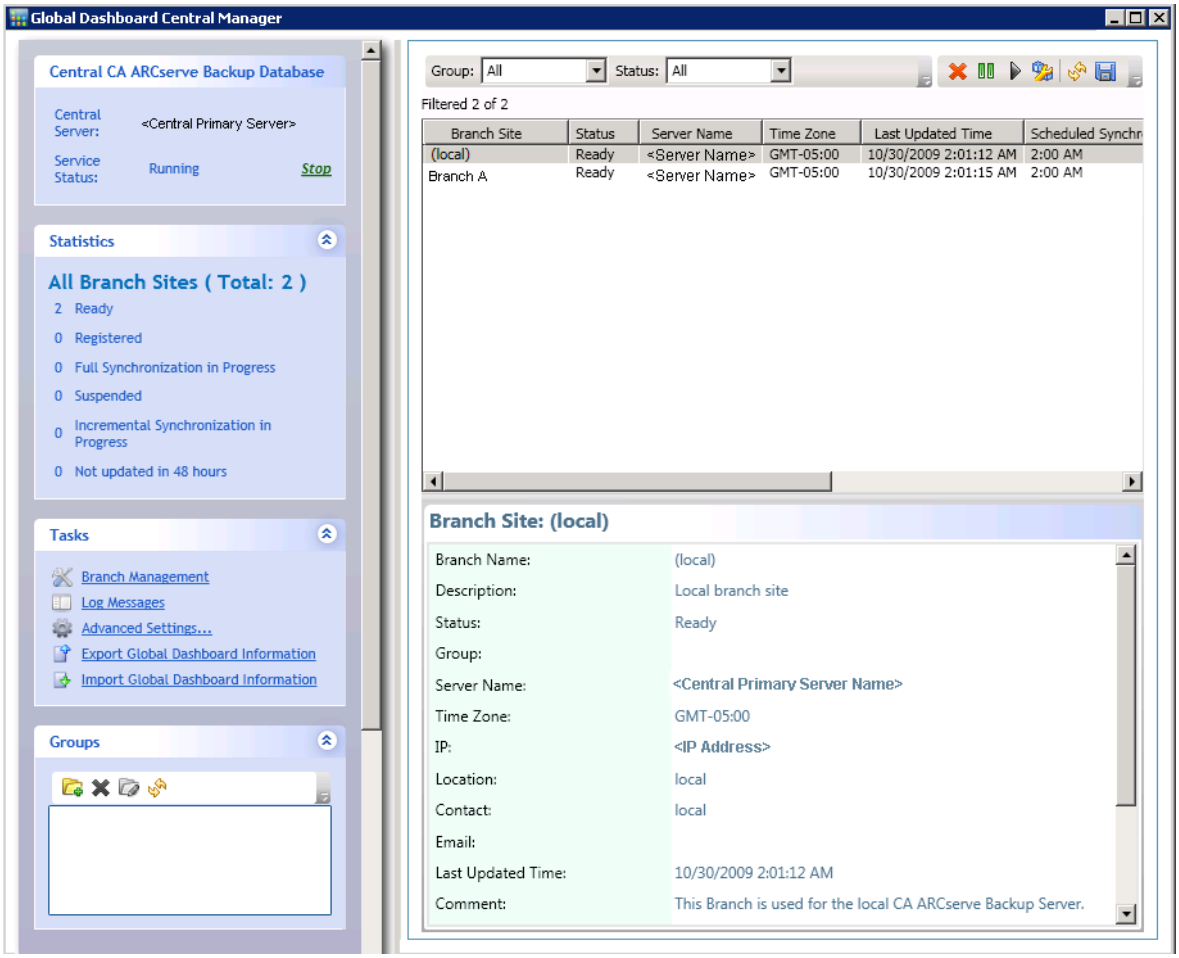
Global Dashboard User Interfaces (see page 65)
Manage Branch Groups (see page 85)
Synchronize Data (see page 89)
Manually Configure a Branch Site (see page 90)
Export/Import Global Dashboard Information (see page 92)

Global Dashboard User Interfaces

Before you use Global Dashboard, you should be familiar with the related user interfaces. These interfaces consist primarily of the Central Manager and Branch Manager interfaces.

Understanding Central Manager

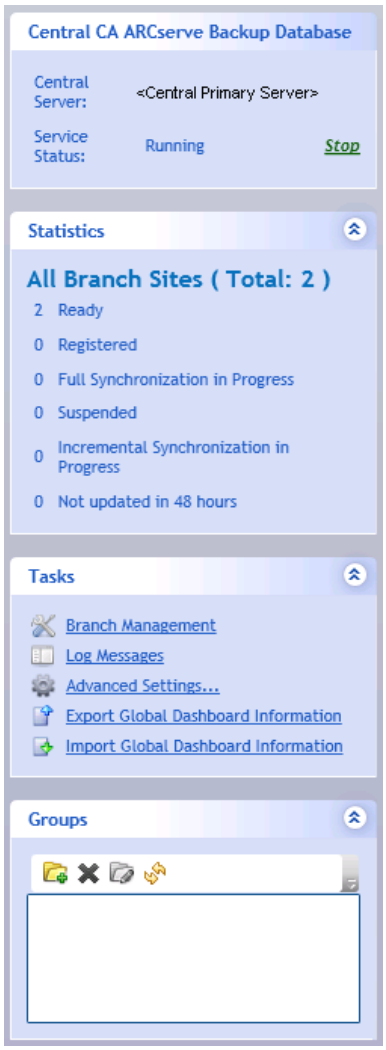
The Central Manager provides a snapshot overview of your entire Global Dashboard environment. This user interface lets you quickly and easily monitor the status of any or all registered branch sites from a single location. The Central Manager also displays any log messages associated with the branch sites. The Central Manager is accessible from the Global Dashboard Console (when the Global View mode is selected) by clicking the icon button on the Global Dashboard toolbar.



From the Central Manager, you can perform the following tasks:

- Stop and start the Global Dashboard Service (Arcserve Backup Central Remoting Server)
- Manage and monitor the status of all registered branch sites
- Manage branch site groups
- Display log messages
- Change the Advanced Settings

The left pane of the Central Manager contains mainly data synchronization status information with sections for Central Arcserve Backup Database, Statistics, Tasks, and Groups.



Central Arcserve Backup Database

The Central Arcserve Backup Database section displays the name of the Central Primary Server that the database is connected to. You can also click on the Start or Stop indicator to toggle the status of the Global Dashboard Service (Arcserve Backup Central Remoting Server). You can stop the service if you need to perform maintenance.

Statistics

The Statistics section displays the overall status of all registered branch sites. The status categories are as follows:

Ready

Branch sites are registered and data synchronization (full or incremental) has been successfully completed.

Registered

Branch sites are registered, but a full data synchronization has not been performed.

Full Synchronization in Progress

Full data synchronization for branch sites is in progress.

Suspended

Branch connection is suspended. The Central Primary Server is unable to receive data from these branch sites.

Incremental Synchronization in Progress

Incremental data synchronization for branch sites is in progress.

Not updated in 48 hours

Data synchronization for branch sites have not been performed in the past 48 hours.

Tasks

The Tasks section contains the following selections:

Branch Management

Displays branch site status information in the right pane of the Central Manager, For more information, see Understanding Branch Management Screen (see page 71).

Log Messages

Displays log message information in the right pane of the Central Manager. For more information, see Understanding Log Messages Screen (see page 78).

Advanced Settings

Displays the Advanced Settings dialog to let you specify certain behavior parameters for the connection of a branch site to the central site. For more information, see Understanding Advanced Settings (see page 80).

Export Global Dashboard Information

Lets you export dashboard information (grouping configuration and registered branch information) from a Central Primary Server to a temporary location. You can then import this saved information into another Central Primary Server. For more information, see Export Global Dashboard Information (see page 93).

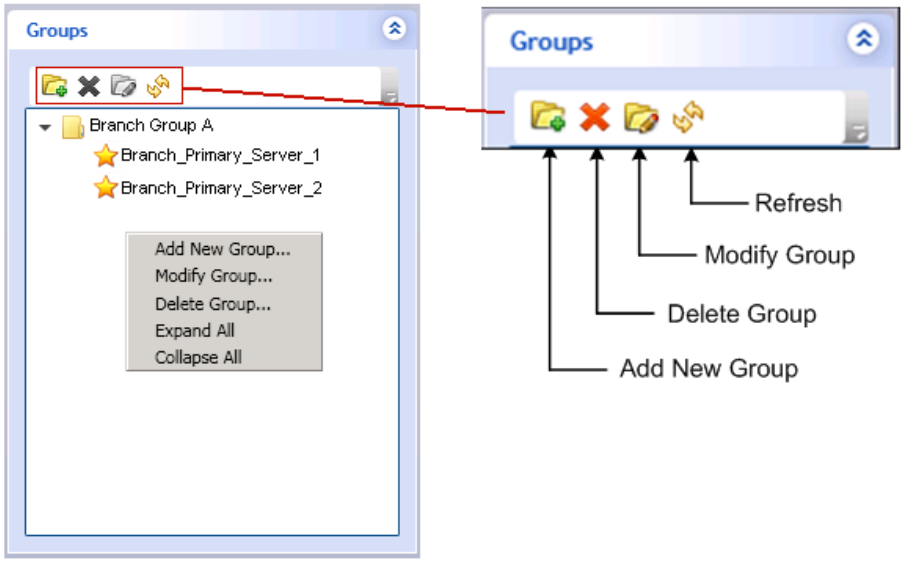
Import Global Dashboard Information

Lets you retrieve dashboard information (grouping configuration and registered branch information) that was previously exported to a temporary location and import it into a Central Primary Server. For more information, see Import Global Dashboard Information (see page 94).

Groups

The Groups section displays the names of the configured Branch Groups. Each listed Branch Group can be expanded to display the names of the Branch Primary Servers that are included in the corresponding group. From this section you can perform the following group-related tasks from either context menu or toolbar button:

Note: For any of these group-related tasks, you must re-launch the Global Dashboard Console to view the changes.



Add a New Group

Specifies to add a new branch site group. A branch site can be part of multiple branch groups. For more information, see Add a New Branch Group (see page 86).

Delete a Group

Specifies to delete an existing branch group. You can use this command to either delete a selected branch site from the branch group, or delete an entire branch group. For more information, see Delete a Branch Group (see page 87).

Modify a Group

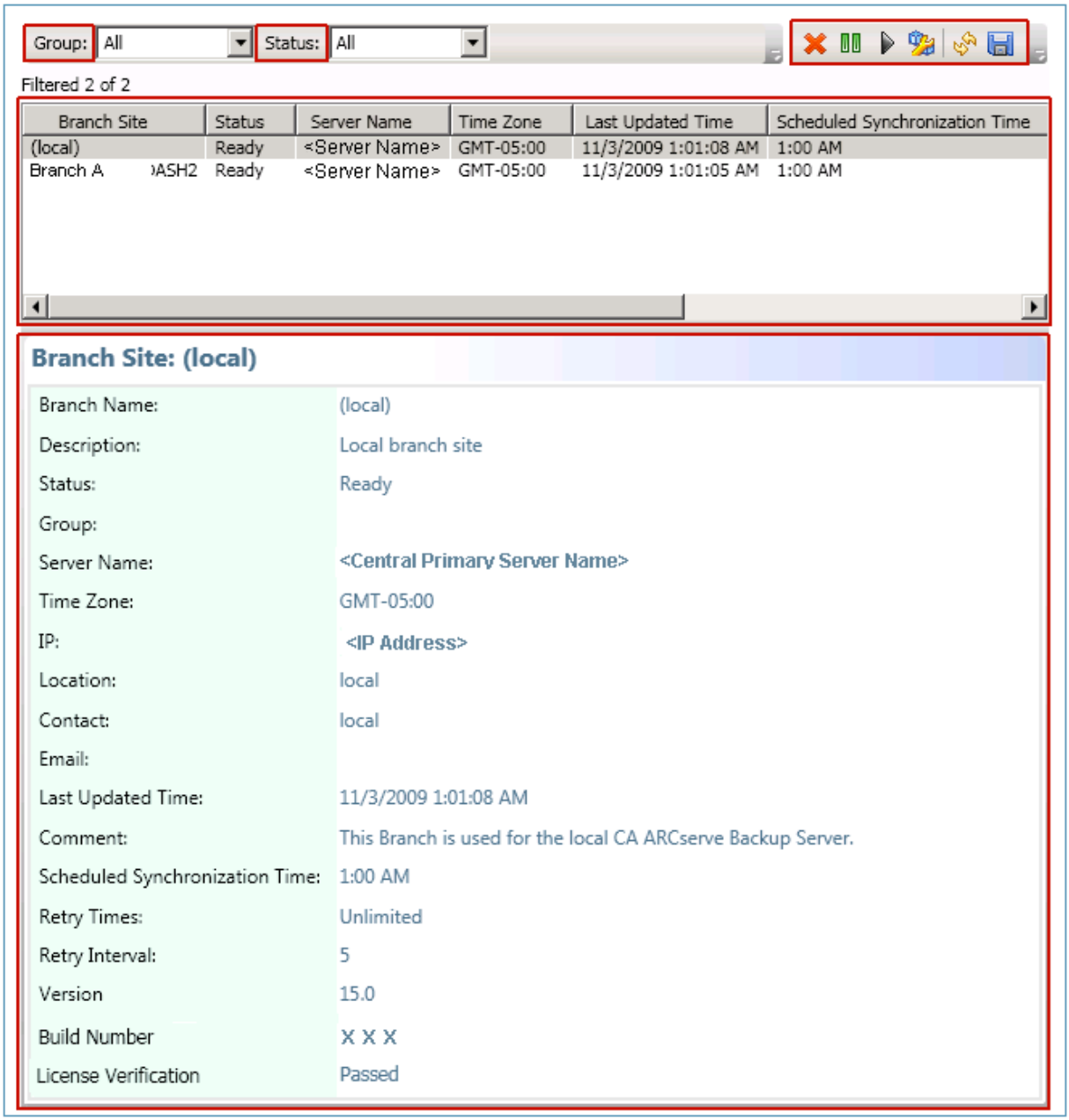
Specifies to modify the branch sites contained within an existing branch group. For more information, see Modify a Branch Group (see page 87).

Refresh

Specifies to refresh the displayed information for the selected branch group.

Understanding Branch Management Screen

The Branch Management screen is accessed from the Tasks section of the Central Manager left pane. The Branch Management screen displays status information for the branch groups and associated branch sites. This screen consists of an upper and lower section.



Branch Management Screen - Upper Section

The upper section of the Branch Management screen can display status information for all registered branch sites or can be filtered for just a specific branch group. This listing can also be filtered to display only information for the following branch site status:

All

Specifies to display all branch sites (not filtered).

Ready

Specifies to display only branch sites that are Ready (registered and data synchronization has been successfully completed).

Registered

Specifies to display only branch sites that are registered, but full data synchronization has not been performed yet.

Full Synchronization in Progress

Specifies to display only branch sites where full data synchronization is in progress.

Suspended

Specifies to display only branch sites where the connection has been suspended. The Central Primary Server is unable to receive data from these branch sites.

Incremental Synchronization in Progress

Specifies to display only branch sites where incremental data synchronization is in progress.

Not updated in 48 hours

Specifies to display only branch sites where data synchronization has not been performed in the past 48 hours.

You can click on any of the Branch Management column headings to sort the displayed information by the selected column.

Branch Site

Indicates the name of the registered branch site.

Note: Local indicates the dashboard-related data is for the local server. If your server is configured as the Central Primary Server, the self-contained data for this server is treated the same as a separate Branch Primary Server and reported to the Global Dashboard as the "local" server.

Status

Indicates the status of the corresponding branch site. If a branch site has not been updated (synchronized with the central site) during the past 48 hours, it will be displayed in red to alert you to this condition and allow you to investigate the reason for this inactivity.

Server Name

Indicates the name of the Branch Primary Server for the corresponding branch site.

Time Zone

Indicates the time zone for the corresponding branch site. This listed time zone is based upon the difference in the number of hours relative to GMT (Greenwich Mean Time). It is important to know this difference in time zones when scheduling synchronization times and when viewing various displayed times. Displayed times will always be based upon the time at the central site

For example:

- Your central site is in New York (GMT-05:00 time zone)
- Your branch site is in Tokyo (GMT+09:00 time zone)
- If your Tokyo branch site is scheduled to be synchronized to the central site at 7:00 AM (New York local time), your branch site synchronization will occur at the Tokyo local time of 9:00 PM (5 + 9 = 14 hour difference).
- The displayed time in all Global Dashboard fields (Last Updated Time, Scheduled Synchronization Time, Error Message Time, and so on) will be 7:00 AM.

Last Updated Time

Indicates the date and time that the last successful data synchronization (full or incremental) was finished. The date and time information is based on the local time for the Central Primary Server (and not necessarily the local time at the branch site).

Scheduled Synchronization Time

Indicates the time that data synchronization is attempted each day. This daily time will always be based on the local time for the Central Primary Server (and not necessarily the local time at the branch site).

Retry Times

Indicates the number of times that the Branch Primary Server will attempt the data synchronization to the Central Primary Server. If for some reason, the data synchronization cannot not be performed at the scheduled time, the Branch Primary Server will wait the specified number of minutes between attempts, and then try again. If this maximum number of retry attempts is reached without successful data synchronization, the Branch Primary Server will discontinue attempts for that day (and retry again as scheduled on the next day) and an error message will be generated.

Retry Interval

Indicates the amount of time (in minutes) that the Branch Primary Server will wait between attempts to perform the data synchronization upload to the Central Primary Server. If for some reason, the data synchronization cannot not be performed at the scheduled time, the Branch Primary Server will wait this specified number of minutes between attempts, and then try again.

Version

Indicates the version of Arcserve Backup installed at the branch site.

Build Number

Indicates the Arcserve Backup build number installed at the branch site.

License Verification

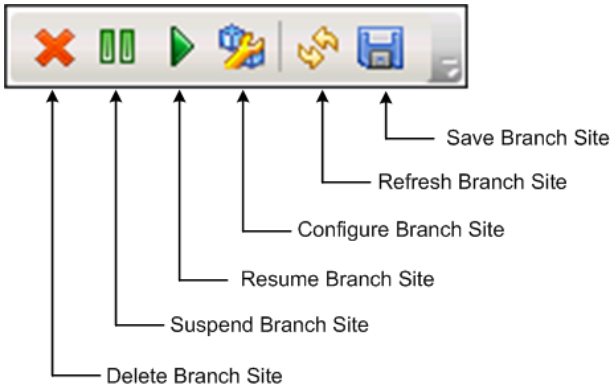
Indicates the status of the license check (Passed or Failed) performed at the central site for each corresponding branch site. If the license status is Failed, the branch site information will be displayed in red text and you will need to obtain additional licenses or re-allocate your existing licenses, to enable data synchronization to the Central Primary Server.

Branch Management Screen - Lower Section

The lower section displays summary information for the selected branch site.

Branch Management Screen - Icon Buttons

The Branch Management screen also includes icon buttons to manage the selected branch site.



Delete Branch Site

Specifies to delete the selected branch site. The branch site will be removed from the Global Dashboard environment and any related data will not be reported. After a branch site is deleted, the only way to add (and re-register) the branch site back to the central site is with the "Re-register" link at the bottom of the Global Dashboard Branch Manager dialog.

For more information, see Understanding Branch Manager (see page 81).

Suspend Branch Site

Specifies to suspend the connection from the selected branch site to the Central Primary Server. You can use this mode if you need to perform maintenance or if there is a problem at the branch site. While suspended, dashboard-related data will not be uploaded from this branch site to the Central Primary Server.

Resume Branch Site

Specifies to resume the suspended connection from the selected branch site to the Central Primary Server. Dashboard-related data will now be uploaded from this branch site to the Central Primary Server at the next scheduled synchronization time.

Configure Branch Site

Specifies to configure the selected branch site. When this button is clicked, the Branch Configuration dialog opens and lets you specify parameters for scheduling data synchronization. For more information, see Understanding Branch Configuration Dialog (see page 76).

Refresh Branch Site

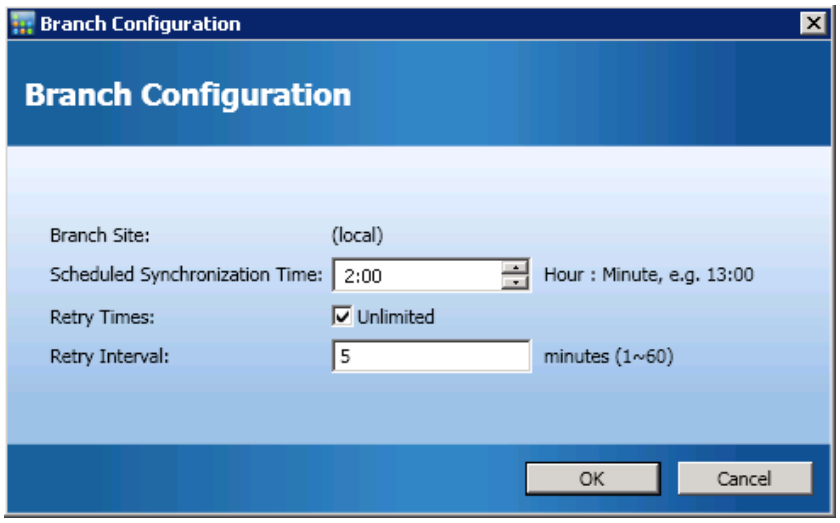
Specifies to refresh the data displayed in the Branch Management screen columns.

Save Branch Site

Specifies to save all data displayed in the Branch Management screen columns. When this button is clicked, the Save As dialog opens and lets you save the displayed data as a Comma-Separated Values (CSV) file to store the tabular data and be used in a spreadsheet.

Understanding Branch Configuration Dialog

The Branch Configuration dialog is accessed from Central Manager (Configure Branch Site icon) and lets you specify behavior parameters for scheduling the data synchronization process. Any modifications to these branch configuration settings will not be applied until the next data synchronization.



Branch Site

This displays the name of the selected Branch Primary Server. All subsequent settings on this dialog will apply to data synchronization process for this branch site only. (If "Local" is displayed, it indicates that the settings will apply to the local Branch Primary Server, even if it is configured to be the Central Primary Server).

Scheduled Synchronization Time

Specifies the time that data synchronization is attempted each day. This daily time will always be based on the local time for the Central Primary Server (and not necessarily the local time at the branch site). The time setting uses a 24-hour clock format and the default setting is 2:00 AM.

If the schedule time for branch synchronization is changed, it will not take effect until after the next synchronization is performed.

For example:

- If at 1:00 AM, you change the scheduled synchronization time from 2:00 AM to 4:00 AM, the branch site will connect to the central site at 2:00 AM *today* and get the new schedule time of 4:00 AM. So the next incremental synchronization will be performed *today* at 4:00 AM.
- If at 3:00 AM, you change the scheduled synchronization time from 2:00 AM to 4:00 AM, the branch site will connect to the central site at 2:00 AM on the *next day* and get the new schedule time of 4:00 AM. So the next incremental synchronization will be performed the *next day* at 4:00 AM.
- If you want to synchronize your branch site data to the new time without waiting until 2:00 AM, you can restart the "Arcserve Dashboard Sync Service" at the respective branch site.

Retry Times

Specifies the number of times that the Branch Primary Server will attempt the data synchronization to the Central Primary Server. If for some reason, the data synchronization cannot not be performed at the scheduled time, the Branch Primary Server will wait the specified number of minutes between attempts, and then try again. If this maximum number of retry attempts is reached without successful data synchronization, the Branch Primary Server will discontinue attempts for that day (and retry again as scheduled on the next day) and an error message will be generated.

By default the Unlimited check box is selected, indicating there is no limit for the number of retry attempts. If this check box is unselected, an additional field is displayed, allowing you to specify a number for the retry attempts. This specified number must be between 0 and 100 and the default setting is 10 retry attempts.

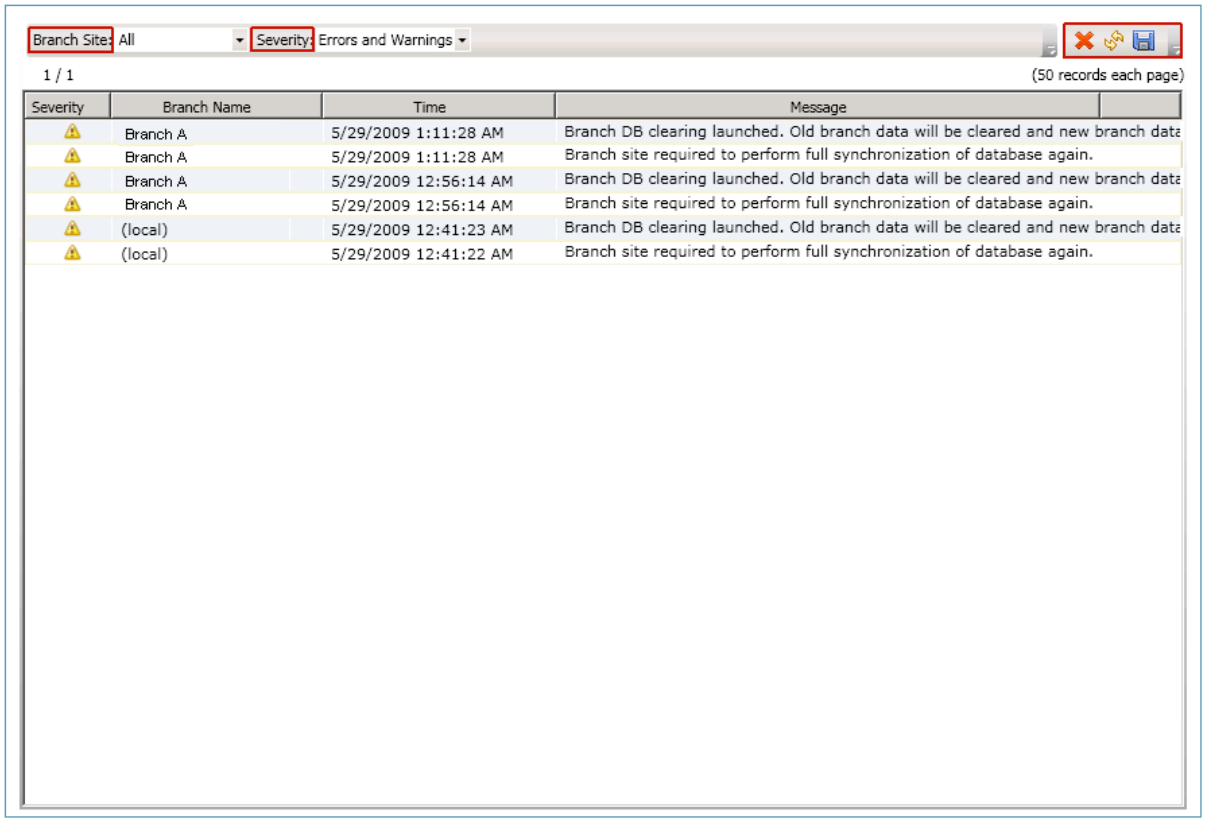
Retry Interval

Specifies the amount of time (in minutes) that the Branch Primary Server will wait between attempts to perform the data synchronization upload to the Central Primary Server. If for some reason, the data synchronization cannot not be performed at the scheduled time, the Branch Primary Server will wait this specified number of minutes between attempts, and then try again.

This number must be between 1 and 60 and the default setting is 5 minutes between retry attempts.

Understanding Log Messages Pane

The Log Messages screen is accessed from the Tasks section of the Central Manager left pane. The Log Messages screen displays log message information for the registered branch sites.



This listing can display log messages for all registered branch sites or can be filtered for just a specific branch site. This listing can also be filtered to display only messages for a specific severity level (All, Messages, Warnings, Errors, and Errors and Warnings).

You can click on any of the Log Messages column headings to sort the displayed information by the selected column.

Severity

Indicates the severity level of the displayed log message. The available levels are Error, Warning, or Message. The default setting is Errors and Warnings.

Branch Name

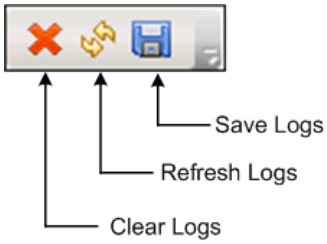
Indicates the name of the Branch Primary Server that recorded the log message.

Note: Local indicates the dashboard-related data is for the local server. If your server is configured as the Central Primary Server, the self-contained data for this server is treated the same as a separate Branch Primary Server and reported to the Global Dashboard as the "local" server.

Time

Indicates the date and time that the log message was recorded. The date and time information is based on the local time for the Central Primary Server (and not necessarily the local time at the branch site).

The Log Messages screen also includes icons to clear all log entries, refresh the log display, and save the logs.



Understanding Advanced Settings

The Advanced Settings dialog is accessed from the left pane of the Central Manager (Tasks area) and lets you specify certain behavior parameters for the connection of a branch site to the central site.

Maximum Concurrent Connections

Specifies the maximum number of concurrent connections for data synchronization that can be performed simultaneously from branch sites to the central site. Generally as the number of concurrent connections is increased, it will have a greater affect on your system resources. Therefore, for larger and more powerful systems, this number can be increased to minimize the total time for data synchronization. For smaller and less powerful systems, this number can be reduced to improve system performance, but the total time for data synchronization will be increased.

The number must be between 1 and 40. The default value is a maximum of 40 concurrent connections.

For example, if you specify that the maximum concurrent connections is 5 and you have 8 branch sites scheduled to perform data synchronization at the same time, only the first 5 branch sites will begin the synchronization process at the scheduled time. The remaining 3 branch sites will wait a specified number of minutes between retry attempts and then if there are less than the maximum 5 synchronizations being performed, additional branch sites will be allowed to connect to the central site and begin their data synchronization.

Central Primary Server Port

Specifies the input port number that a registered Branch Primary Server will use when connecting to the Central Primary Server to transfer dashboard-related data. Because this port number can only be controlled from the central site, any changes from the default number must also be changed at each branch site to enable connection.

This number must be between 1024 and 65535. The default port number is 18001.

DB Connection Timeout

Specifies the amount of time (in minutes) that the Arcserve Backup Central Remoting Server service (on the Central Primary Server) will wait for a response from the central database to upload the dashboard-related data from a branch database to the central database. Generally as the number of timeout minutes is increased, it will decrease the possibility of a timeout error occurring. You may need to increase the value of DB connection timeout if the central database response time is slow (especially when the central database is on a remote server). Therefore, for smaller and less powerful systems (or very busy systems), this number can be increased to reduce the possibility of a timeout error occurring.

This number must be between 1 and 60 minutes. The default database connection timeout is 5 minutes.

Understanding Branch Manager

The Global Dashboard Branch Manager dialog is accessed from the Start menu (Programs\CA\ARCserve Backup\Branch Manager) and provides each local branch site with a means to perform the following tasks:

- Modify your branch site configuration information
- Modify your branch site connection information which is used for connecting to the central site
- Modify the authentication information which is used to connect to the Arcserve Backup central database
- Manually launch the data synchronization process
- Manually control the running of the Branch Synchronization Service
- Display the most recent log messages

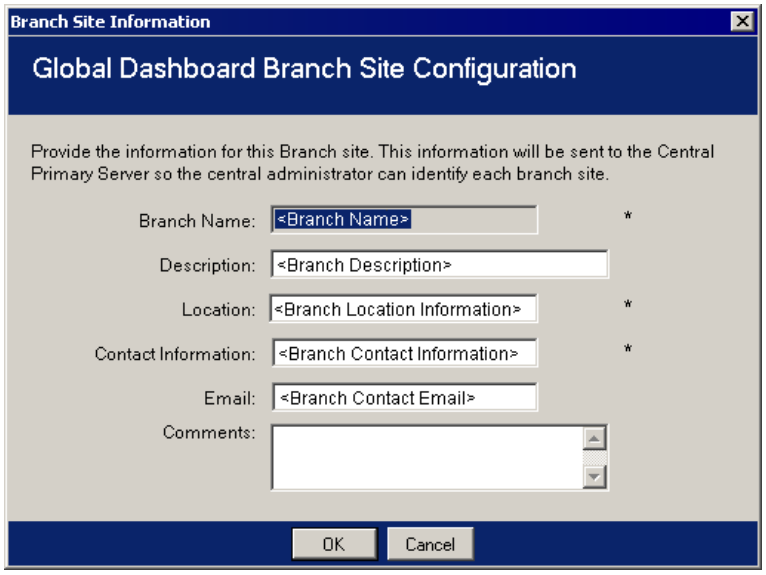
Note: The "Re-register" link at the bottom of this dialog lets you register the branch site to the same central site in case your branch registration was inadvertently deleted.

Branch Primary Server Information

When you click the Modify button, the Branch Site Information dialog opens. This dialog displays information about your local branch site.

From this dialog you can change the branch name, description, location, and contact information (including email address) for your branch site, and add any useful comments.

After you have updated your branch site information and click OK, the modified information will immediately be sent to the central site and displayed on the Central Manager.



Central Primary Server Information

When you click the Modify button, the Central Site Information dialog opens. This dialog displays connection information to the central site. For a branch site to properly communicate to the central site, these parameters must be the same as specified for the central site configuration.

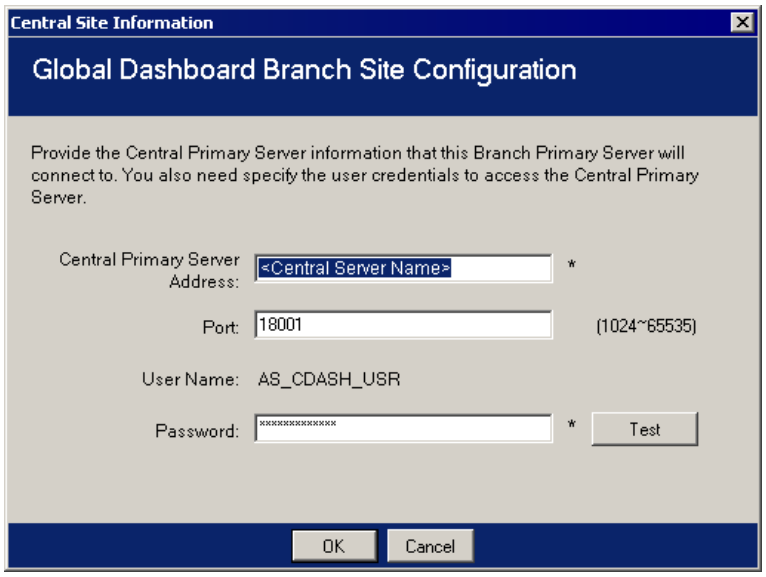
If any of these connection parameters do not match the central site configuration parameters, you can use this dialog to change the name (or IP address) of the Central Primary Server, the Port number to access the Central Primary Server, or the authentication Password for the user. You can click the Test button to verify the connection status to the central site.

After you have updated your central site connection information and click OK, the modified information will be used by the Branch Synchronization Service to upload your branch site data to the central site at the next scheduled synchronization time.

You can use this dialog to modify the Central Site Information on your branch site for the following reasons:

- You previously configured the Central Primary Server through an IP address and now the IP address has changed.
- You changed the port number of the Arcserve Backup Central Remoting Server service on the Central Primary Server.
- You changed the password of Windows account AS_CDASH_USR (this could be due to the password policy requirements on the Central Primary Server).

Note: If you change the Central Primary Server, you must then register to the new Central Primary Server from all Branch Primary Servers.



Data Synchronization

When you click the Synchronize button, you will manually initiate a full data synchronization for your local branch site.

Important! Full data synchronization will completely overwrite all previously uploaded data from your branch site. As a result, you should only perform a manual full data synchronization when it is either the first time your branch site is synchronizing data to the central site or when you suspect that the branch site data that was previously uploaded to the central site may be out-of-date or corrupted.

During a full data synchronization process, the Arcserve Backup database engine will be shut down for a few minutes and may prevent the logging of any Arcserve Backup job information into the database until the process is complete. Verify that this is a convenient and non-intrusive time before continuing.

Data Synchronization Service

When you click the Stop button, you will toggle the status of the Data Synchronization Service ("Arcserve Dashboard Sync Service") from Running to Stopped (and the button title will also toggle to Start). When you click the Start button, you will toggle the status of the Data Synchronization Service from Stopped to Running (and the button title will also toggle to Stop).

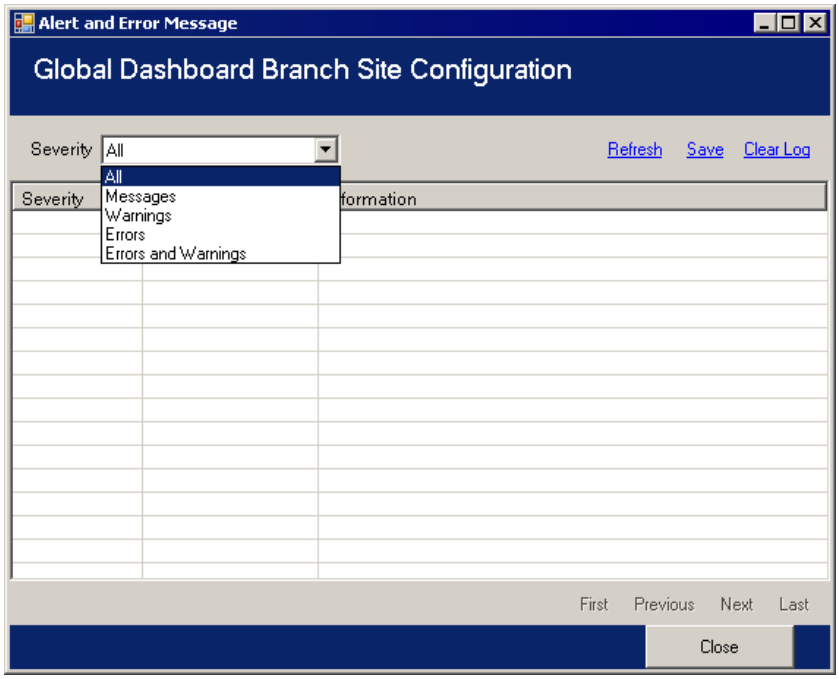
The Data Synchronization Service is responsible for uploading any branch site data which has been modified, deleted, or added since the last synchronization was performed.

With this service running, the branch site data will be synchronized to the central site when requested (either as scheduled or manually initiated). With this service stopped, the communication from the branch site to the central site will be stopped and data synchronization will not occur.

Most Recent Error Messages

Lists the most recent error messages reported from the branch site. These Branch Manager messages are different from the log messages listed on the Central Manager. These errors are detected by the branch site (errors encountered during data transmitting), while the Central Manager errors are detected at the central site (errors encountered during data receiving).

The Refresh link updates the most recent error messages displayed. The Show More link opens the Alert and Error Message window to display an expanded view of all branch-related messages. These displayed messages can be filtered based upon the Severity level (Errors, Warnings, Messages, and so on). In addition, from this window you can also Refresh the display, Save the log entries as a CSV file, and Clear all log entries.



Manage Branch Groups

A Global Dashboard Branch Group is a customized collection of branch sites that when selected displays consolidated report information from a pre-configured grouping of Branch Primary Servers. Branch Groups let you organize the display of report information based upon your specific needs or preferences. Branch Groups can be logically organized by such categories as geographical locations, group functions, departments within your company, and so on. Branch Groups help you focus on the status within specific areas of your dashboard environment. A branch site can be part of multiple Branch Groups.

From the left pane of the Central Manager, you can access the Groups section to perform various branch group-related tasks. Each listed Branch Group can be expanded to display the names of the Branch Primary Servers that are included in the corresponding group. From this section you can perform group-related tasks from either a context menu or a toolbar button.

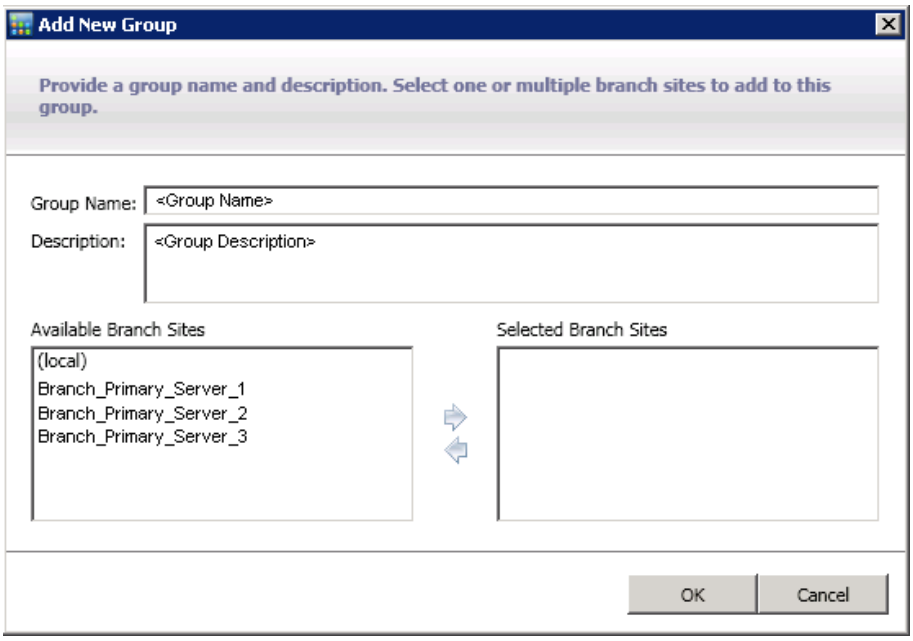
Add a New Branch Group

Global Dashboard lets you add new branch groups that display your customized grouping of branch sites when selected.

Add a New Branch Group

1. From the Central Manager Groups pane, click the Add New Group button.

   The Add New Group dialog opens, displaying a listing of all available registered branch sites.



2. Enter a Group Name and description for the new branch group being created.

   The group name is not case sensitive.

   Note: You cannot have two branch groups with the same name.

3. From the Available Branch Sites box, select the branch site(s) to be included in the new branch group and click the right arrow icon.

   The branch sites are added to the Selected Branch Sites box.

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

4. Click OK to save the changes.

   The name of the new branch group appears on the Central Manager Groups list and can be selected.

   Note: For this group-related task, you must re-launch the Global Dashboard Console to view the changes.

Delete a Branch Group

Global Dashboard lets you delete an entire branch group or remove a selected branch site from within a Branch Group.

Delete a Branch Group

1. From the Central Manager Groups pane, select an existing branch group that you want to delete (or expand a branch group listing and select a specific branch site).

   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 branch group (or delete the selected branch site from the branch group).

3. Click Yes to confirm the delete request (or No to stop the process).

   The selected branch group (or branch site) will no longer be displayed in the Groups pane.

   Note: For this group-related task, you must re-launch the Global Dashboard Console to view the changes.

Modify a Branch Group

Global Dashboard lets you modify an existing branch group when selected.

Modify a Branch Group

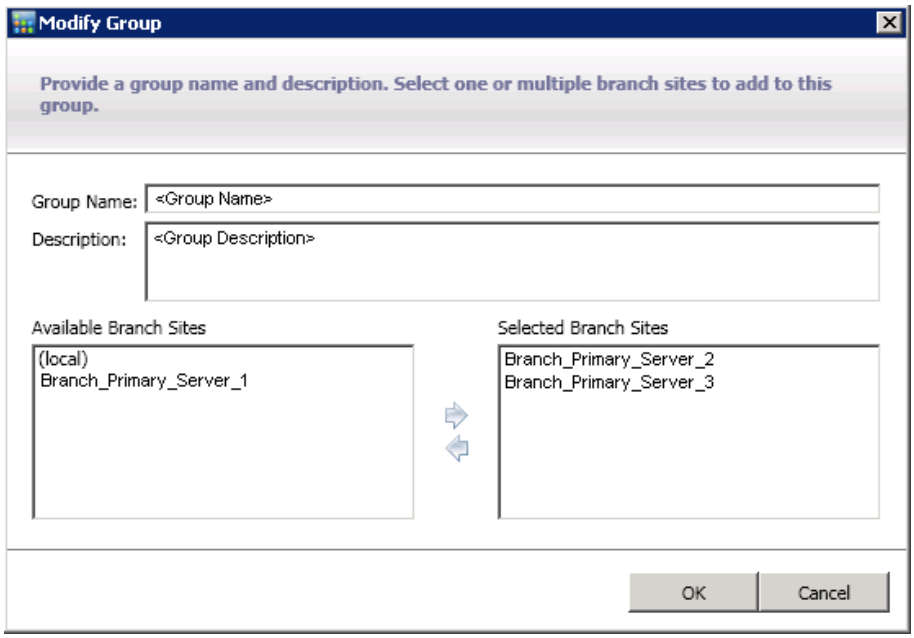
1. From the Central Manager Groups pane, select an existing branch group that you want to modify.

   The Modify Groups button becomes enabled.

2. Click the Modify Group button.

   The Modify Group dialog opens, displaying a listing of all branch sites that are included in the selected branch group and all available registered branch sites.

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



   a. To add a branch site to the branch group, from the Available Branch Sites box select the branch site and click the right arrow icon button.

      The branch site is removed from the Available Branch Sites box and added to the Selected Branch Sites box.

   b. To remove a branch site from the branch group, from the Selected Branch Sites box select the branch site and click the left arrow icon button.

      The branch site is removed from the Selected Branch Sites box and added to the Available Branch Sites box.

3. Click OK to save the changes.

   The modified branch group appears on the Central Manager Groups list and can be selected.

Synchronize Data

Data synchronization is the process of transmitting dashboard-related information from a branch site database to the central site database. Synchronizing data will keep the data in the different databases consistent and up-to-date so that the central site database contains (and reports) the same information as each of the registered branch site databases. During a full synchronization process, the Arcserve Backup database engine will be shut down for a few minutes. During incremental data synchronization, no Arcserve Backup services will be shut down.

Data synchronization can be performed automatically based upon a specified schedule or manually at any time.

Modify Automatic Data Synchronization

Automatic data synchronization will be attempted every day at a specified scheduled time. This daily time will always be based on the local time for the Central Primary Server (and not necessarily the local time at the branch site).

The behavior parameters for scheduling the data synchronization of each branch site are specified on the Branch Configuration dialog. From this dialog you can view and modify the automatic data synchronization parameters.

Modify the Automatic Data Synchronization Parameters

1. From the left pane of the Central Manager, click on the Branch Management task option.

   The Branch Management screen is displayed in the right pane.

2. From the Branch Management screen, select the branch site that you want to view or modify the data synchronization parameters.

   The Configure Branch Site icon button is enabled.

3. Click the Configure Branch Site icon button.

   The Branch Configuration dialog opens, displaying the name of the selected branch site.

4. Modify the data synchronization parameters (scheduled daily synchronization time, maximum number of retry attempts, and time interval between retry attempts) as necessary and click OK. For more information about these parameters, see Understanding Branch Configuration Dialog (see page 76).

   The new data synchronization parameters are saved and the Branch Configuration dialog is closed.

Manually Synchronize Data

If you do not want to wait until the next scheduled data synchronization attempt, you can manually initiate the data synchronization process for your branch site. When you manually perform a data synchronization, it will always be a full data synchronization.

Important! Full data synchronization will completely overwrite all previously uploaded data from your branch site. As a result, you should only perform a manual full data synchronization when it is either the first time your branch site is synchronizing data to the central site or when you suspect that the branch site data that was previously uploaded to the central site may be out-of-date or corrupted.

During a full data synchronization process, the Arcserve Backup database engine will be shut down for a few minutes and may prevent the logging of any Arcserve Backup job information into the database until the process is complete. Verify that this is a convenient and non-intrusive time before continuing.

Manually Synchronize Data

1. From the Start menu, select Programs/CA/ARCserve Backup/Branch Manager.

   The Branch Manager dialog opens.

2. Click the Synchronize button.

   A full data synchronization will begin. Data from your branch site will be uploaded to the central site.

   When the data synchronization process is completed, the Branch Manager dialog will be updated to display the new date and time for the last full data synchronization. For more information, see Understanding Branch Manager (see page 81).

Manually Configure a Branch Site

If you need to modify your branch site configuration information, you can manually change your local branch site settings or the connection settings from your branch site to the central site.

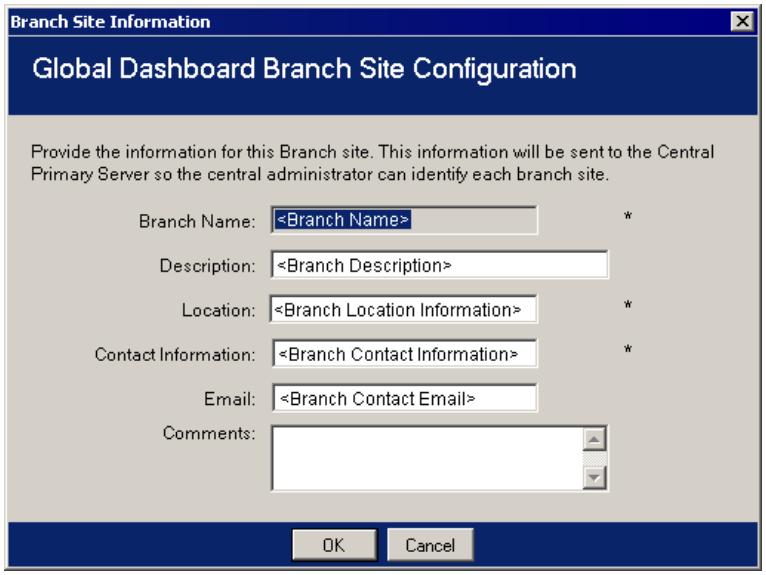
Manually Configure a Branch Site

1. From the Start menu, select Programs/CA/ARCserve Backup/Branch Manager.

   The Branch Manager dialog opens. For more information, see Understanding Branch Manager (see page 81).

2. To change your local branch site information, click the Modify button for the branch site.

   The Branch Site Information dialog opens.



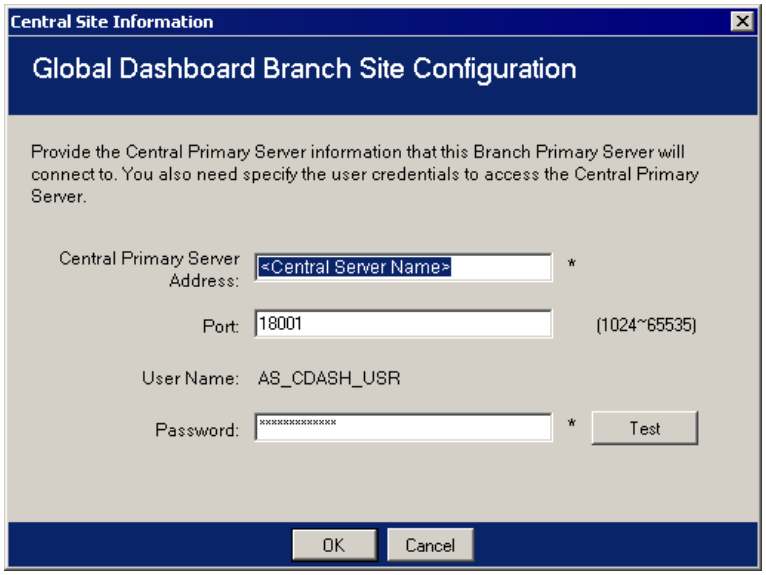
   This dialog displays information about your local branch site. From this dialog you can change the description, location, and contact information (including email address) for your branch site, and add any useful comments.

3. After you have updated your branch site information, click OK to save your settings.

   The modified information will immediately be sent to the central site and displayed on the Central Manager.

4. To change your connection information to the central site, click the Modify button for the Connection to Central Primary Server.

   The Central Site Information dialog opens.



   This dialog displays connection information to the central site. For a branch site to properly communicate to the central site, these parameters must be the same as specified for the central site configuration.

   If any of these connection parameters do not match the central site configuration parameters, you can use this dialog to change the name (or IP address) of the Central Primary Server, the Port number to access the Central Primary Server, or the authentication Password for the user.

   You can click the Test button to verify the connection status to the central site.

5. After you have updated your central site connection information, click OK.

   The modified information will immediately be used by the Branch Synchronization Service to upload your branch site data to the central site.

Export/Import Global Dashboard Information

In a Global Dashboard domain, the Central Primary Server contains the grouping configuration information for the registered Branch Primary Servers. In Arcserve Backup, you can promote a member server to a primary server or demote a primary server to a member server. If during this promotion/demotion process you also are changing which primary server will be configured as the Global Dashboard Central Primary Server, you may want to continue to use the collected information from the old Central Primary Server. Global Dashboard lets you export (and save) this information from the old Central Primary Server and import it into the new Central Primary Server.

For each of the following scenarios you should consider exporting the Global Dashboard information prior to performing the task

- Demoting the Central Primary Server to a member server
- Promoting a member server to the Central Primary Server
- Changing the Central Primary Server database to Microsoft SQL Server Express or Microsoft SQL Server 2000. (Global Dashboard does not support Microsoft SQL Express or Microsoft SQL 2000, and as a result this server will no longer function as the Global Dashboard Central Primary Server).

  Notes:

  - If the server is a Central Primary Server in a Global Dashboard domain and the new selected database is Microsoft SQL Server Express or Microsoft SQL Server 2000 (which are not supported by a Central Primary Server), you may want to export and retain the Global Dashboard information prior changing the database. After the change database operation is completed, the Global Dashboard information will be lost because the server will no longer be a supported Central Primary Server. If you want to retain the grouping configuration and the registered branch information, you need to export this Global Dashboard information to a temporary location before performing the change database operation.
  - If you change the Central Primary Server database from one SQL Server to another SQL Server, you do not need to export the Global Dashboard information.
  - If you overwrite the Arcserve Backup database (ASDB) for the Central Primary Server, you need to manually perform a "Re-register" operation from all associated Branch Primary Servers because the branch configuration information will also be overwritten. The "Re-register" operation will perform the full synchronization automatically.

Export Global Dashboard Information

When you are changing the Global Dashboard Central Primary Server (demoting or promoting), you may want to retain and reuse the grouping configuration and the registered branch information. To do this, you must first export (and save) this dashboard information to a temporary location until a new Global Dashboard Central Primary Server is configured and then import the saved information into this new Central Primary Server.

When you complete the export process, two new files are created

- GlobalDashboardInfo.xml
- BranchContactInfo.txt

You need to specify where these new files will be saved so that they can be retrieved and imported when the new Central Primary Server is configured.

Export Global Dashboard Information

1. From the left pane of the Central Manager, click on the Export Global Dashboard Information task option.

   A Browse for Folder dialog opens.

2. From the Browse for Folder dialog, specify or browse to the destination folder where you want the Global Dashboard information to be exported to. If necessary, you can create a new folder to store this information.

   Important! It is important to remember (and record) the location of this destination folder so that it can be easily located and selected during the import process.

3. Click OK to launch the export process.

   The "GlobalDashboardInfo.xml" and "BranchContactInfo.txt" files are generated and exported to the specified destination folder. If the exported files already exist in the folder, an alert message is displayed asking you if you want to overwrite the existing files.

   The Exporting Global Dashboard Information screen opens, indicating the status of the export process.

4. When the export process is complete, an information message screen is displayed. Click OK.

   Verify that the newly created "GlobalDashboardInfo.xml" and "BranchContactInfo.txt" files are located in the specified destination folder.

Import Global Dashboard Information

When you are promoting a primary server to the Global Dashboard Central Primary Server, you may want to reuse the grouping configuration and the registered branch information that existed in the previous Central Primary Server. To do this, you must retrieve the dashboard information files that was previously exported to a temporary location and import them into the new Global Dashboard Central Primary Server.

Import Global Dashboard Information

1. From the left pane of the Central Manager, click on the Import Global Dashboard Information task option.

   A Browse for Folder dialog opens.

2. From the Browse for Folder dialog, locate the folder that contains the "GlobalDashboardInfo.xml" and "BranchContactInfo.txt" files that were previously exported.

   Note: You only need to select the folder where the files are contained, and not the individual files themselves.

3. Click OK to launch the import process.

   The "GlobalDashboardInfo.xml" and "BranchContactInfo.txt" files are imported into the new Central Primary Server.

   - If the selected folder does not contain the exported files, an alert message is displayed asking you to select a different folder.
   - If the Central Primary Server already contains branch contact information for a branch that is also included in the import files, an alert message is displayed, asking you if you want to overwrite this branch contact information.

   The Importing Global Dashboard Information screen opens, indicating the status of the import process.

4. When the import process is complete, an information message screen is displayed. Click OK.

5. Contact the administrators for each of the registered Branch Primary Servers (included in the imported "BranchContactInfo.txt" file) to inform them about the change to the new Central Primary Server and request that they each perform a full data synchronization from their branch site to the new Central Primary Server.

Chapter 6: Dashboard Reports

This section contains the following topics:

Arcserve Backup Dashboard Report Types (see page 98)
Agent Distribution Report (see page 100)
Application Data Trend Report (see page 104)
Backup Data Location Report (see page 106)
Backup Server Load Distribution Report (see page 109)
Client Node Software Report (see page 113)
CPU Report (see page 116)
Data Distribution on Media Report (see page 120)
Deduplication Benefits Estimate Report (see page 122)
Deduplication Status Report (see page 124)
Disk Report (see page 128)
Job Archive Status Report (see page 131)
Job Backup Status Report (see page 135)
License Report (see page 141)
Media Assurance Report (see page 143)
Memory Report (see page 145)
Network Report (see page 149)
Node Archive Status Report (see page 151)
Node Backup Status Report (see page 155)
Node Disaster Recovery Status Report (see page 160)
Node Encryption Status Report (see page 164)
Node Recovery Points Report (see page 168)
Node Summary Report (see page 172)
Node Tiers Report (see page 175)
Node Whose Most Recent Backup Failed Report (see page 178)
OS Report (see page 181)
Recovery Point Objective Report (see page 183)
SCSI/Fiber Card Report (see page 186)
SRM PKI Utilization Reports (see page 189)
Tape Encryption Status Report (see page 196)
Top Nodes with Failed Backups Report (see page 200)
Top Nodes with Fastest/Slowest Backup Throughputs Report (see page 204)
Top Nodes with Most Unchanged Files Report (see page 206)
Total Archive Size Report (see page 207)
Total Protection Size Report (see page 209)
Virtual Machine Recovery Points Report (see page 211)
Virtualization Most Recent Backup Status Report (see page 215)
Volume Report (see page 218)
Volume Trend Report (see page 222)

Arcserve Backup Dashboard Report Types

The Arcserve Backup Dashboard reports are categorized into three types of reports; Backup Reports, Archive 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.

Note: For all Dashboard reports, when you access a report using the Global View option, an additional filter is available to let you limit the data displayed by specifying the Branch name (or selecting the Branch name from the drop-down menu). In addition, all table format reports will be expanded to include an additional column to list the Branch Name.

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 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 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.

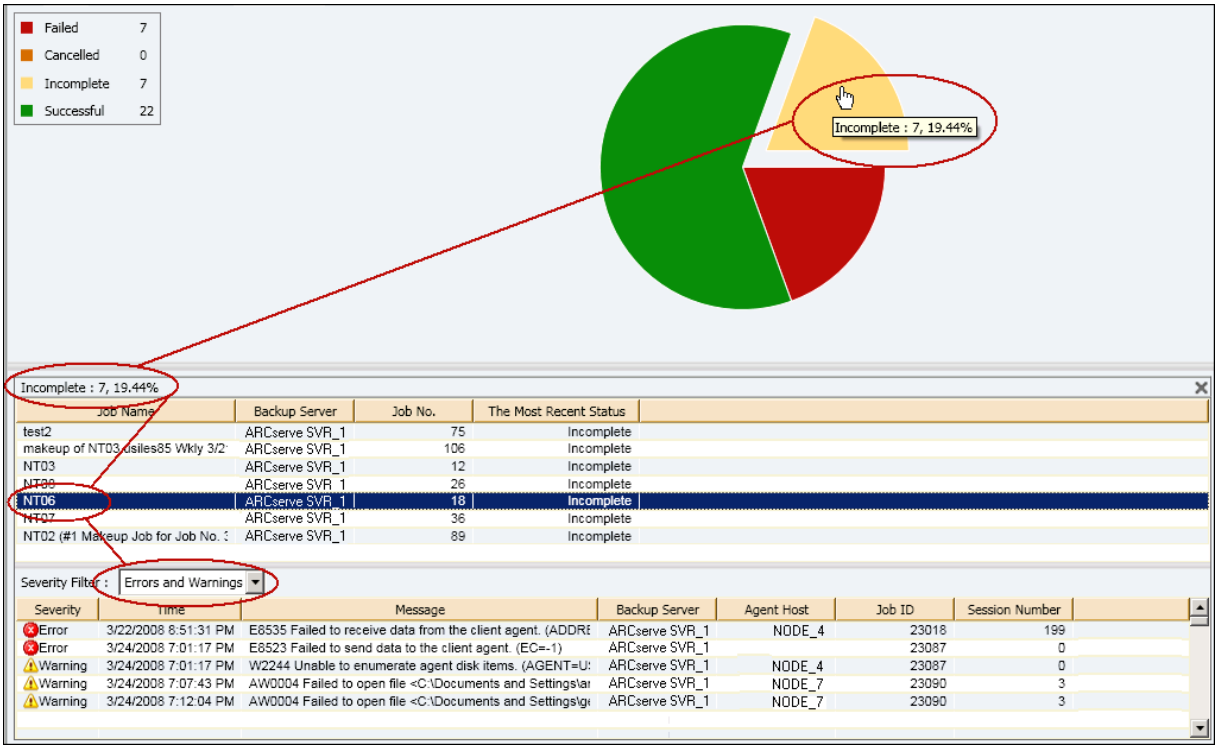
It is important to evaluate these SRM reports in tandem with each other to compare results and get a better overall picture of what is occurring in your storage environment.

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 process occurs at 2 PM every day. However, if you want to immediately collect and 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 Prober Settings (see page 33).

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 Arcserve Backup agents that are installed on each node. Dashboard only supports Arcserve Backup r12.5 and later and its related agents. To fully utilize Dashboard and take advantage of its features, all agents must also be at the r12.5 or later version. If an agent is not at the r12.5 or later 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 Arcserve Backup.

This report can be used to quickly determine the version status of your 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 Arcserve Backup agents are installed on each node. Dashboard only supports Arcserve Backup r12.5 and later and its associated agents.

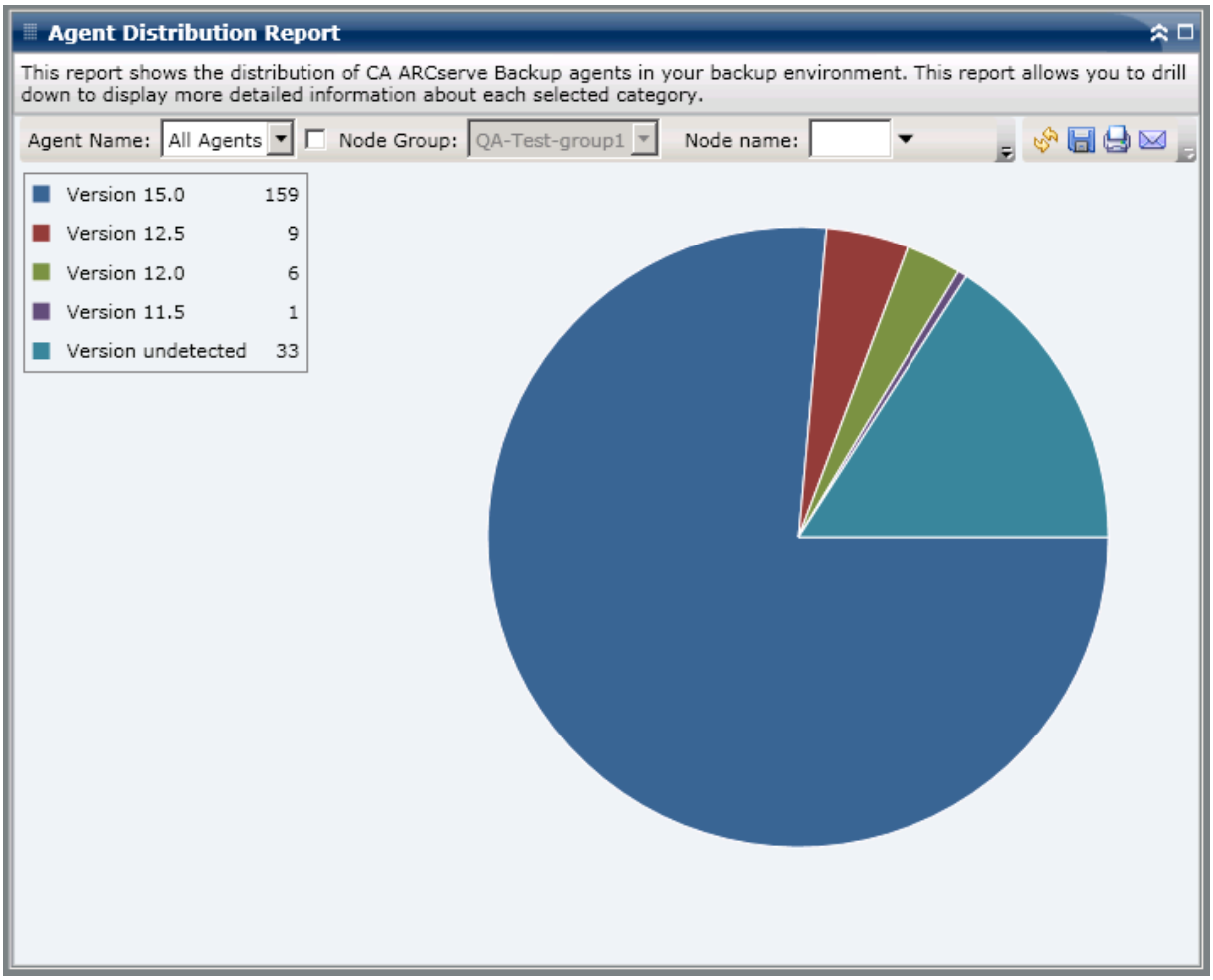
If you find that not all your backup data is being displayed on the various Dashboard reports, you can use this report to determine if some or all of your Arcserve Backup agents have not been updated to the r12.5 or later version. To take full advantage of the latest features offered by the Arcserve 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 Arcserve Backup agents:

- Contact Technical Support for online technical assistance and a complete list of locations, primary service hours, and telephone numbers.
- Use the Agent Deployment tool, which is available from the Administration section of the Navigation bar of Arcserve Backup.

Report View

The Agent Distribution Report is displayed in a pie chart format, showing the version distribution of the selected agent name. This report contains filters for Agent Name, Node Group, Node Name, and Node Tier.

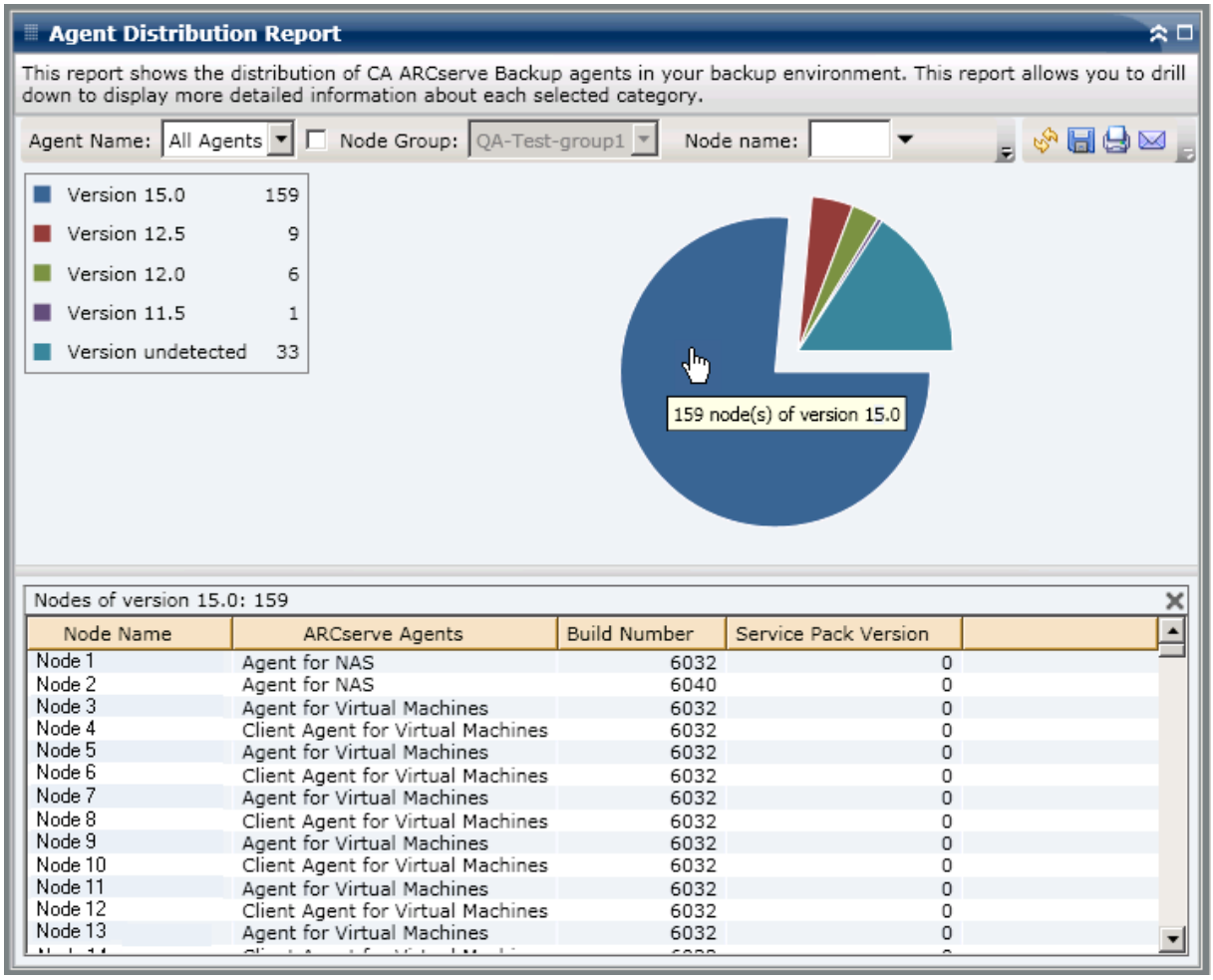


Drill Down Reports

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: In the list of Arcserve Agents, the Agent for SAP will be counted as an Agent for Oracle.

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 62).



The Agent Distribution Report will only display the Service Pack (SP) version of nodes that have 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 Arcserve support at https://www.arcserve.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 General Availability (or initial) release of this version.						

Application Data Trend Report

The Application Data Trend Report is an SRM-type report that displays the data size in use for each type of application in a historical view and then projects the growth trend for these applications so that you can anticipate and prepare for future disk space requirements. This report displays the information for nodes which run a supported Windows operating system and allows you to drill down to display more detailed information for a single node.

Report Benefits

The Application Data Trend Report is helpful in analyzing the current (and historical) size of data in use for Arcserve Backup protected applications. In addition, this report is also helpful in determining the future application size needs based upon anticipated growth trends. With this information, you can then predict disk space requirements for a future time period and take actions accordingly to ensure you are properly protected. The Application Data Trend Report lets you select a specific application to analyze or select several applications to analyze the overall data size for these applications.

Report View

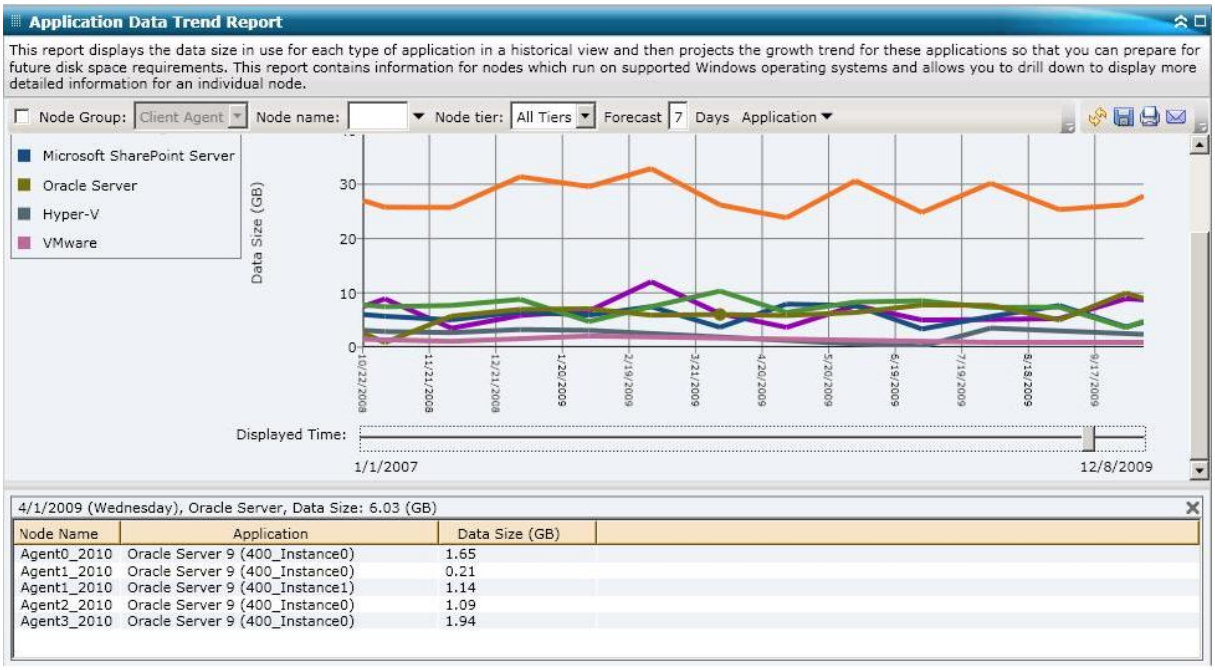
The Application Data Trend Report is displayed in graph format showing the amount of data in use (in GB) for each particular application, along with the anticipated trends during a future time period. The report lets you specify the view mode (Week, Month, Year, All, and Customized Time Range) for the displayed time period. You can use the scroll bar at the bottom of the chart to adjust the time period being displayed or click on any sample point along the data line to display more details about that specific sample point. You can also filter the data by individual applications and the forecasted time range.

This report lets you easily see the projected trends in storage capacity for the applications to help you plan for your future data storage needs. The data from each application is displayed as a separate line with a separate color and the projected data for that application is displayed in a lighter color. A summary line chart is also available to display the overall data size (and trend) for all selected applications. Only data from installed applications (protected by Arcserve Backup) will be displayed.

Note: To ensure that you are reporting the correct database size of an Oracle database, the Oracle instance should in the archive mode.

The Application Data Trend Report can be further expanded to display more detailed information. You can click on a sample point on the line chart to show the details of that time period. This drill-down report includes the node names, along with the associated application types and data size (in GB) for each listed application.

This report contains filters for Node Group, Node Name, Node Tier, Forecast, and Application.



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 five possible recovery location categories (Replicated, Disk, Cloud, 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 Arcserve Replication and High Availability and backed up by Arcserve Backup as Arcserve Replication and High Availability scenarios.

Disk

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

Cloud

Nodes that were backed up to cloud by creating cloud connections and cloud-based devices, see *Administration Guide* for more details on cloud 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.

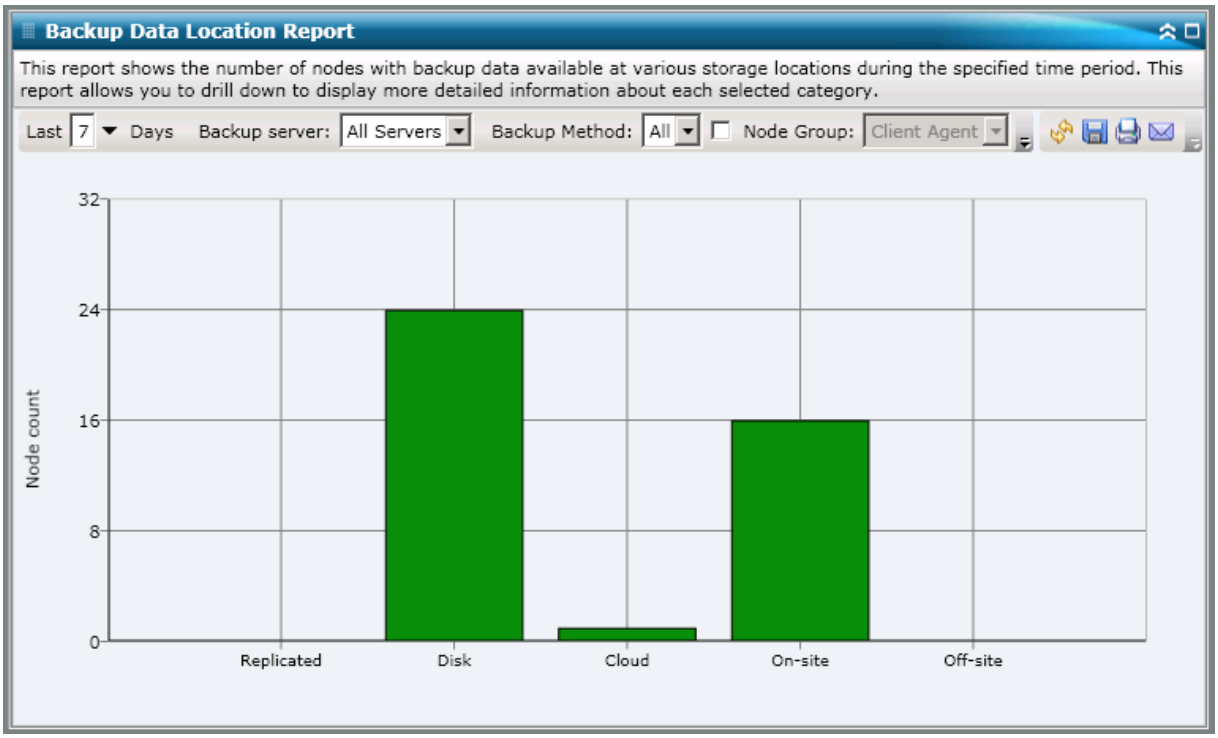
For example, if this report shows that most of your protected data is located on an onsite tape, but not also located on an offsite tape, then you should modify your backup plan because your data is not well-protected in the event of a local disaster.

In addition, this report can also be helpful in determining the most efficient means of recovering the backed up data from if necessary.

For example, if this report shows 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. This report contains filters for Last # Days, Backup Server, Backup Method, Node Group, Node Name, and Node Tier.

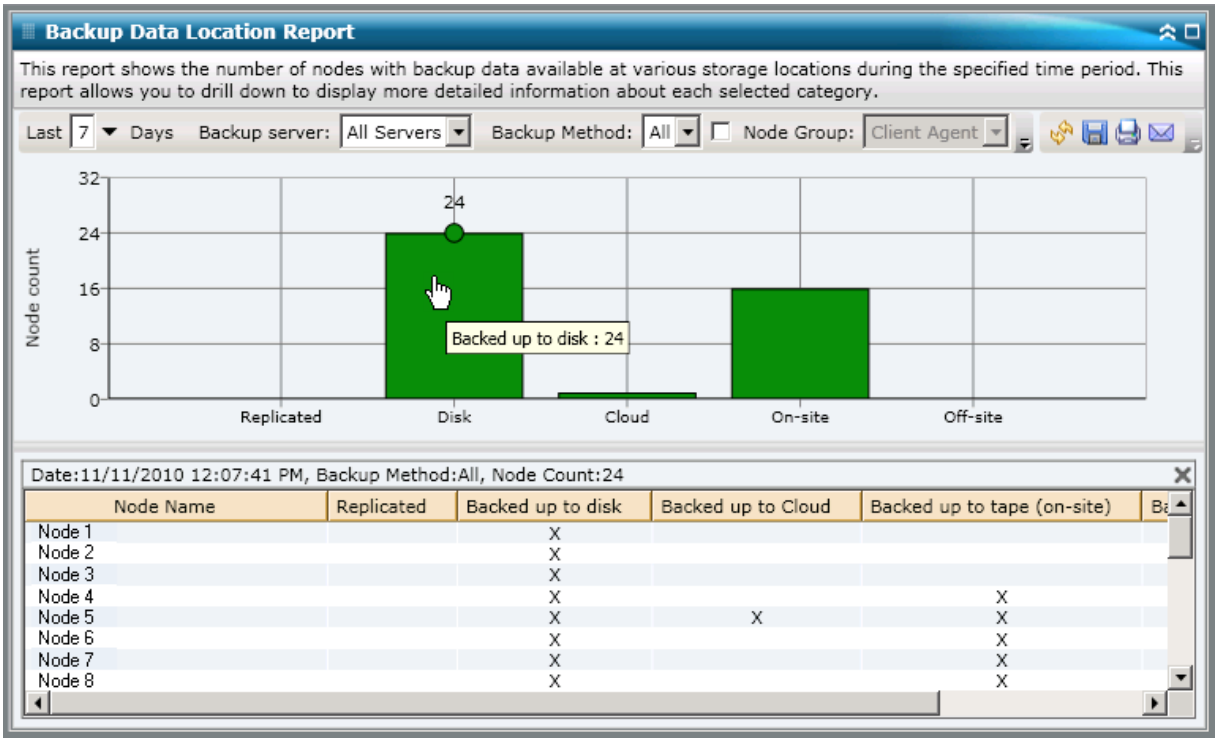


Drill Down Reports

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 62).



Backup Server Load Distribution Report

The Backup Server Load Distribution Report lists the load distribution of data on each 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 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. This report contains filters for Last # Days and Backup Method.

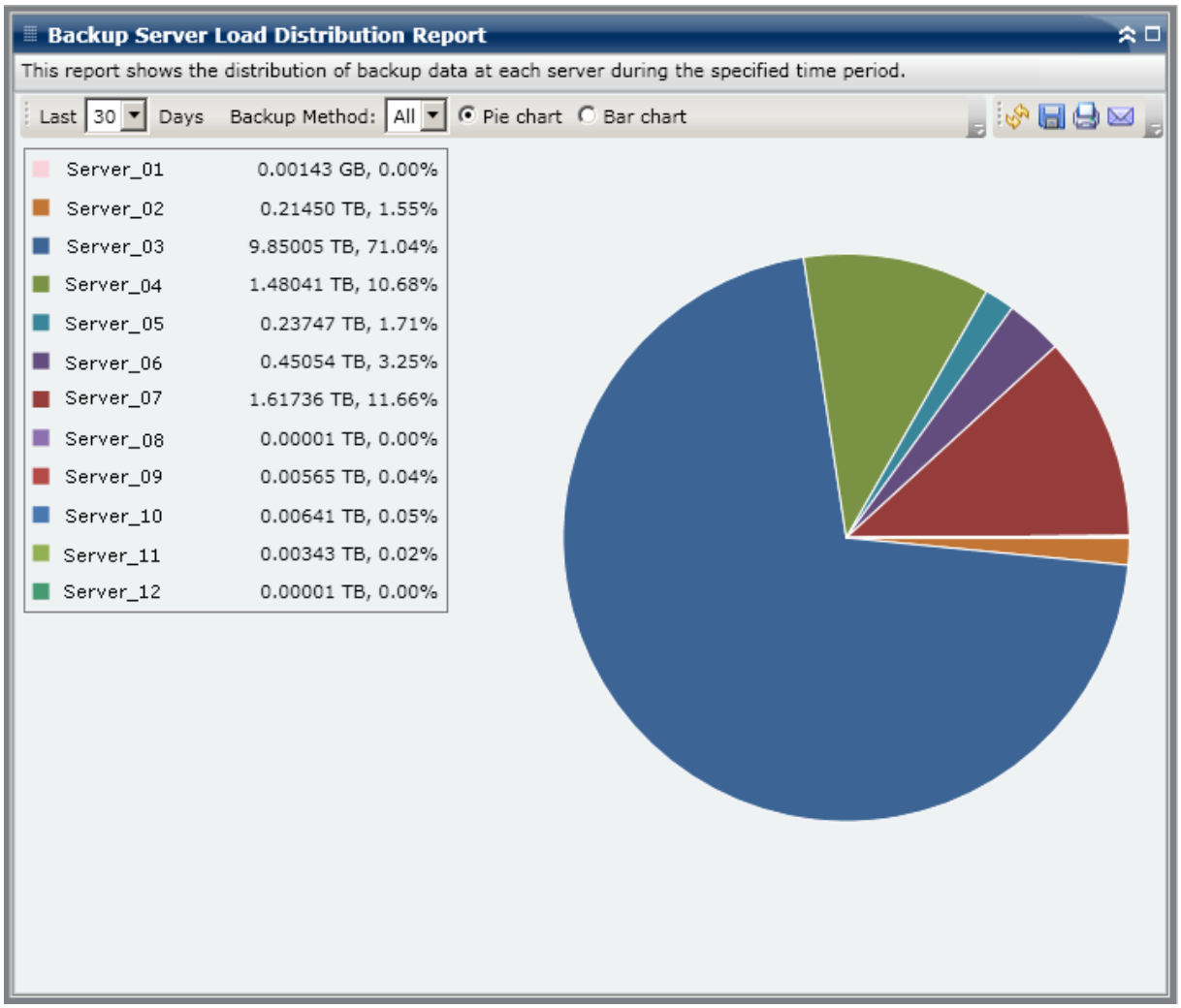
Note: If a media is reformatted, the amount of reported data in the Backup Server Load Distribution Report does not count data from any old reformatted media.

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 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).

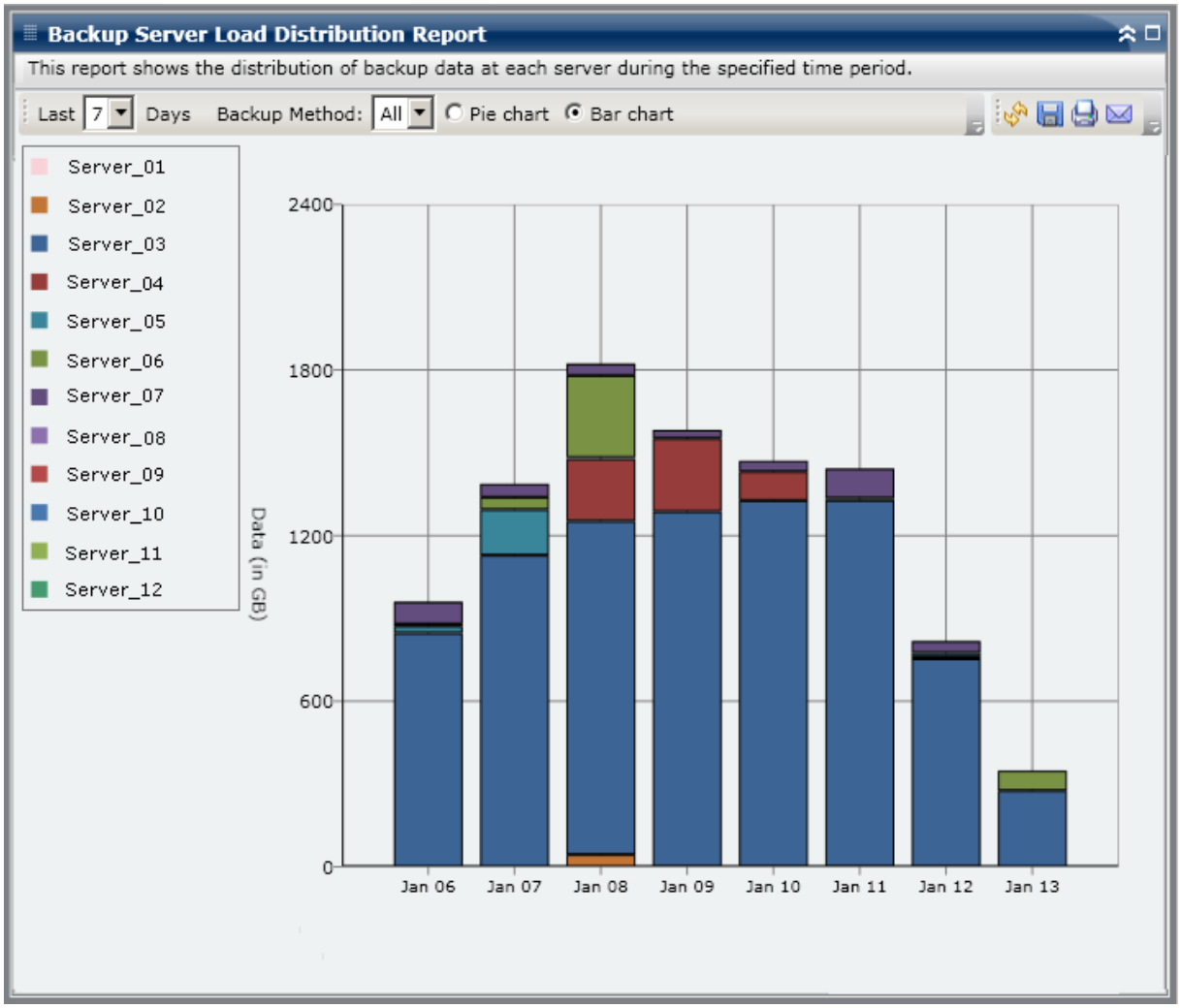


Bar Chart

The bar chart provides a detailed level view of how the backed up data is distributed between 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, 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).



Client Node Software Report

The Client Node Software Report is an SRM-type report that displays the number of nodes that contain applications that can be protected by Arcserve Backup and the protection status. This report can be used to evaluate how well the data on these applications is protected and help you to identify the applications that should be protected using Arcserve Backup agents.

Report Benefits

The Client Node Software Report is helpful in analyzing and determining the effectiveness of your protected data environment. From this report you can get a snapshot view of the installed applications on your nodes and easily determine if your application-related data is protected or not.

For example, if this report shows that you have a SQL Server, but do not have a corresponding Arcserve Backup SQL Server Agent installed on it, then you know that any data on that server is not protected and you should obtain a valid license for that agent.

In addition, this report can also be helpful in determining if you have a problem with your backups.

For example, if this report shows that you have a SQL Server and you also have a corresponding Arcserve Backup SQL Server Agent installed on it, but there has not been a successful backup during the last specified number of days, then you know that any data on that server is not protected and you should either review your scheduled backup plan to determine if a backup was attempted or investigate the reason why your backup failed.

Report View

The Client Node Software Report is displayed in bar chart or table format. This report contains filters for Not Backed Up # Days, Node Group, Node Name, and Node Tier.

Bar Chart

For each application, the bar chart displays the total node counts for the protection status classifications in your environment. A legend is also included to provide an overall summary of each application and each corresponding status classification.

For each installed application which can be protected by Arcserve Backup, there are three corresponding protection status classifications:

Protected

The corresponding Arcserve Backup agent is installed and a successful backup for this application was performed within the last specified number of days. The specified number of days can be configured from the tool bar. The default value is 7 days.

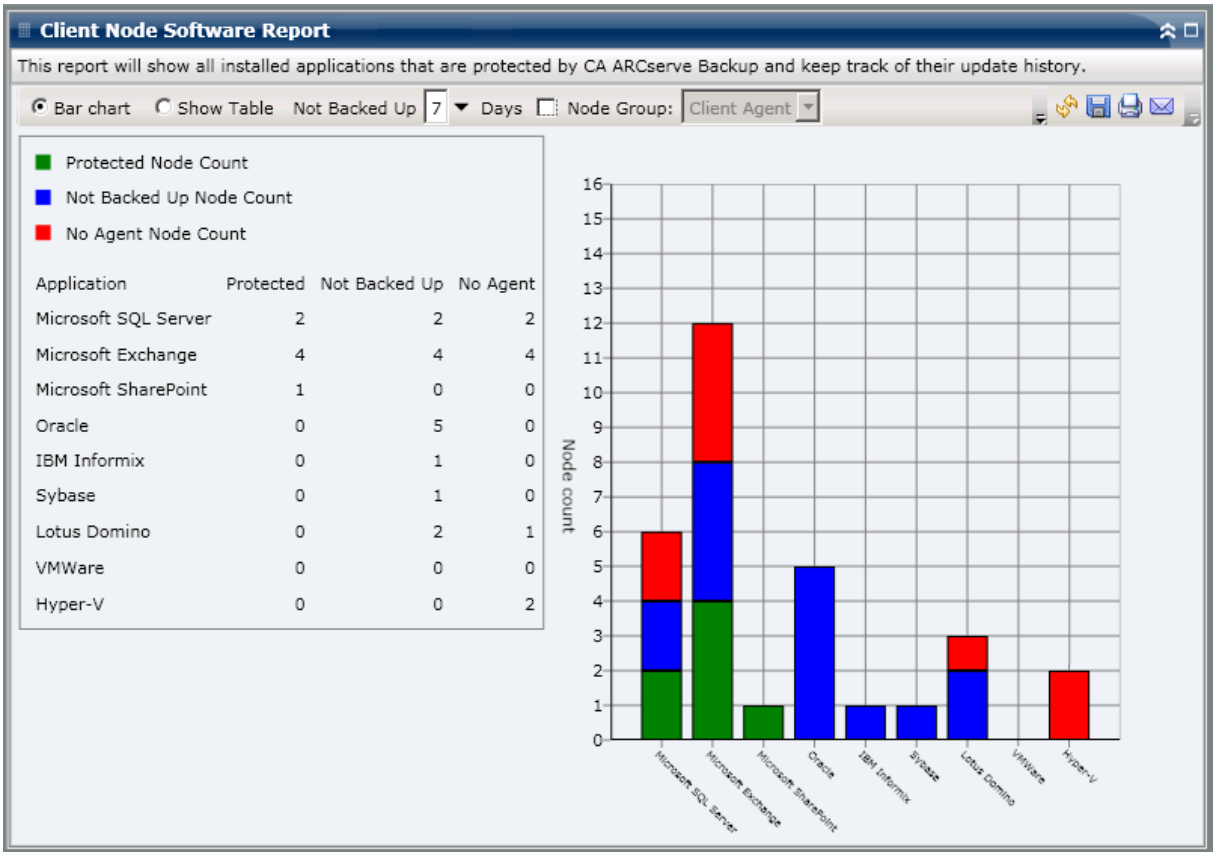
The ideal condition is for this chart to display all green (protected) bars.

Not Backed Up

The corresponding Arcserve Backup agent is installed, but there has not been a successful backup for this application in last specified number of days. Any related data is not protected by a backup and is at risk.

No Agent

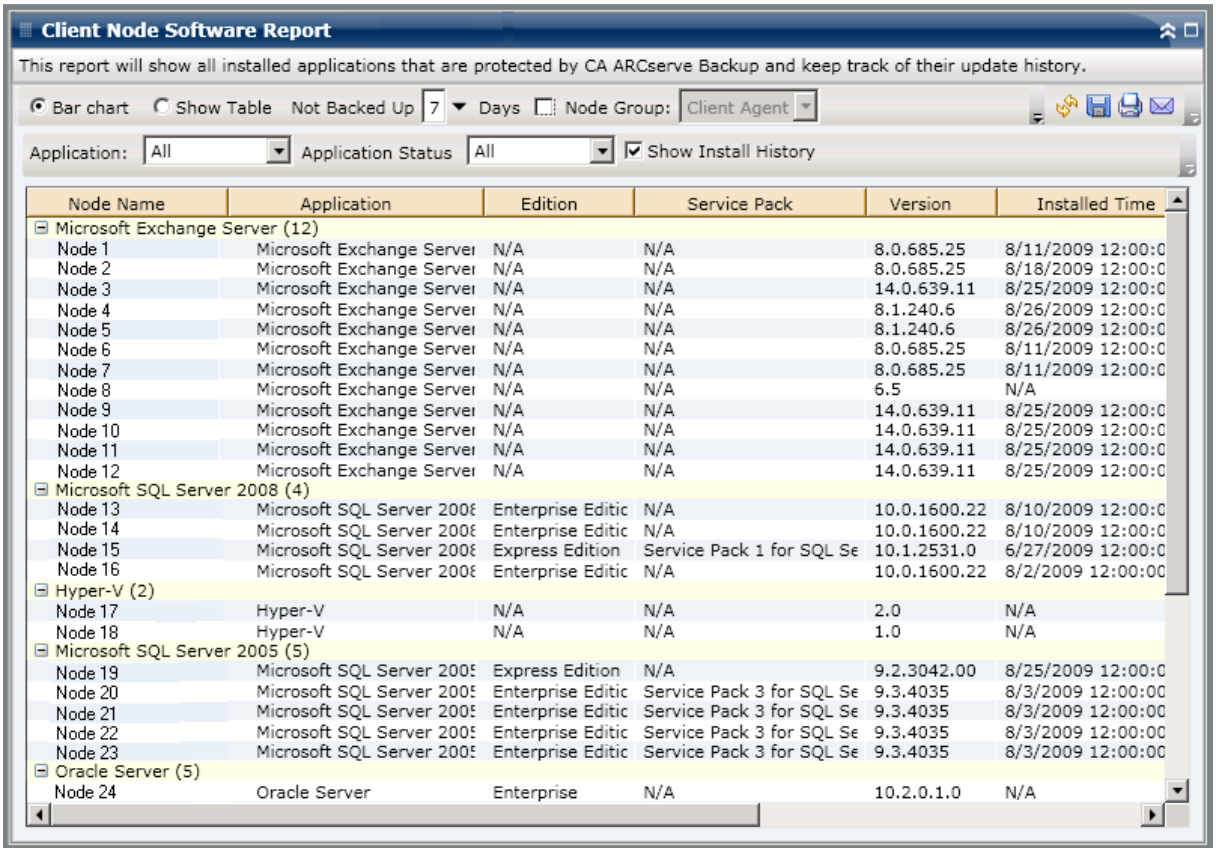
The corresponding Arcserve Backup agent is not installed for this application. Any related data is not protected by a backup and is at risk.



Application	Protected	Not Backed Up	No Agent
Microsoft SQL Server	2	2	2
Microsoft Exchange	4	4	4
Microsoft SharePoint	1	0	0
Oracle	0	5	0
IBM Informix	0	1	0
Sybase	0	1	0
Lotus Domino	0	2	1
VMWare	0	0	0
Hyper-V	0	0	2

Show Table View

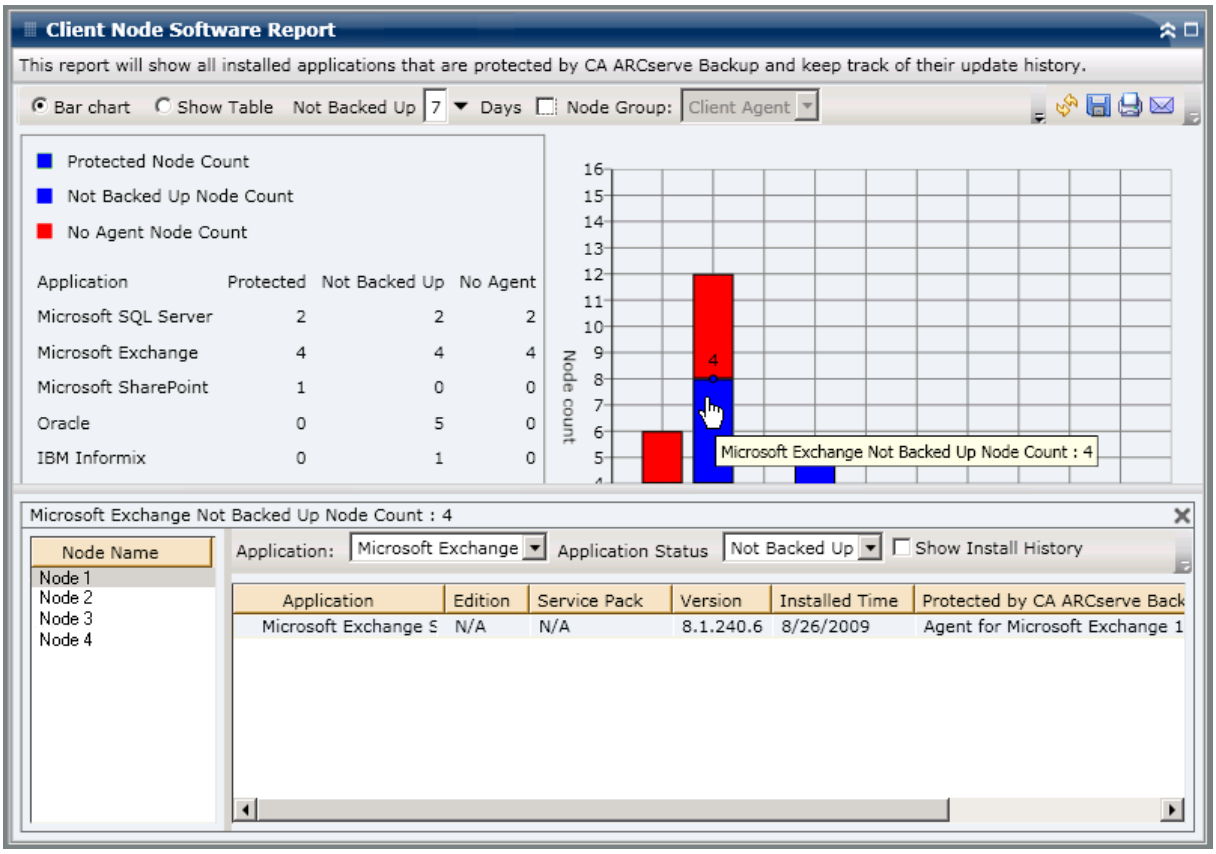
For each node, the table view displays the installed application information, as well as the associated backup status information for the node. The table listing can be filtered by a specific type of application and/or a specific backup protection status classification. You can also select to display the installation history of the listed applications.



Node Name	Application	Edition	Service Pack	Version	Installed Time
Microsoft Exchange Server (12)					
Node 1	Microsoft Exchange Server	N/A	N/A	8.0.685.25	8/11/2009 12:00:0
Node 2	Microsoft Exchange Server	N/A	N/A	8.0.685.25	8/18/2009 12:00:0
Node 3	Microsoft Exchange Server	N/A	N/A	14.0.639.11	8/25/2009 12:00:0
Node 4	Microsoft Exchange Server	N/A	N/A	8.1.240.6	8/26/2009 12:00:0
Node 5	Microsoft Exchange Server	N/A	N/A	8.1.240.6	8/26/2009 12:00:0
Node 6	Microsoft Exchange Server	N/A	N/A	8.0.685.25	8/11/2009 12:00:0
Node 7	Microsoft Exchange Server	N/A	N/A	8.0.685.25	8/11/2009 12:00:0
Node 8	Microsoft Exchange Server	N/A	N/A	6.5	N/A
Node 9	Microsoft Exchange Server	N/A	N/A	14.0.639.11	8/25/2009 12:00:0
Node 10	Microsoft Exchange Server	N/A	N/A	14.0.639.11	8/25/2009 12:00:0
Node 11	Microsoft Exchange Server	N/A	N/A	14.0.639.11	8/25/2009 12:00:0
Node 12	Microsoft Exchange Server	N/A	N/A	14.0.639.11	8/25/2009 12:00:0
Microsoft SQL Server 2008 (4)					
Node 13	Microsoft SQL Server 2008	Enterprise Editic	N/A	10.0.1600.22	8/10/2009 12:00:0
Node 14	Microsoft SQL Server 2008	Enterprise Editic	N/A	10.0.1600.22	8/10/2009 12:00:0
Node 15	Microsoft SQL Server 2008	Express Edition	Service Pack 1 for SQL Se	10.1.2531.0	6/27/2009 12:00:0
Node 16	Microsoft SQL Server 2008	Enterprise Editic	N/A	10.0.1600.22	8/2/2009 12:00:00
Hyper-V (2)					
Node 17	Hyper-V	N/A	N/A	2.0	N/A
Node 18	Hyper-V	N/A	N/A	1.0	N/A
Microsoft SQL Server 2005 (5)					
Node 19	Microsoft SQL Server 2005	Express Edition	N/A	9.2.3042.00	8/25/2009 12:00:0
Node 20	Microsoft SQL Server 2005	Enterprise Editic	Service Pack 3 for SQL Se	9.3.4035	8/3/2009 12:00:00
Node 21	Microsoft SQL Server 2005	Enterprise Editic	Service Pack 3 for SQL Se	9.3.4035	8/3/2009 12:00:00
Node 22	Microsoft SQL Server 2005	Enterprise Editic	Service Pack 3 for SQL Se	9.3.4035	8/3/2009 12:00:00
Node 23	Microsoft SQL Server 2005	Enterprise Editic	Service Pack 3 for SQL Se	9.3.4035	8/3/2009 12:00:00
Oracle Server (5)					
Node 24	Oracle Server	Enterprise	N/A	10.2.0.1.0	N/A

Drill Down Report

The Client Node Software Report can be further expanded from the bar 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. You can click on a particular node to display all applications for that node. In addition, you can use the Application filter to display all nodes containing a specific type of application.



CPU Report

The CPU Report is an SRM-type report that displays the number of Windows nodes within your 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.

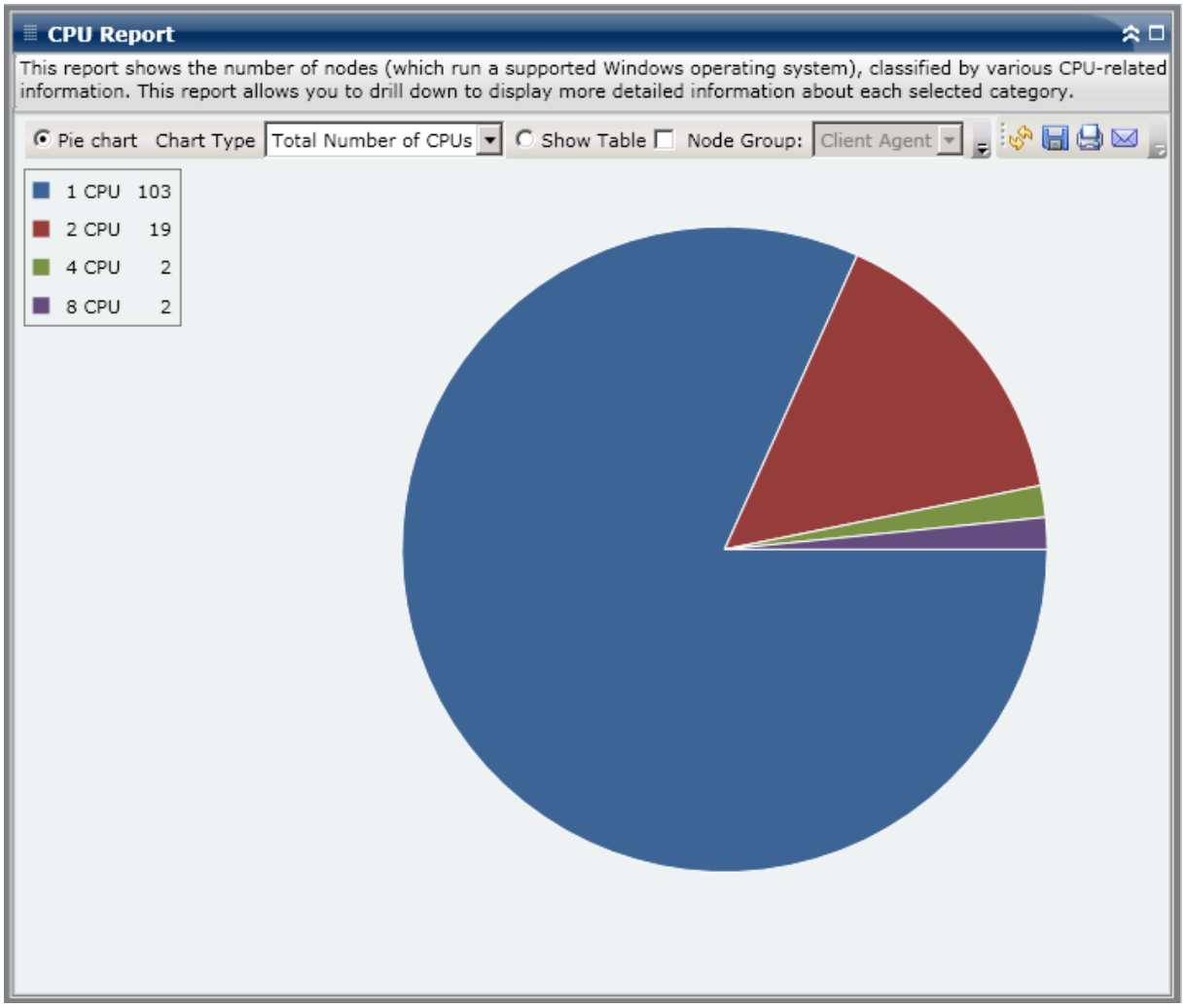
Always look for patterns in behavior to isolate potential problem CPUs and determine if nodes with the same CPUs are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The CPU Report can be displayed in either a pie chart or as a full table. This report contains filters for Chart Type (Total Number of CPUs, Manufacturer, or Architecture), Node Group, Node Name, and Node Tier.

Pie Chart

The pie chart format provides a high-level overview of the nodes within your 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).



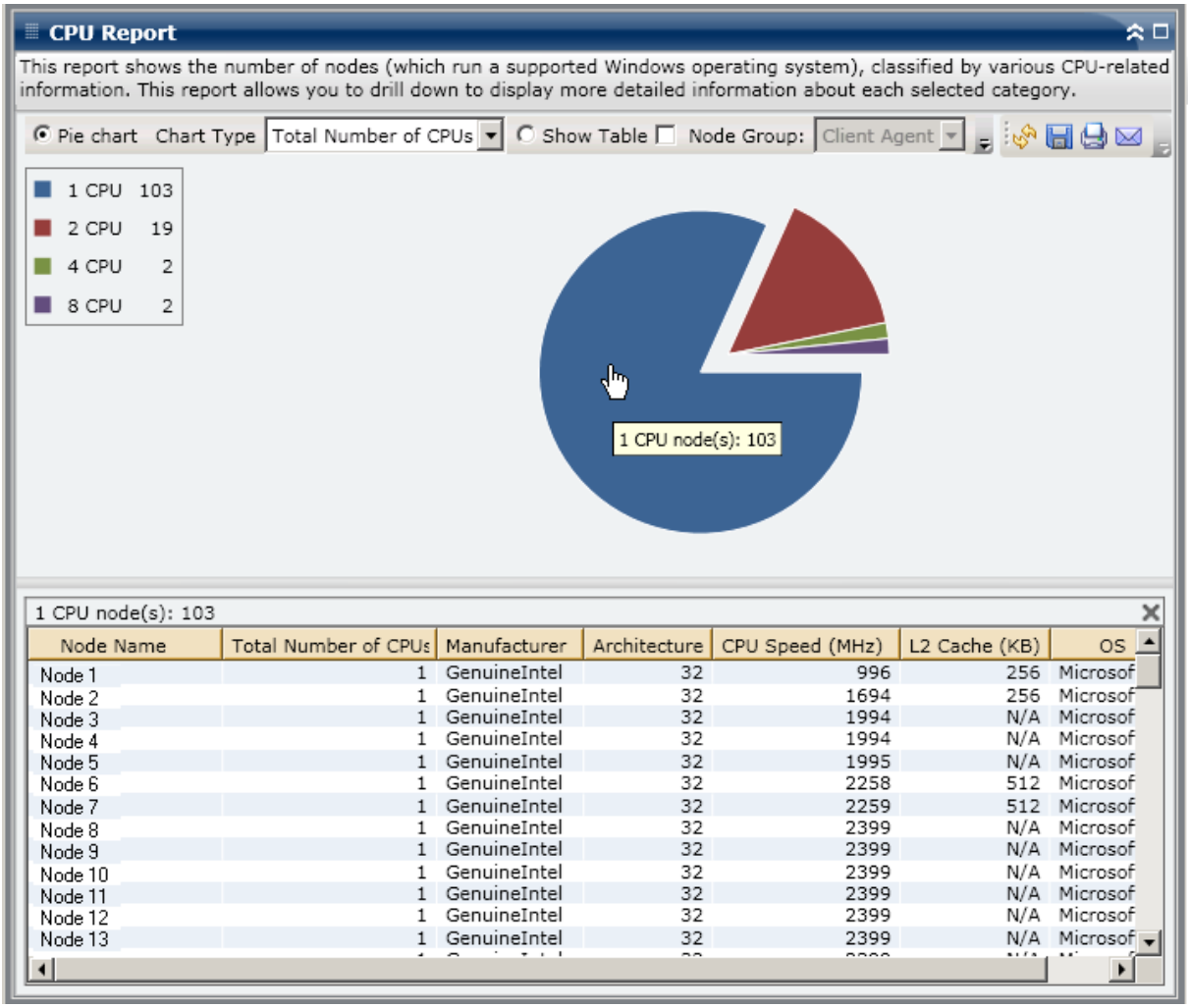
Show Table

The Table view format provides more detailed information about each node within your 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 62).

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, cloud, 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

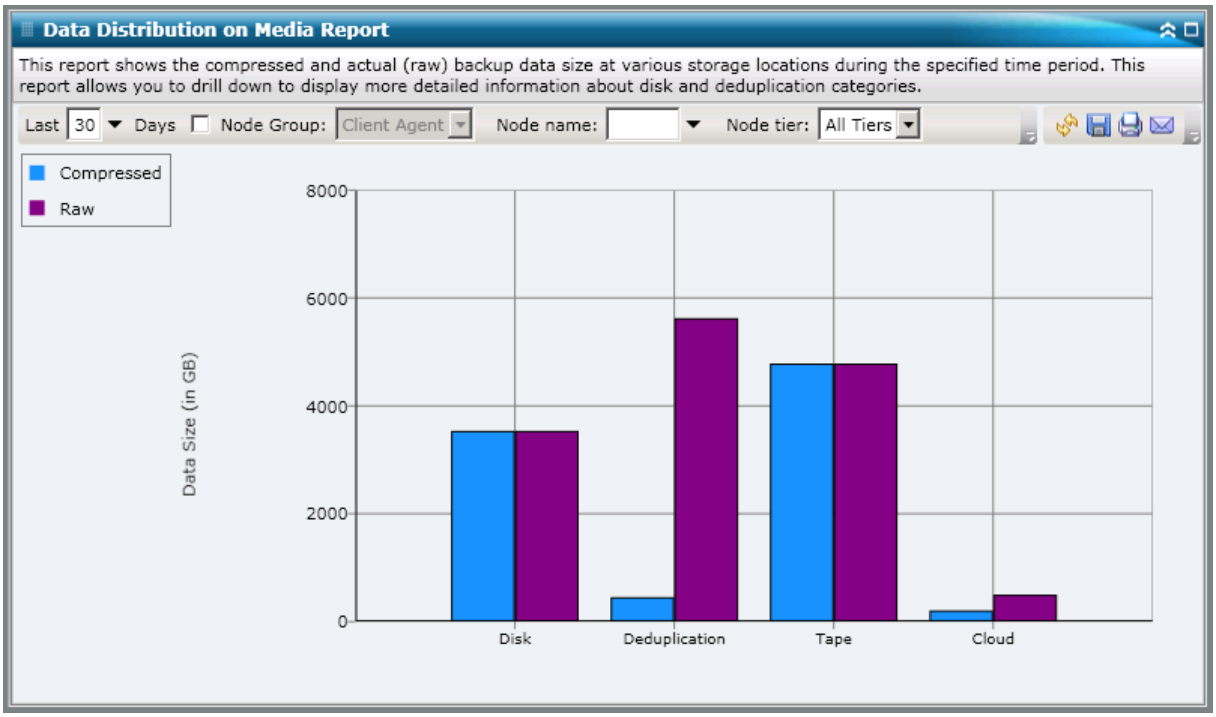
The Data Distribution on Media Report is helpful in analyzing all servers within your Arcserve Backup Domain to see how your data is distributed on various types of backup media. From this report you can also determine the amount of savings (backup size) that was gained by compressing your data during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

For example, from this report you can see that within your 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 fewer 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 a deduplication device results in a significant backup size savings.

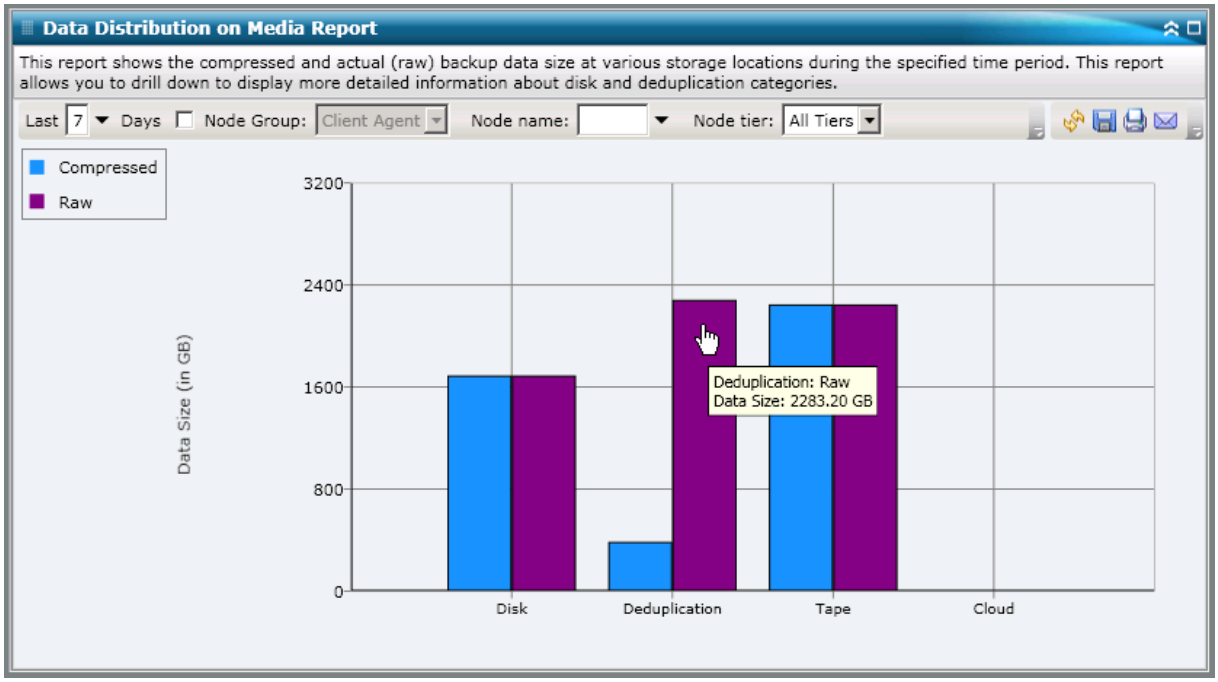
Report View

The Data Distribution on Media Report is displayed in a bar chart format, showing the amount of backup data (in GB) within your 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, Cloud, 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. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.



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, Disk, or Cloud categories to drill down and display detailed bar charts for each individual deduplication device, disk device (FSD and VTL), or Cloud device within the corresponding 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

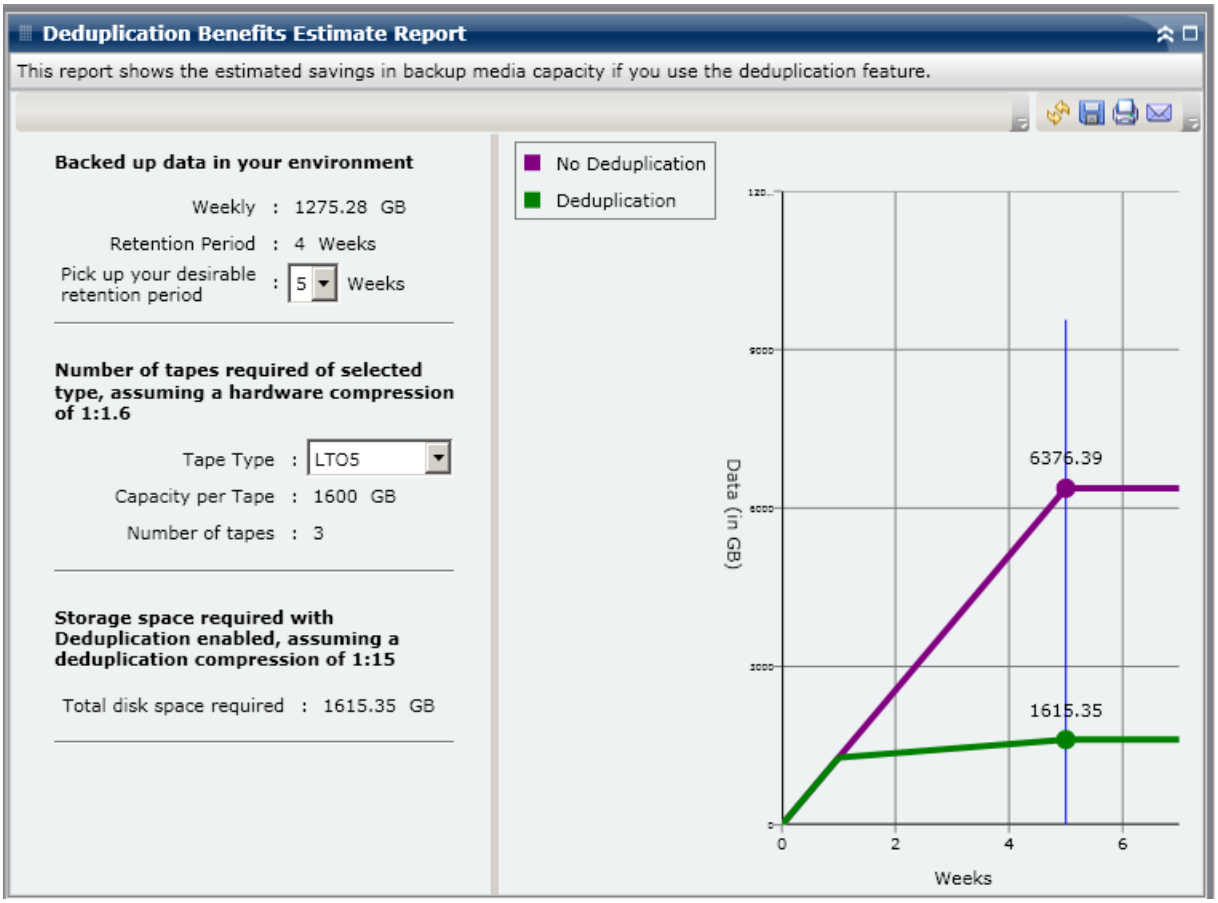
The Deduplication Benefits Estimate Report is helpful in analyzing and determining your backup capacity savings if you use or do not use the Arcserve Backup deduplication feature. This report is based upon the assumption that you are backing up same amount of data with and without deduplication and provides 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 smaller 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 was 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 of the needed backup resources.

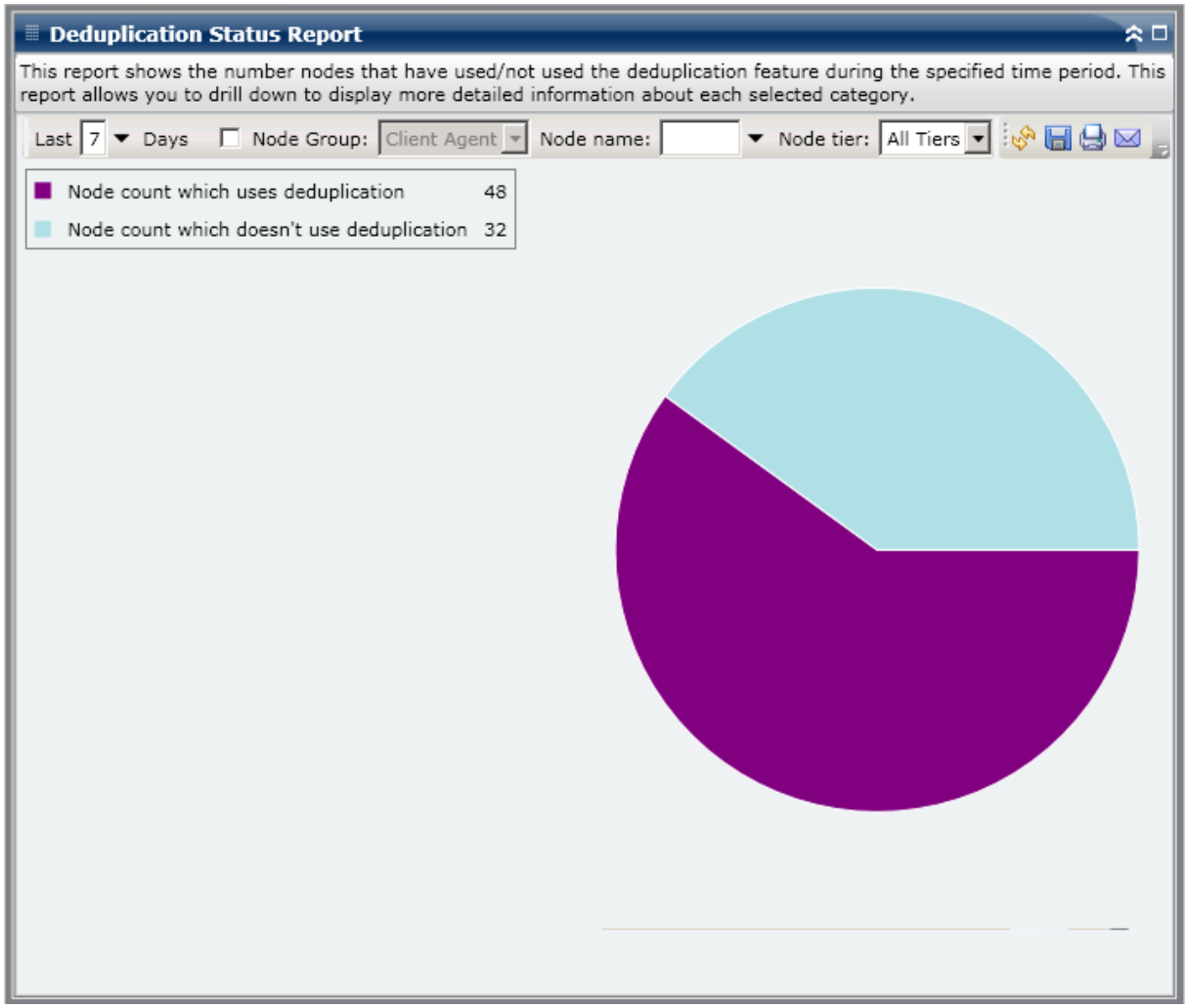
For example, if this report shows that most of your nodes have benefited from deduplication, and the amount of actual savings between the raw backup size and the compressed backup size is significant, you should consider using deduplication for more backups to improve your backup efficiency. In addition, you can also determine whether you need fewer 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 a deduplication device results 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. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

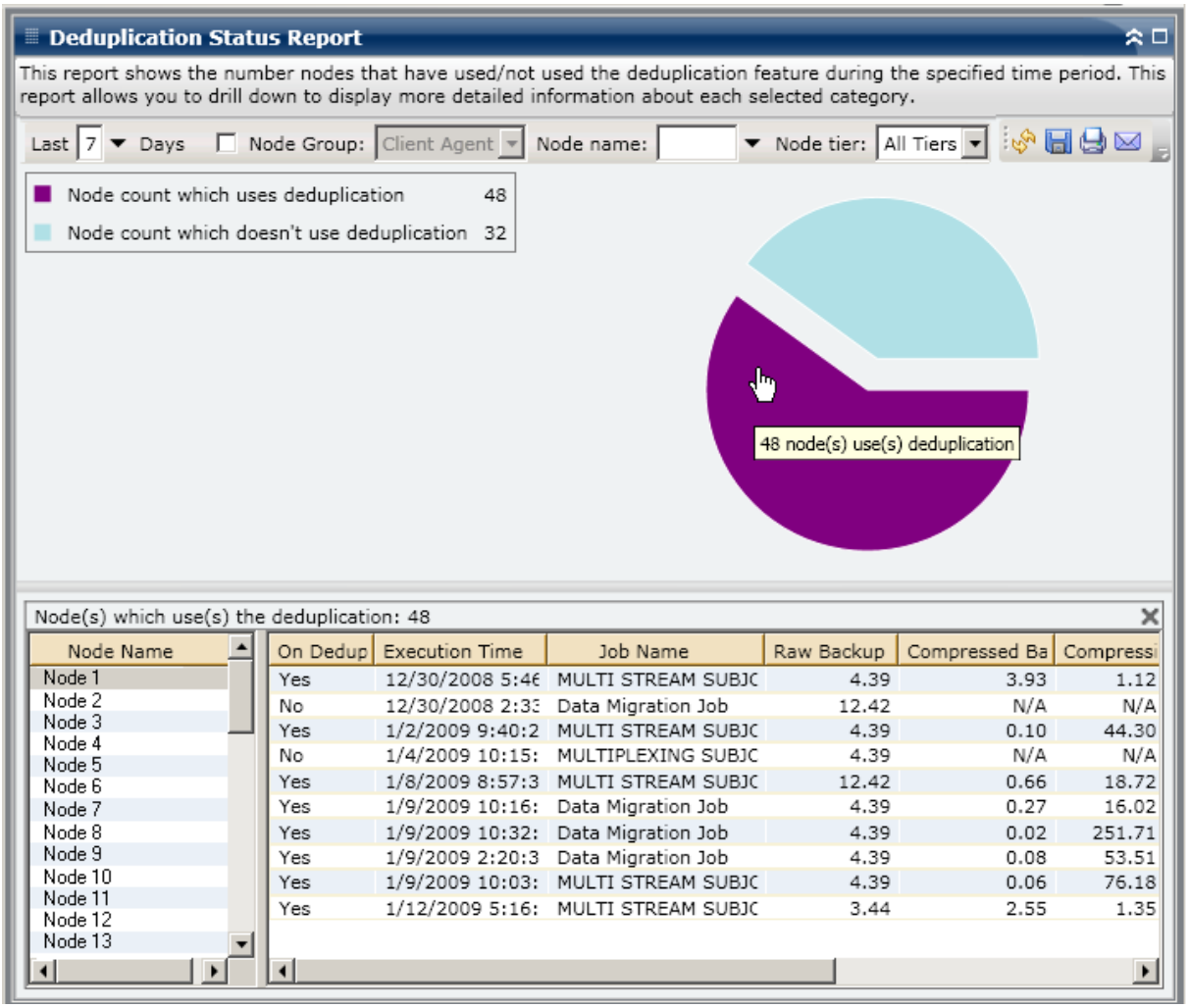
- Node count which benefited from deduplication is defined as the number of nodes that have one or more sessions which used a deduplication device, and the calculated compressed backup size is less than the raw backup size.
- Node count which did not benefit from deduplication is defined as the number 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 62).



Disk Report

The Disk Report is an SRM-type report that displays the disk information for all Windows nodes within your 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 this report shows 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.

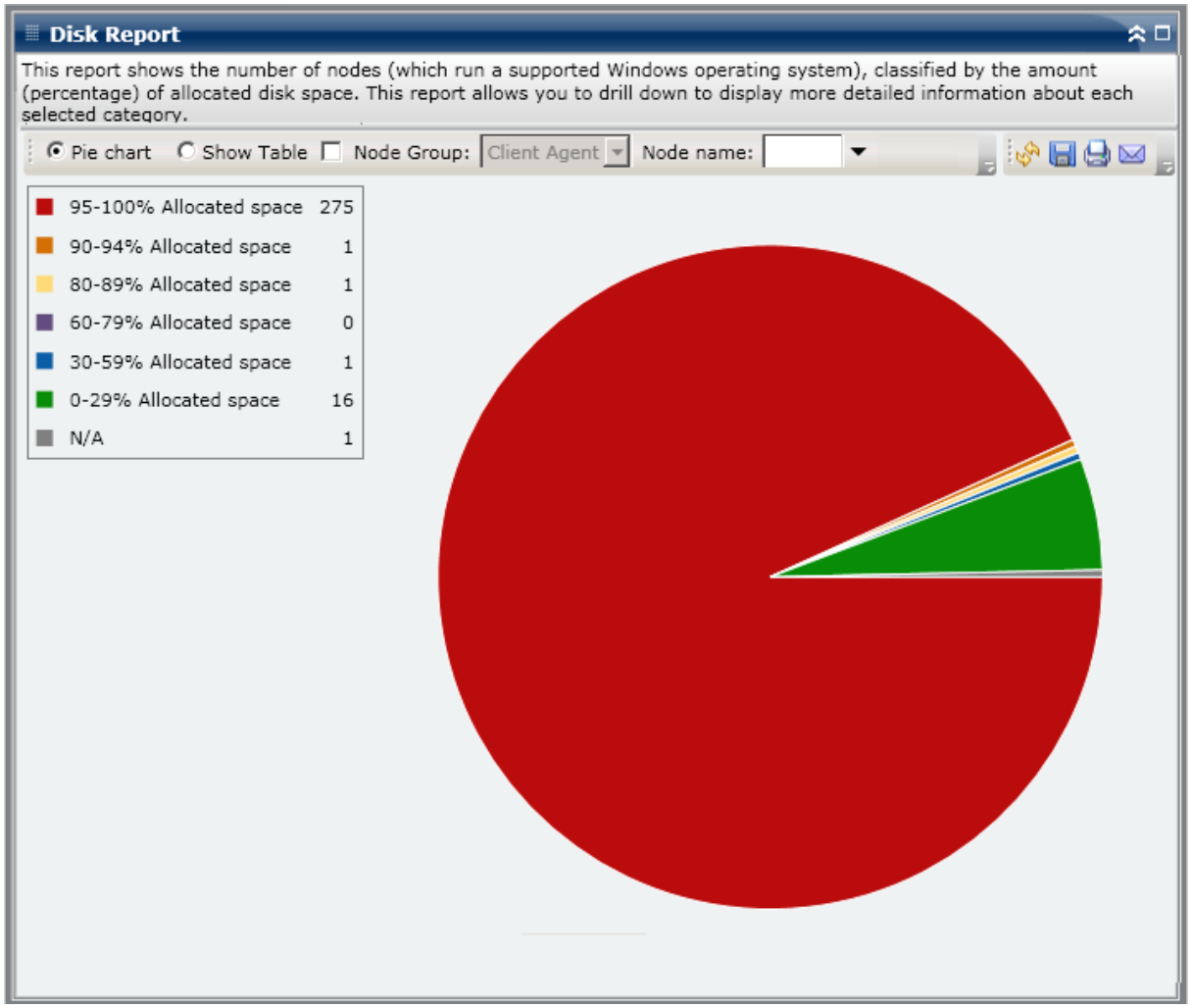
Always look for patterns in behavior to isolate potential problem disks. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Disk Report is displayed in a pie chart format or table format. This report contains filters for Node Group, Node Name, and Node Tier.

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.



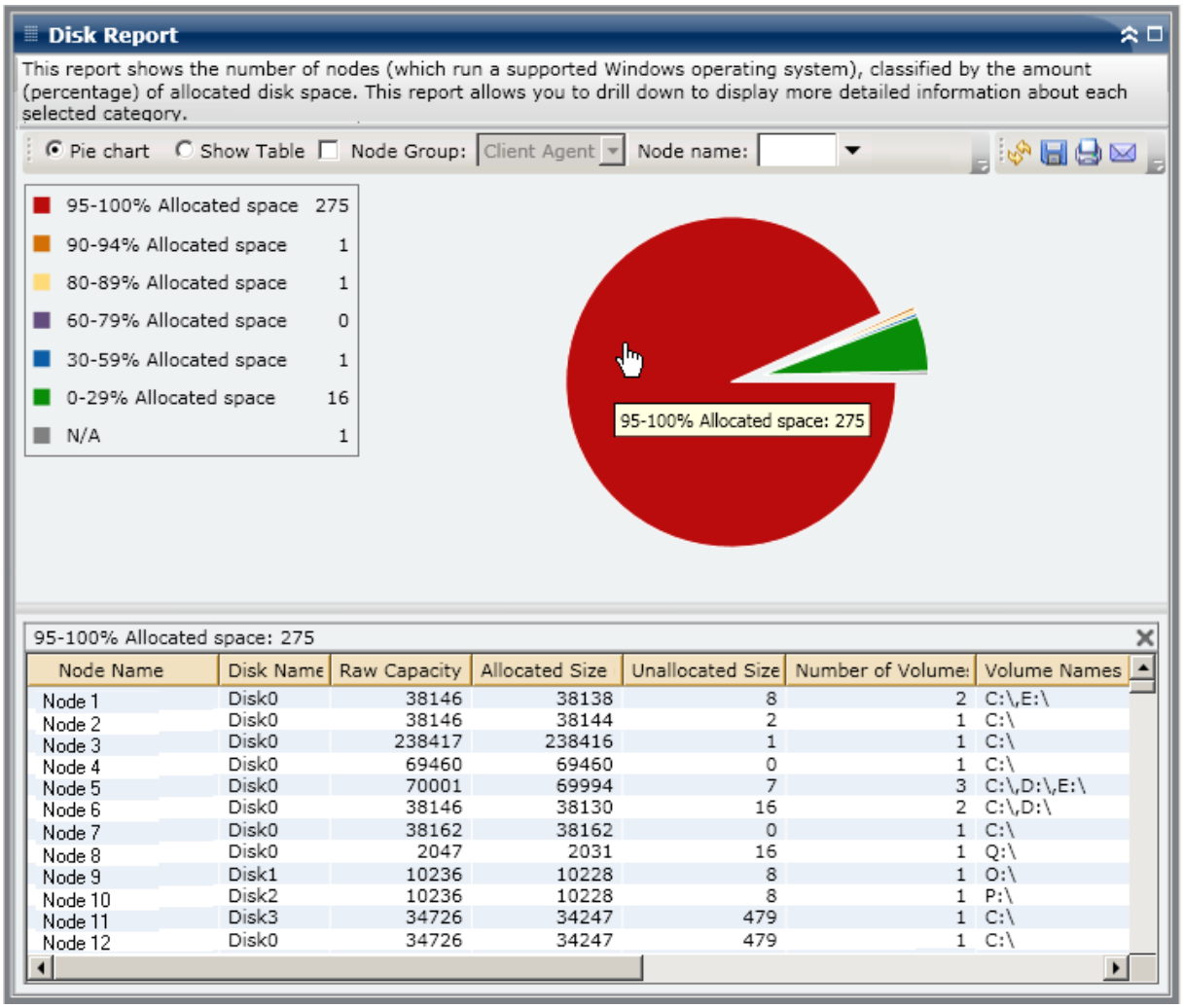
Show Table

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 62).

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 Archive Status Report

The Job Archive Status Report lists the most recent status results of all archive jobs that were initiated for the specified servers during the last specified number of days.

When an archive job has completed, a CSV file is generated and saved with the node name under the directory BAB_HOME\Archived Files on the backup server. CSV files will not be pruned by Arcserve Backup and will not be deleted if Arcserve Backup is uninstalled.

By default, Arcserve Backup r16 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, do the following:

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 Arcserve Backup database.
5. When you finish configuring the JobPruningDays key, close the Registry Editor.

Report Benefits

The Job Archive 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 archive jobs from a job perspective. If the archive status from the previous day is all green (successful), you know that you had a good archive. However, if the 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 archive 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 archive jobs.

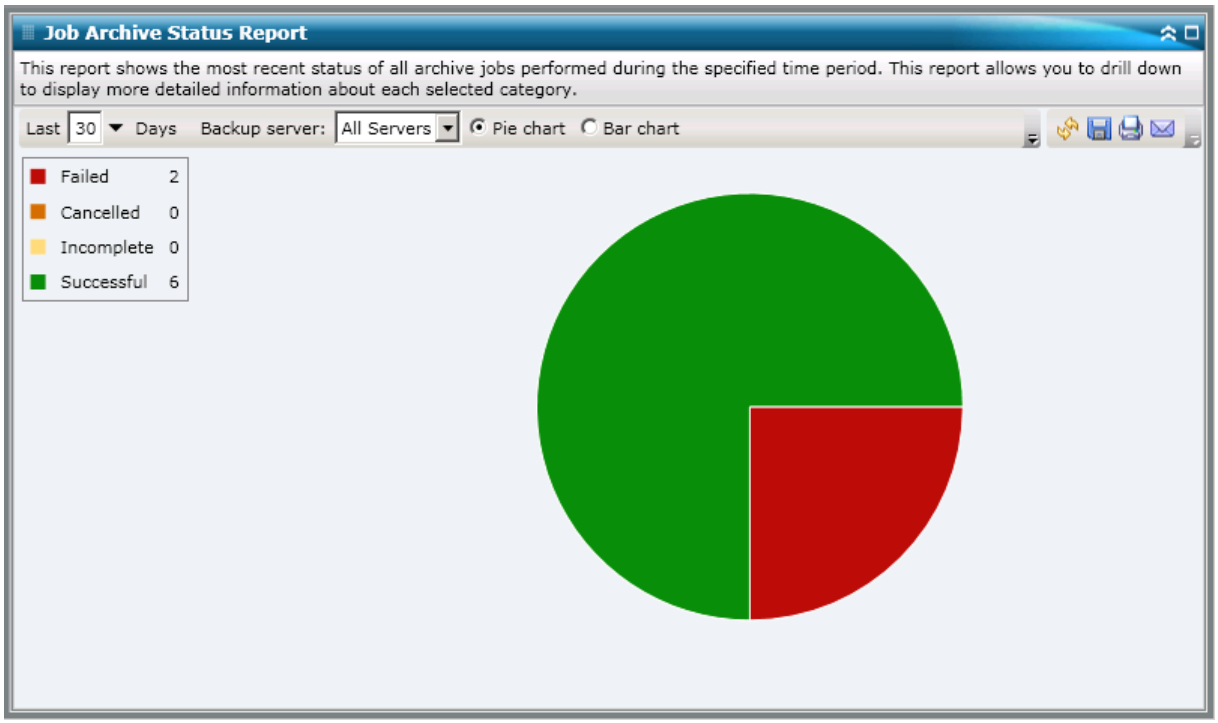
Report View

The Job Archive Status Report can be displayed as either a pie chart or as a bar chart. This report contains filters for Last # Days, Backup Server, and Job Name Contains.

Note: By default, Arcserve Backup only retains Activity Log information for 14 days. If you want 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

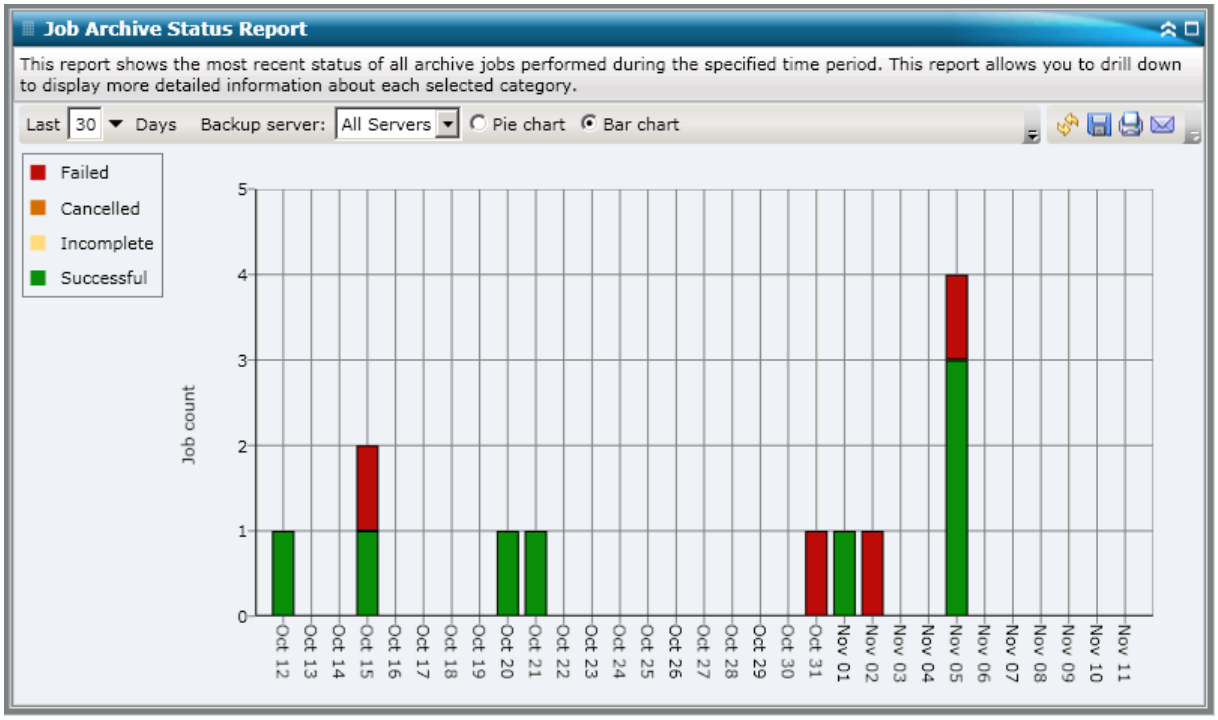
The pie chart provides a high-level overview of archive jobs for the selected server for **all days** of the specified time period. The status categories shown in the pie chart represent a percentage of the **total number** of archive jobs for that server during the last specified number of days, with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



Bar Chart

The bar chart provides a more detailed level view of archive 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 archive jobs for that server during the last specified number of days.

Note: By default, 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).



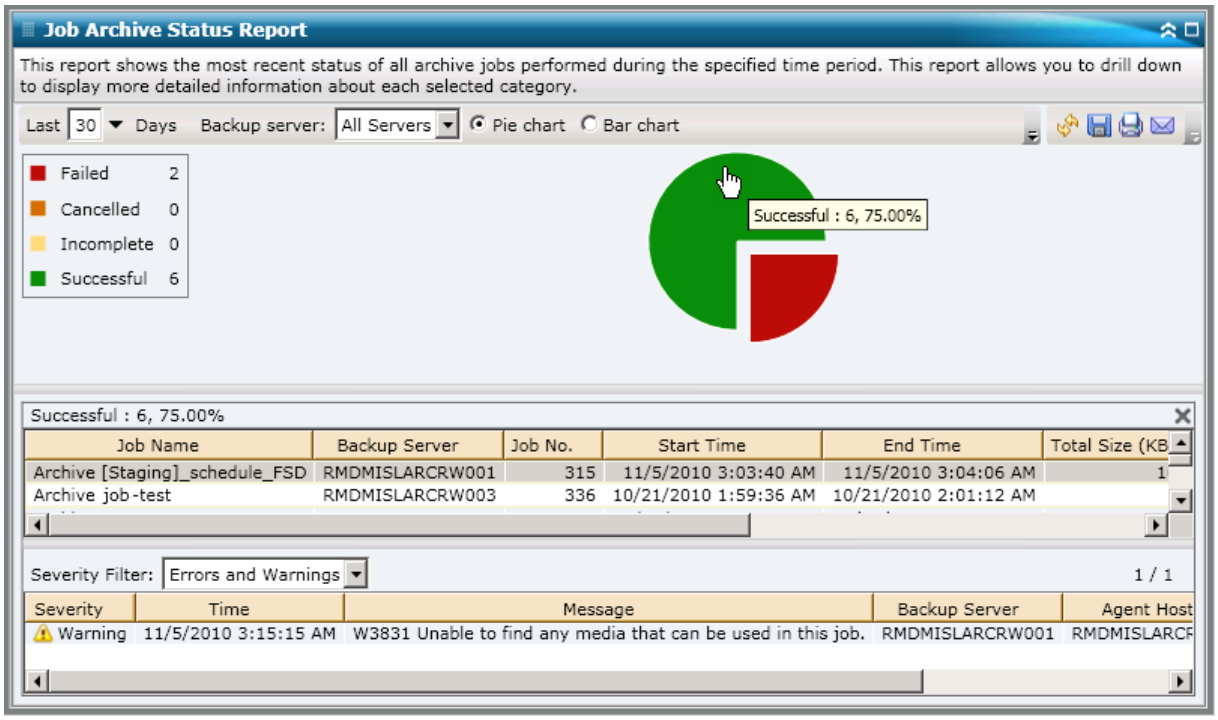
Drill Down Reports

The Job Archive 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 archive 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 archive 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 canceled archive jobs.
- **Active**--A makeup job has been created and is running. The status of the makeup job is unknown yet.
- **Finished**--After the initial archive 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 (Errors and Warnings, Errors, Warnings, Information, or All).

Be aware of the following:

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

Job Backup Status Report

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

By default, Arcserve Backup (starting with r15) 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 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.

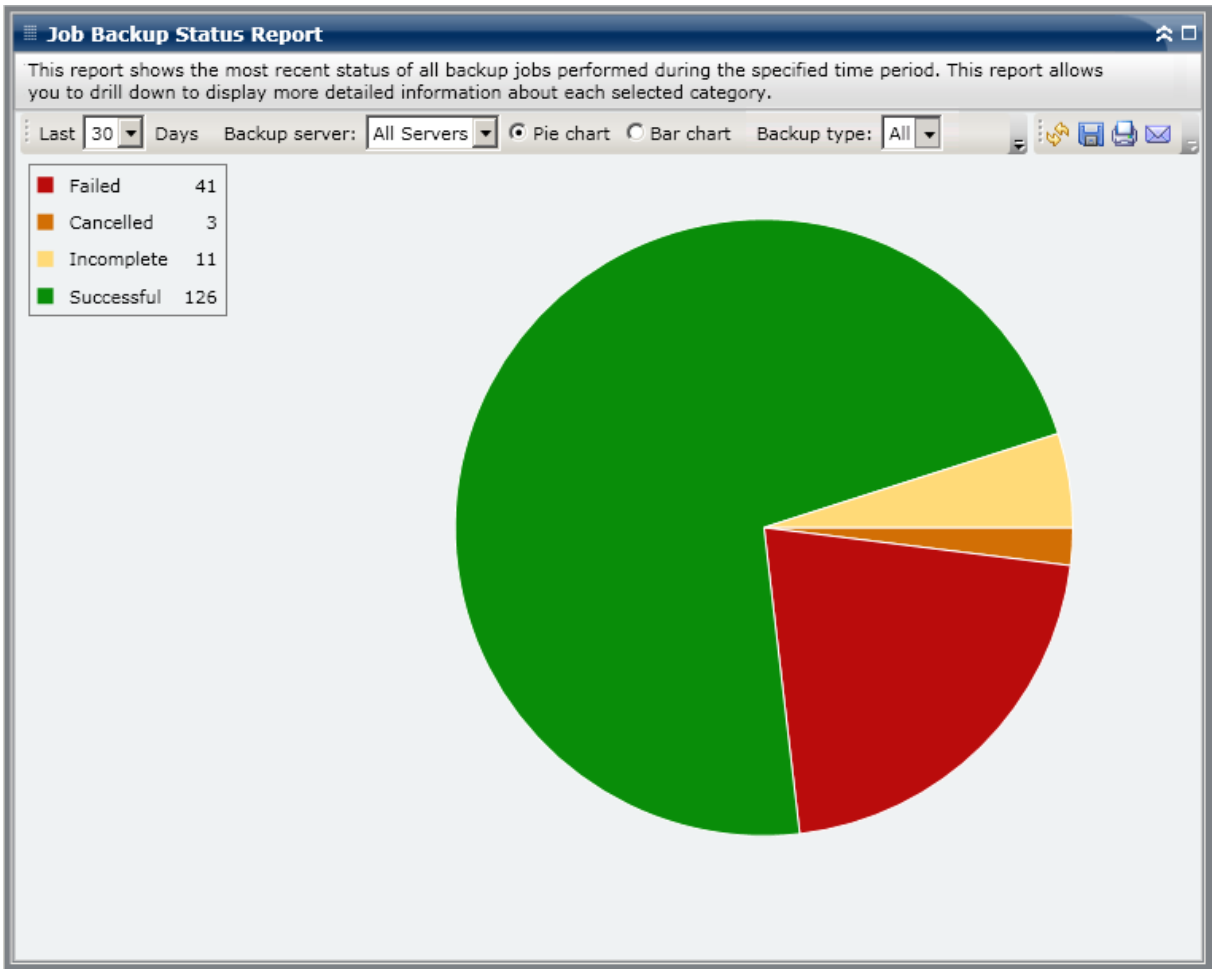
Report View

The Job Backup Status Report can be displayed as either a pie chart or as a bar chart. This report contains filters for Last # Days, Backup Server, Backup Type, and Job Name Contains.

Note: By default, Arcserve Backup only retains Activity Log information for 14 days. If you want 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

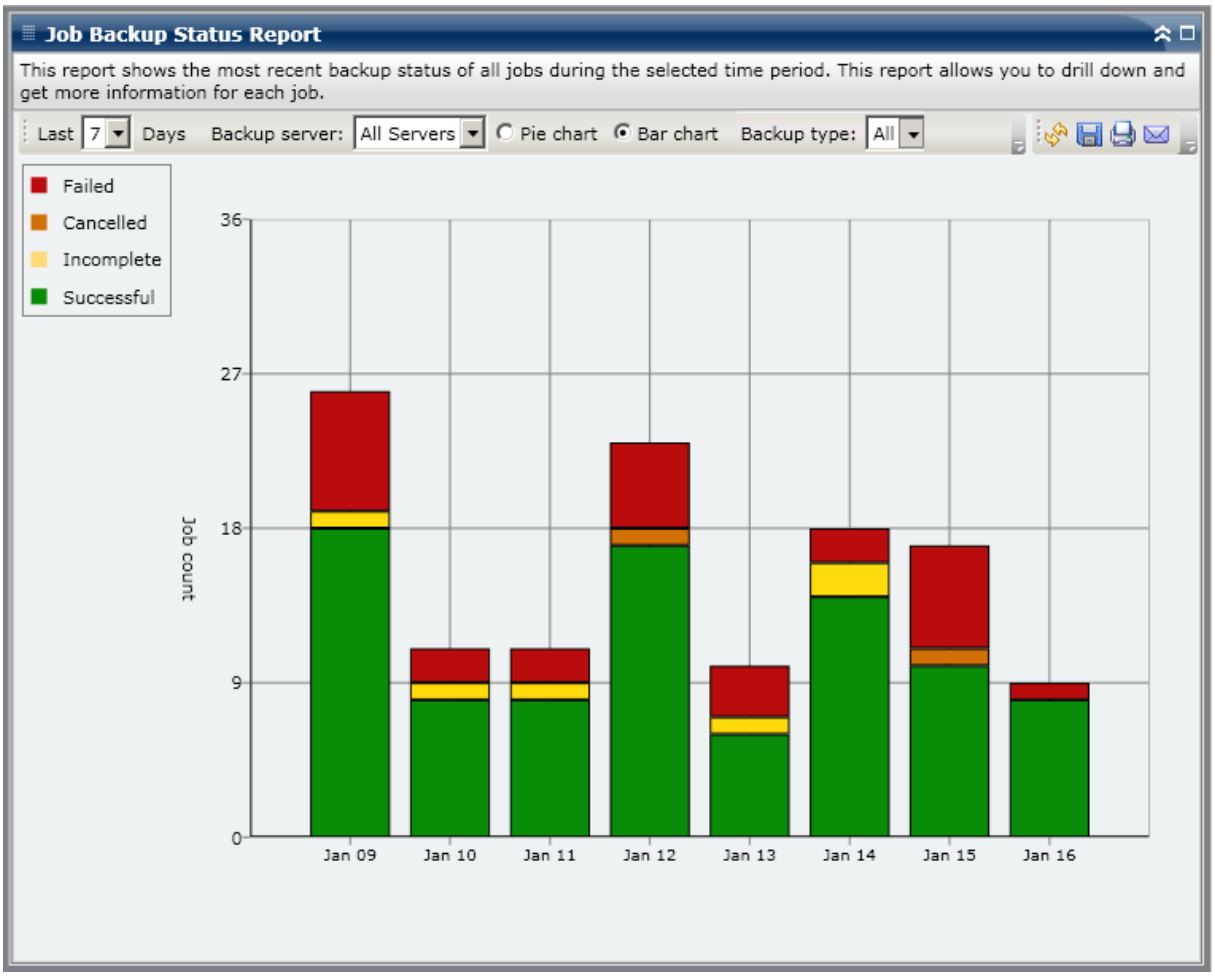
The pie chart provides a high-level overview of backup jobs for the selected server for all days of the specified time period. The status categories shown in the pie chart represent a percentage of the total number of backup jobs for that server during the last specified number of days, with the most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



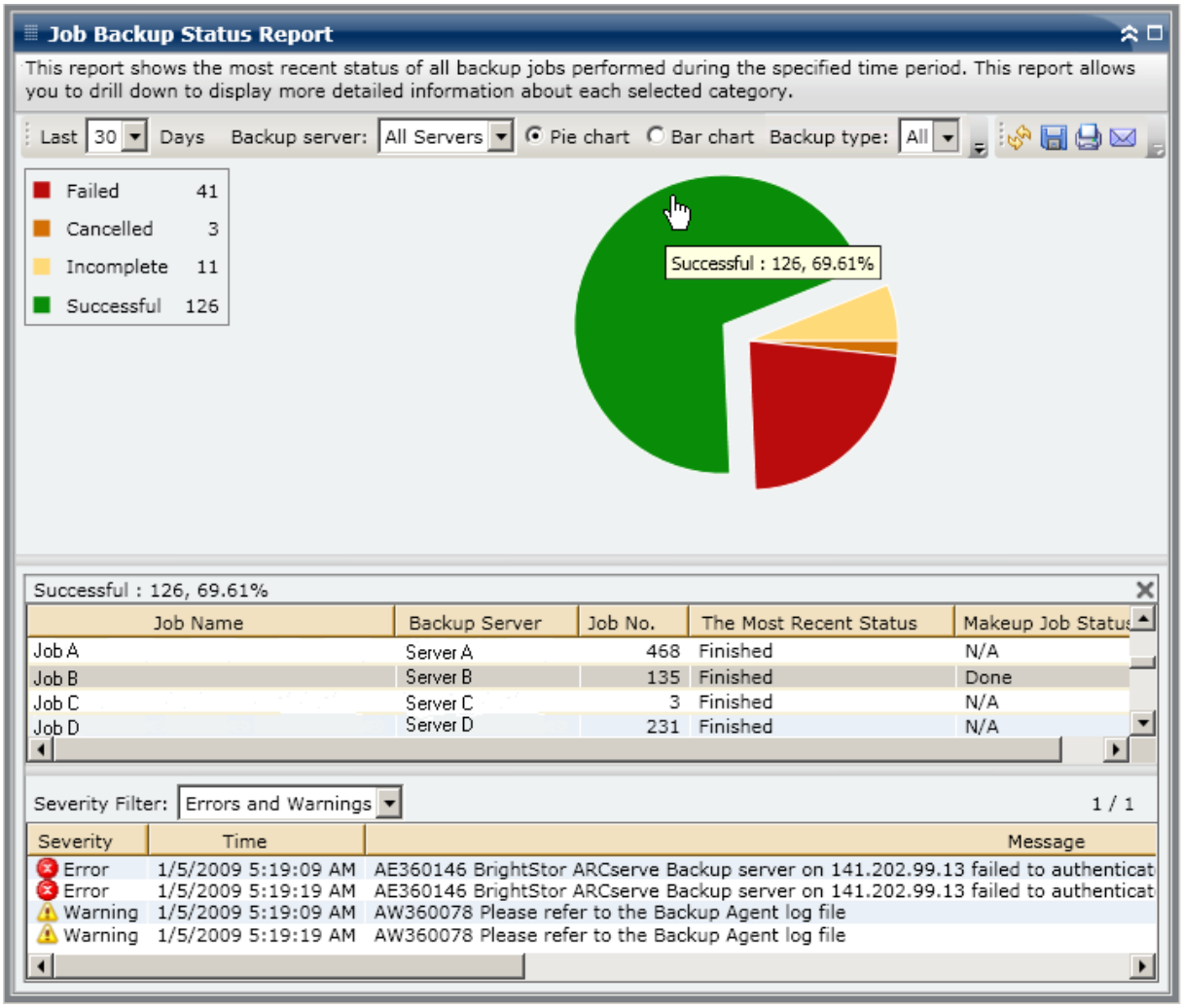
Drill Down Reports

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 canceled 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).

Be aware of the following:

- Dashboard uses pagination to display the first 100 log messages. You can click on the Next page button to view further messages.
- 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 Arcserve Backup agents and server options that are used within your Arcserve Backup domain. If the Active Licenses count for an agent or option is greater than the corresponding Available Licenses 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 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 r11.5, r12, r12.1, r12.5, r15, or r16 versions of the agents and options.

This report can be used to quickly determine the license counts and usage of your 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 Arcserve Backup components (agents and server options) are being used within your 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.

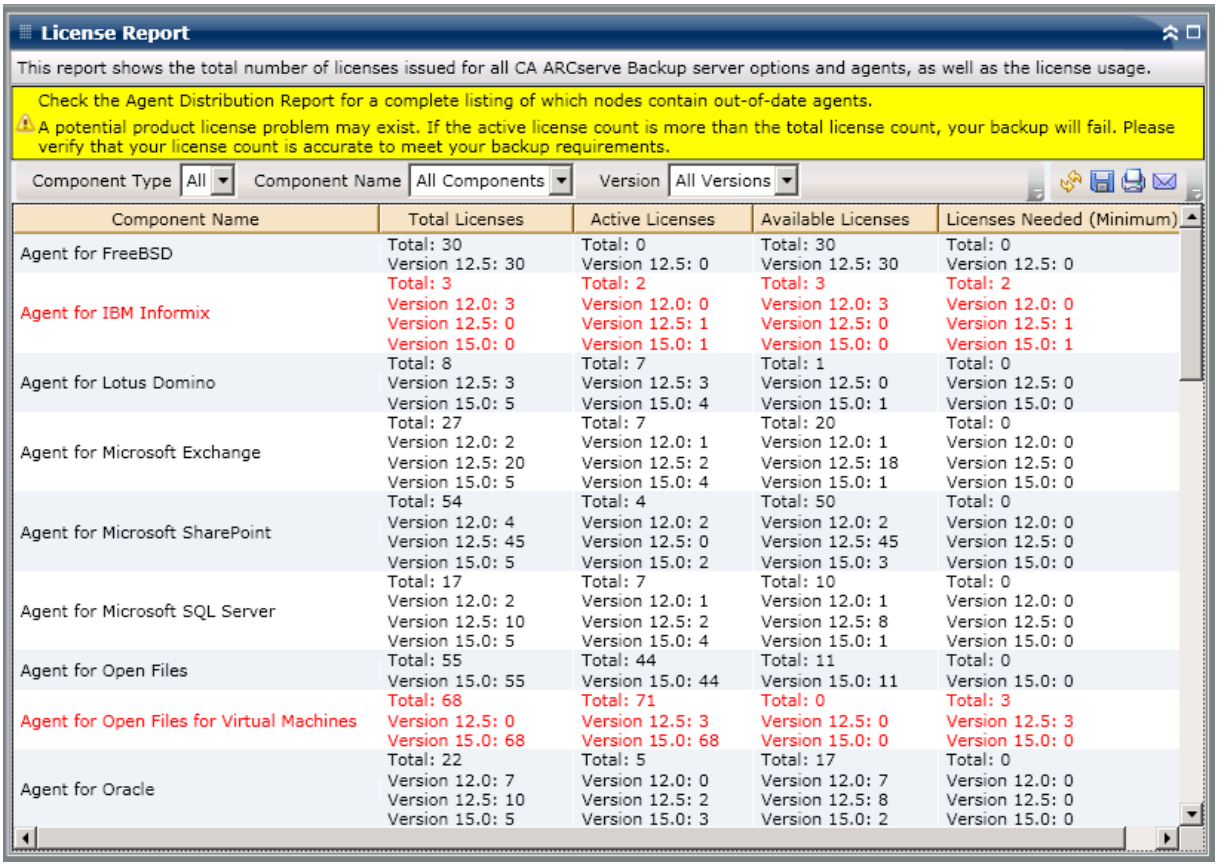
For example, if you find that your backups are failing repeatedly on specific machines, you may not be properly licensed to use certain Arcserve Backup components on that machine. From this report you can quickly determine if you have adequate license count for your current usage. If the Available Licenses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

Report View

The License Report is displayed in a table format, listing the Arcserve Backup licensed components (agents and server options) within your Arcserve Backup domain, along with their corresponding license counts (Total, Active, Available, Needed), and release version of the component. This report contains filters for Component Type, Component Name, and Version.

For this report, the columns have the following meanings:

- **Total Licenses** - Number of licenses that you have.
- **Active Licenses** - Number of licenses already in use by agents that are included in the backup job.
- **Available Licenses** - Number of licenses that you have, but are not being used.
- **Minimum Licenses Needed** - Minimum number of licenses needed for all the agents that are included in the backup job.



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 active license count is more than the total license 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	Total Licenses	Active Licenses	Available Licenses	Licenses Needed (Minimum)
Agent for FreeBSD	Total: 30 Version 12.5: 30	Total: 0 Version 12.5: 0	Total: 30 Version 12.5: 30	Total: 0 Version 12.5: 0
Agent for IBM Informix	Total: 3 Version 12.0: 3 Version 12.5: 0 Version 15.0: 0	Total: 2 Version 12.0: 0 Version 12.5: 1 Version 15.0: 1	Total: 3 Version 12.0: 3 Version 12.5: 0 Version 15.0: 0	Total: 2 Version 12.0: 0 Version 12.5: 1 Version 15.0: 1
Agent for Lotus Domino	Total: 8 Version 12.5: 3 Version 15.0: 5	Total: 7 Version 12.5: 3 Version 15.0: 4	Total: 1 Version 12.5: 0 Version 15.0: 1	Total: 0 Version 12.5: 0 Version 15.0: 0
Agent for Microsoft Exchange	Total: 27 Version 12.0: 2 Version 12.5: 20 Version 15.0: 5	Total: 7 Version 12.0: 1 Version 12.5: 2 Version 15.0: 4	Total: 20 Version 12.0: 1 Version 12.5: 18 Version 15.0: 1	Total: 0 Version 12.0: 0 Version 12.5: 0 Version 15.0: 0
Agent for Microsoft SharePoint	Total: 54 Version 12.0: 4 Version 12.5: 45 Version 15.0: 5	Total: 4 Version 12.0: 2 Version 12.5: 0 Version 15.0: 2	Total: 50 Version 12.0: 2 Version 12.5: 45 Version 15.0: 3	Total: 0 Version 12.0: 0 Version 12.5: 0 Version 15.0: 0
Agent for Microsoft SQL Server	Total: 17 Version 12.0: 2 Version 12.5: 10 Version 15.0: 5	Total: 7 Version 12.0: 1 Version 12.5: 2 Version 15.0: 4	Total: 10 Version 12.0: 1 Version 12.5: 8 Version 15.0: 1	Total: 0 Version 12.0: 0 Version 12.5: 0 Version 15.0: 0
Agent for Open Files	Total: 55 Version 15.0: 55	Total: 44 Version 15.0: 44	Total: 11 Version 15.0: 11	Total: 0 Version 15.0: 0
Agent for Open Files for Virtual Machines	Total: 68 Version 12.5: 0 Version 15.0: 68	Total: 71 Version 12.5: 3 Version 15.0: 68	Total: 0 Version 12.5: 0 Version 15.0: 0	Total: 3 Version 12.5: 3 Version 15.0: 0
Agent for Oracle	Total: 22 Version 12.0: 7 Version 12.5: 10 Version 15.0: 5	Total: 5 Version 12.0: 0 Version 12.5: 2 Version 15.0: 3	Total: 17 Version 12.0: 7 Version 12.5: 8 Version 15.0: 2	Total: 0 Version 12.0: 0 Version 12.5: 0 Version 15.0: 0

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, Arcserve Backup almost eliminates the possibility that your restores will fail.

Generally if a specific node contains high-priority data, 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 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 high priority 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.

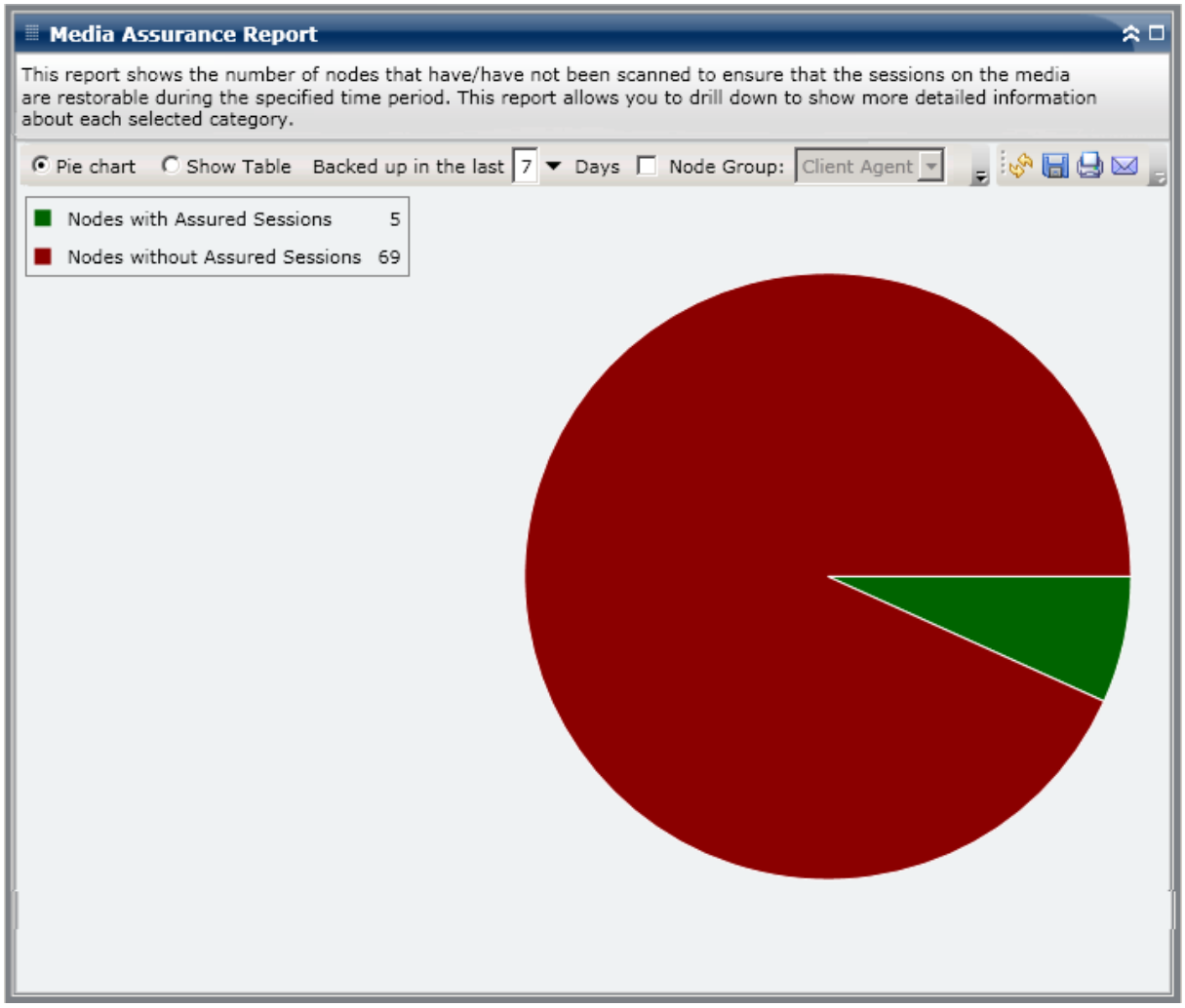
Report View

The Media Assurance Report can be displayed as either a pie chart or as a table. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

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.



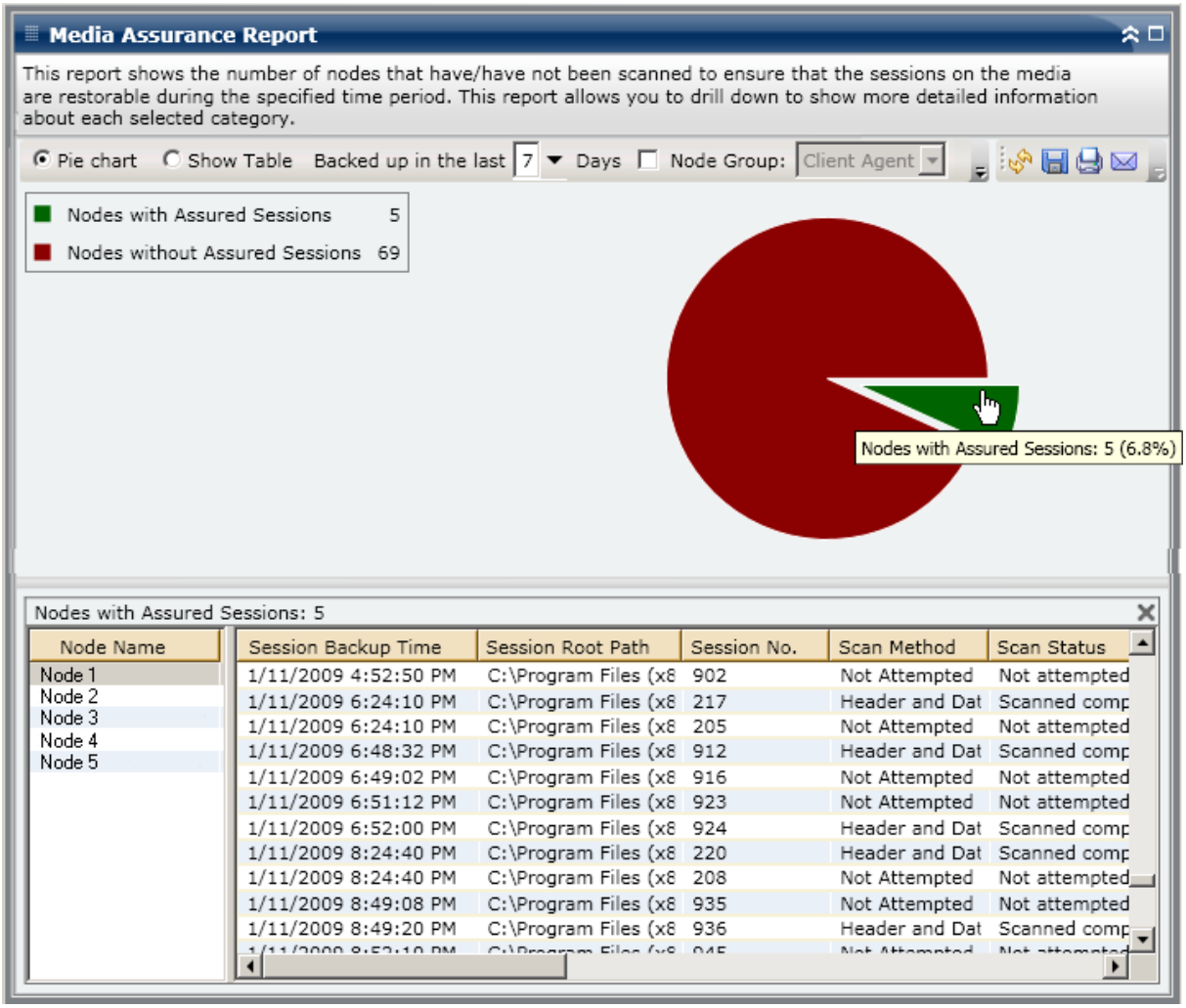
Show Table

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 62).

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 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 this report shows 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.

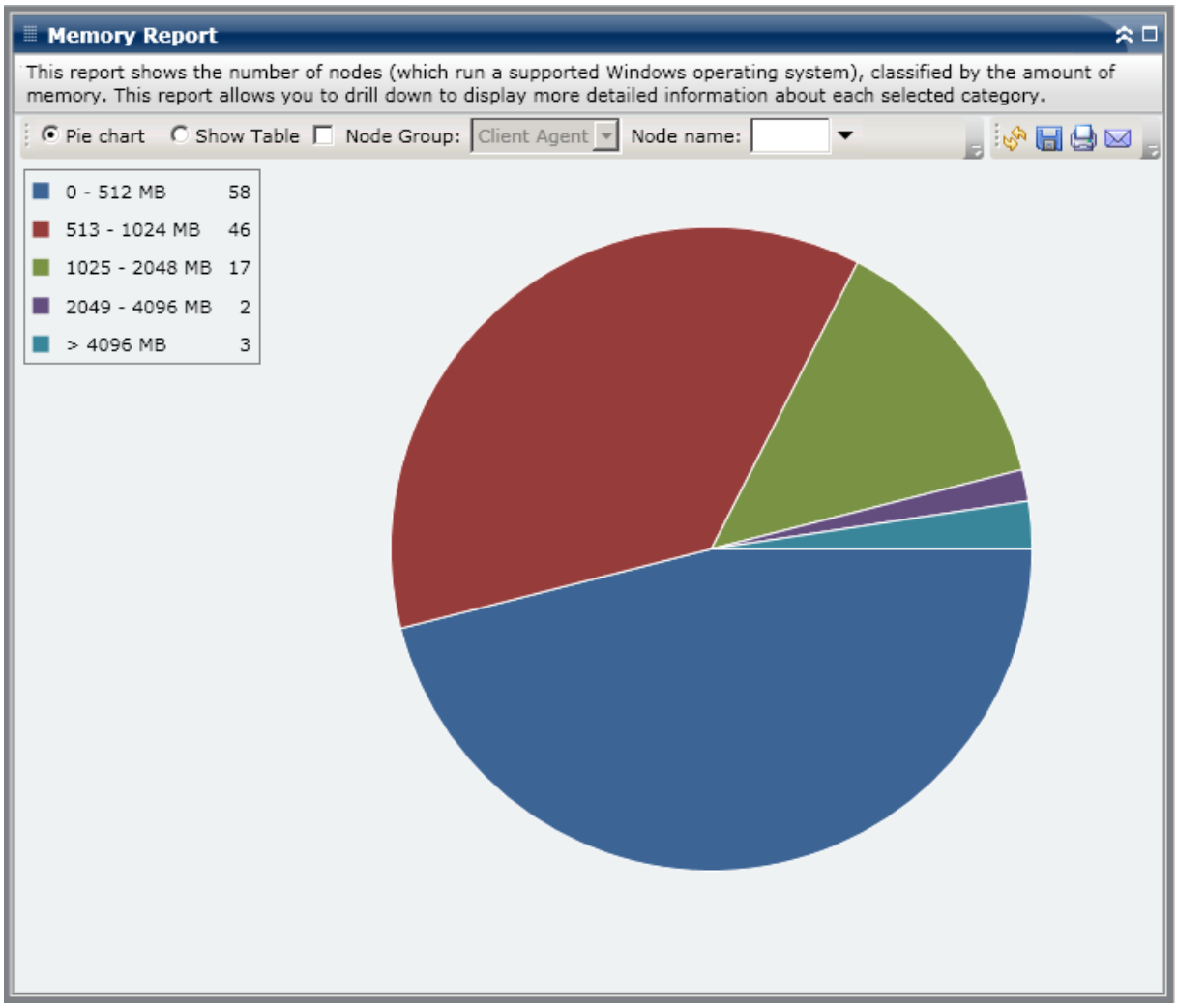
Always look for patterns in behavior to isolate potential problem with memory and determine if nodes with the same amount of memory are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Memory Report can be displayed as either a pie chart or as a table. This report contains filters for Node Group, Node Name, and Node Tier.

Pie Chart

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



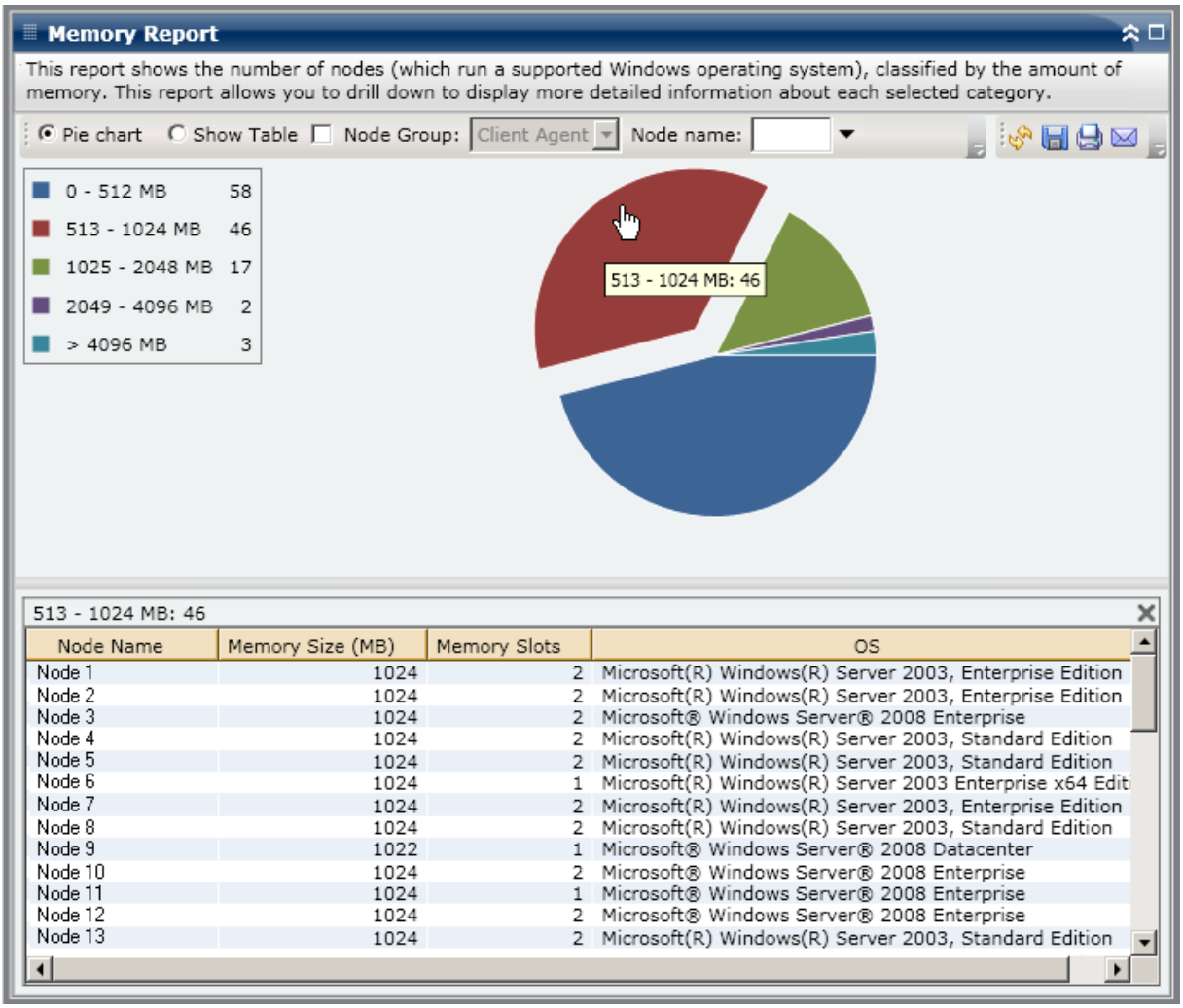
Show Table

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 62).

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.



Network Report

The Network 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 Network 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.

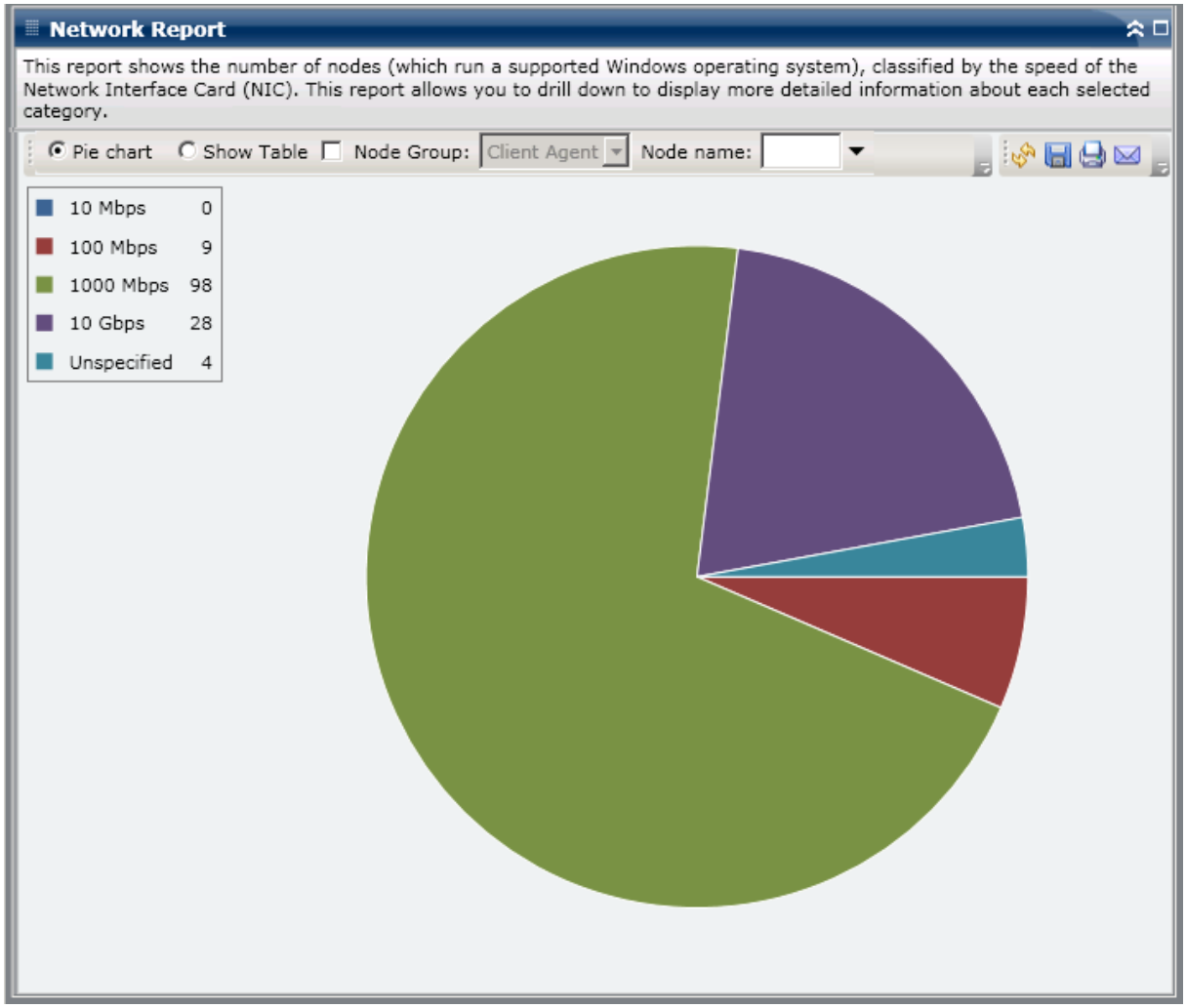
Report View

The Network Report can be displayed as either a pie chart or as a table. This report contains filters for Node Group, Node Name, and Node Tier.

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 network information for all nodes. The data is populated into the pre-configured categories.



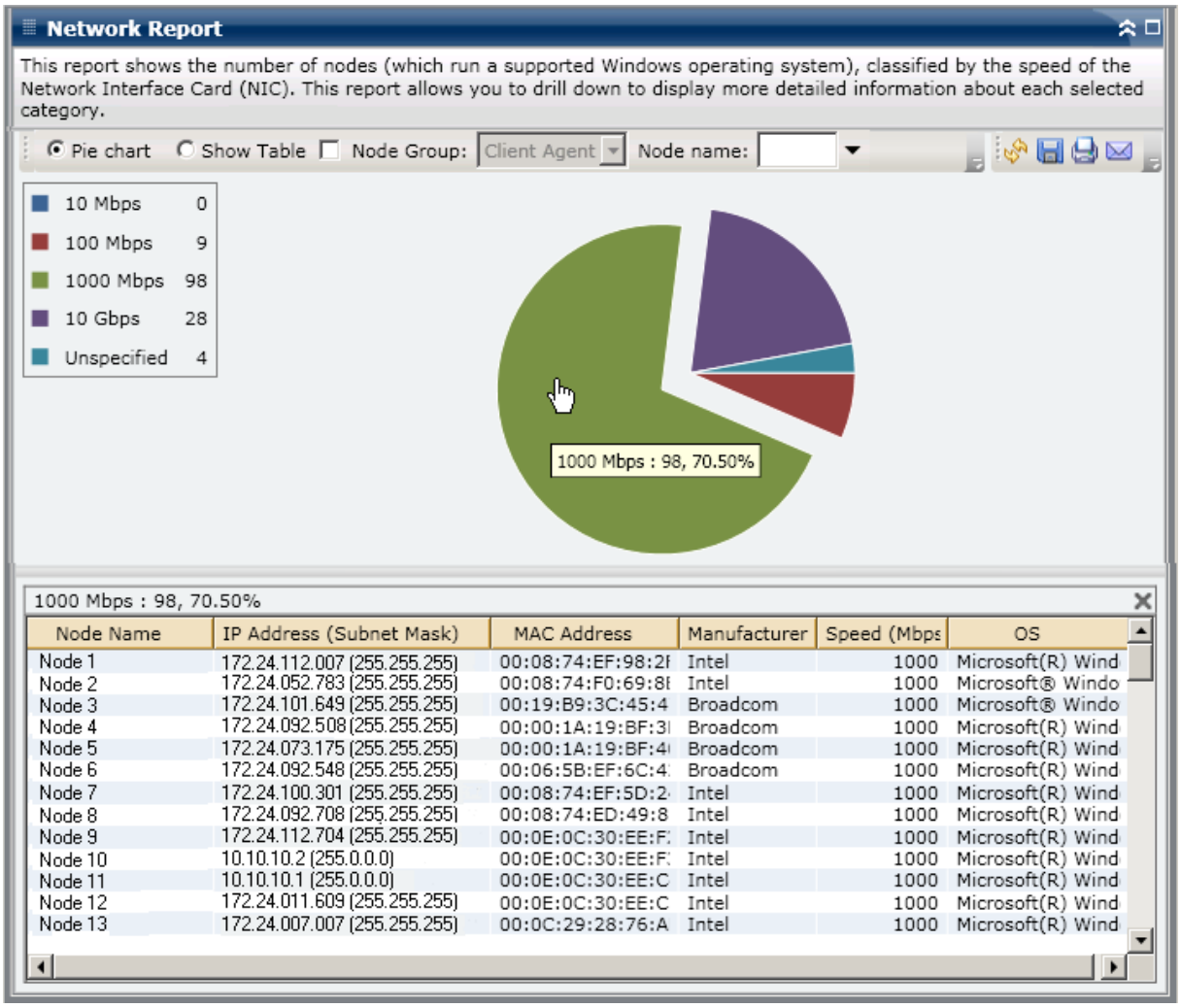
Show Table

If you select Show Table, the Network 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 62).

Drill Down Reports

The Network 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 Archive Status Report

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

Report Benefits

The Node Archive Status Report is helpful in analyzing and determining which nodes are more effective than others for archive 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 archive jobs from a node perspective. If the status from the previous day is all green (successful), you know that the corresponding node had a good archive. However, if the 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.

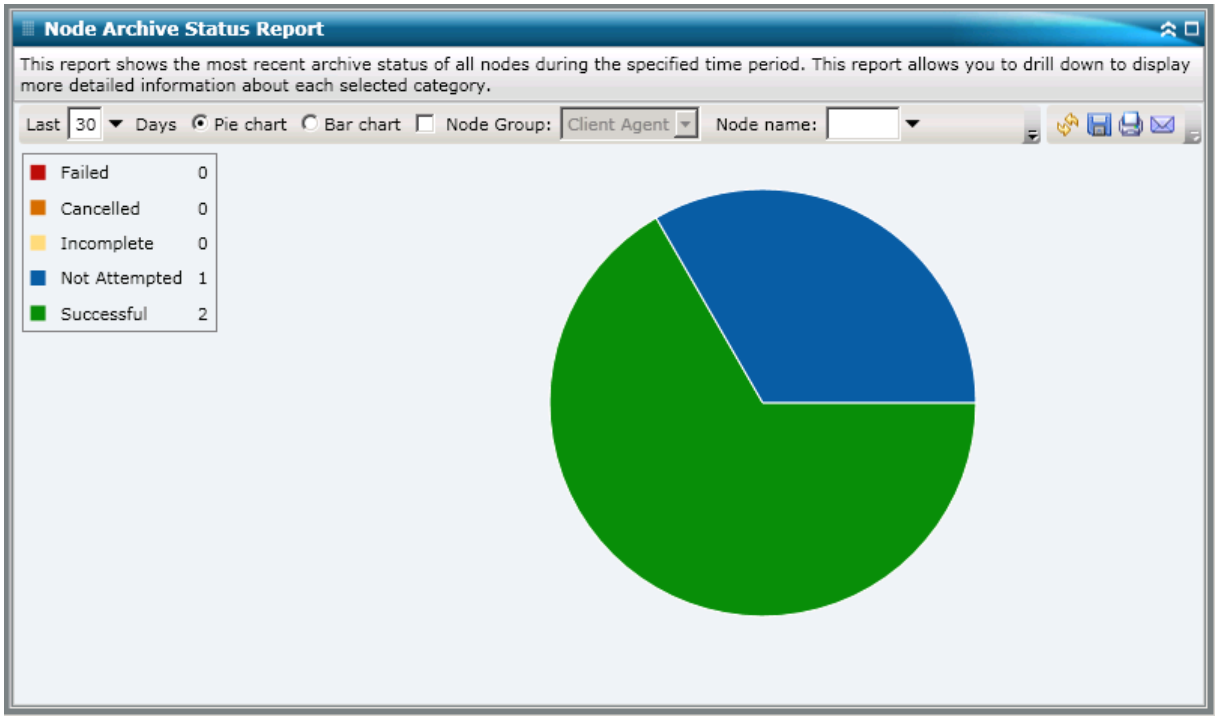
Report View

The Node Archive Status Report can be displayed as either a pie chart or as a bar chart. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

Note: By default, Arcserve Backup only retains Activity Log information for 14 days. If you want 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

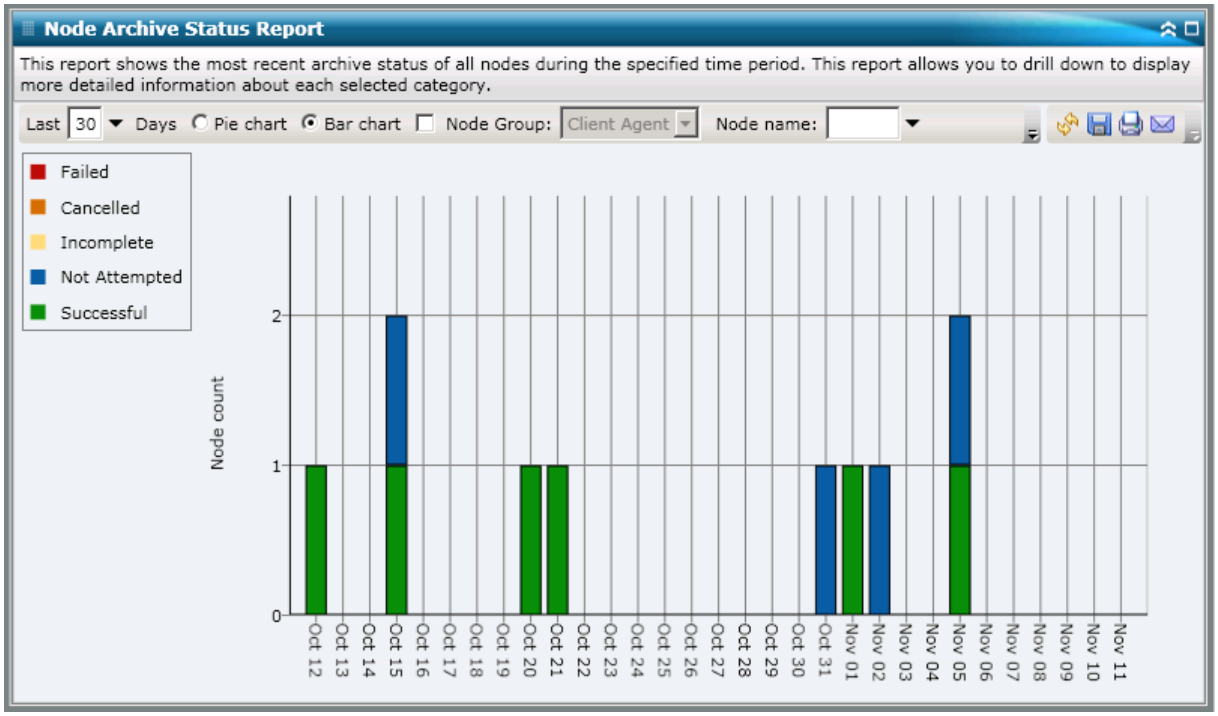
The pie chart provides a high-level overview of nodes that were archived for **all days** of the specified time period. The status categories shown in the pie chart represent a percentage of the **total number** of nodes that were archived during the last specified number of days, with the most recent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



Bar Chart

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

Note: By default, 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).

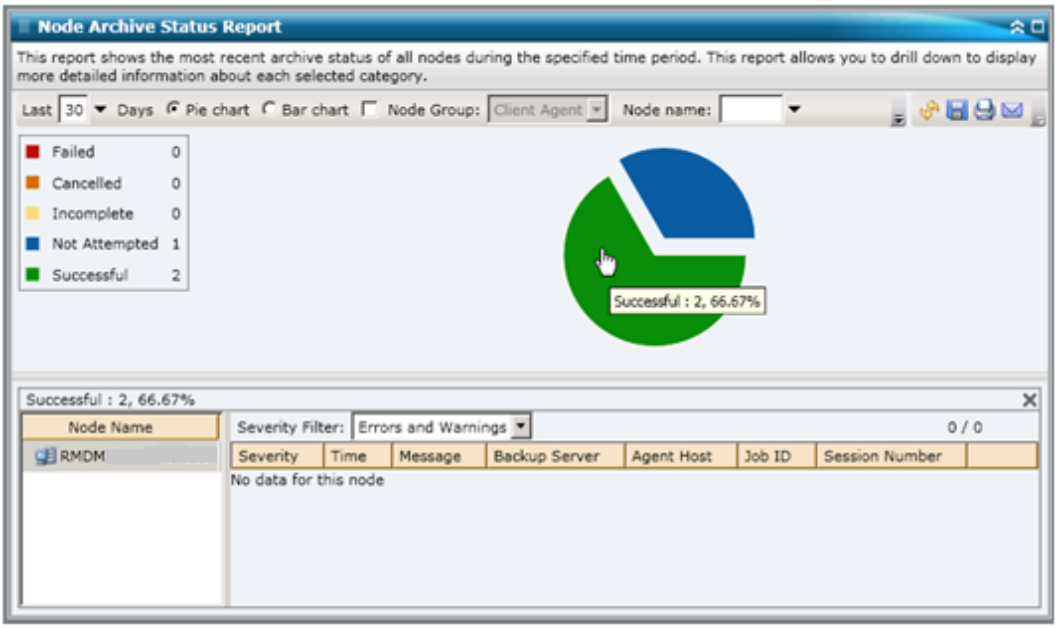


Drill Down Reports

The Node Archive 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.

Be aware of the following:

- 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.
- 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.



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 (Errors and Warnings, Errors, Warnings, Information, or All).

Be aware of the following:

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

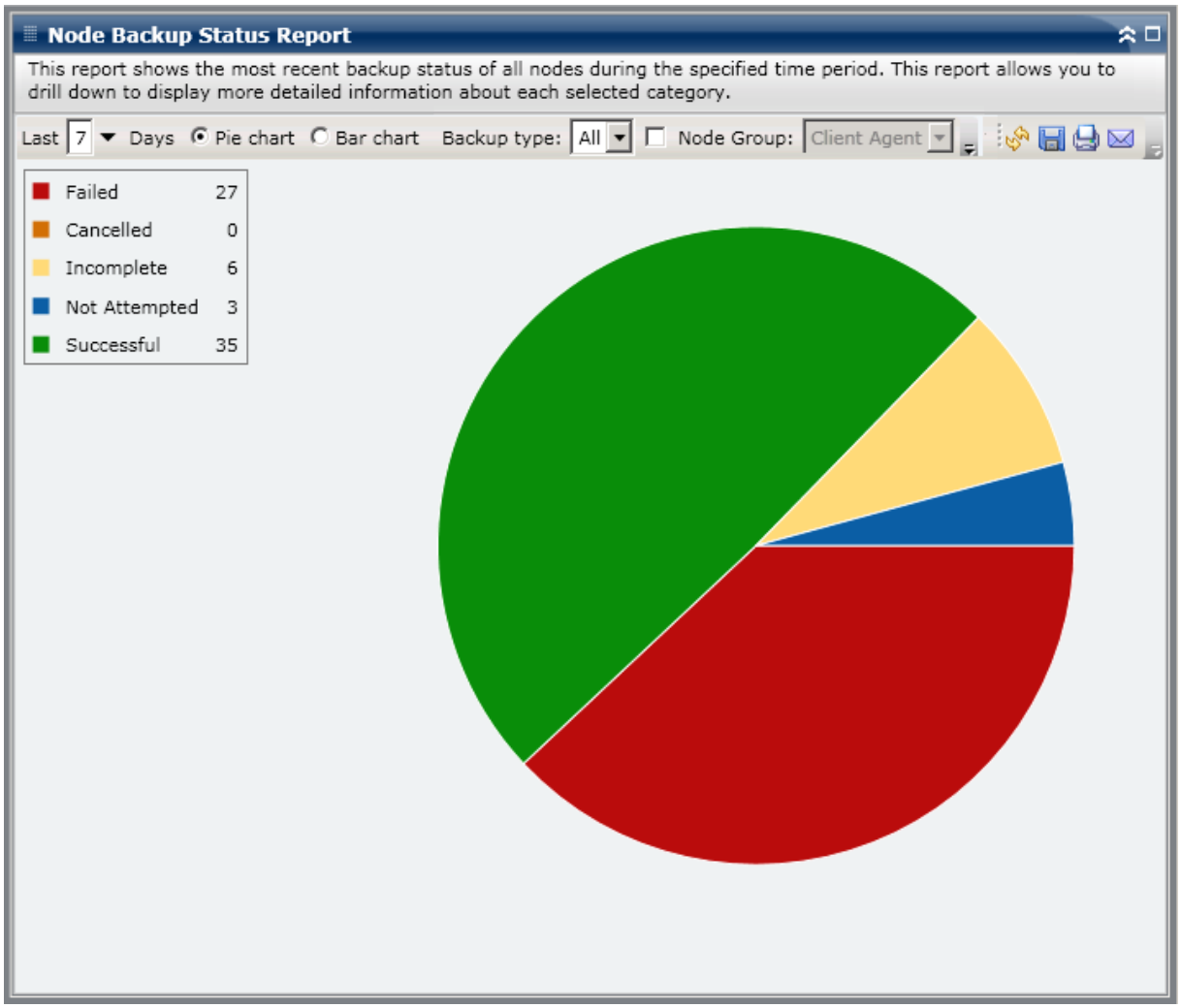
Report View

The Node Backup Status Report can be displayed as either a pie chart or as a bar chart. This report contains filters for Last # Days, Backup Type, Node Group, Node Name, and Node Tier.

Note: By default, Arcserve Backup only retains Activity Log information for 14 days. If you want 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

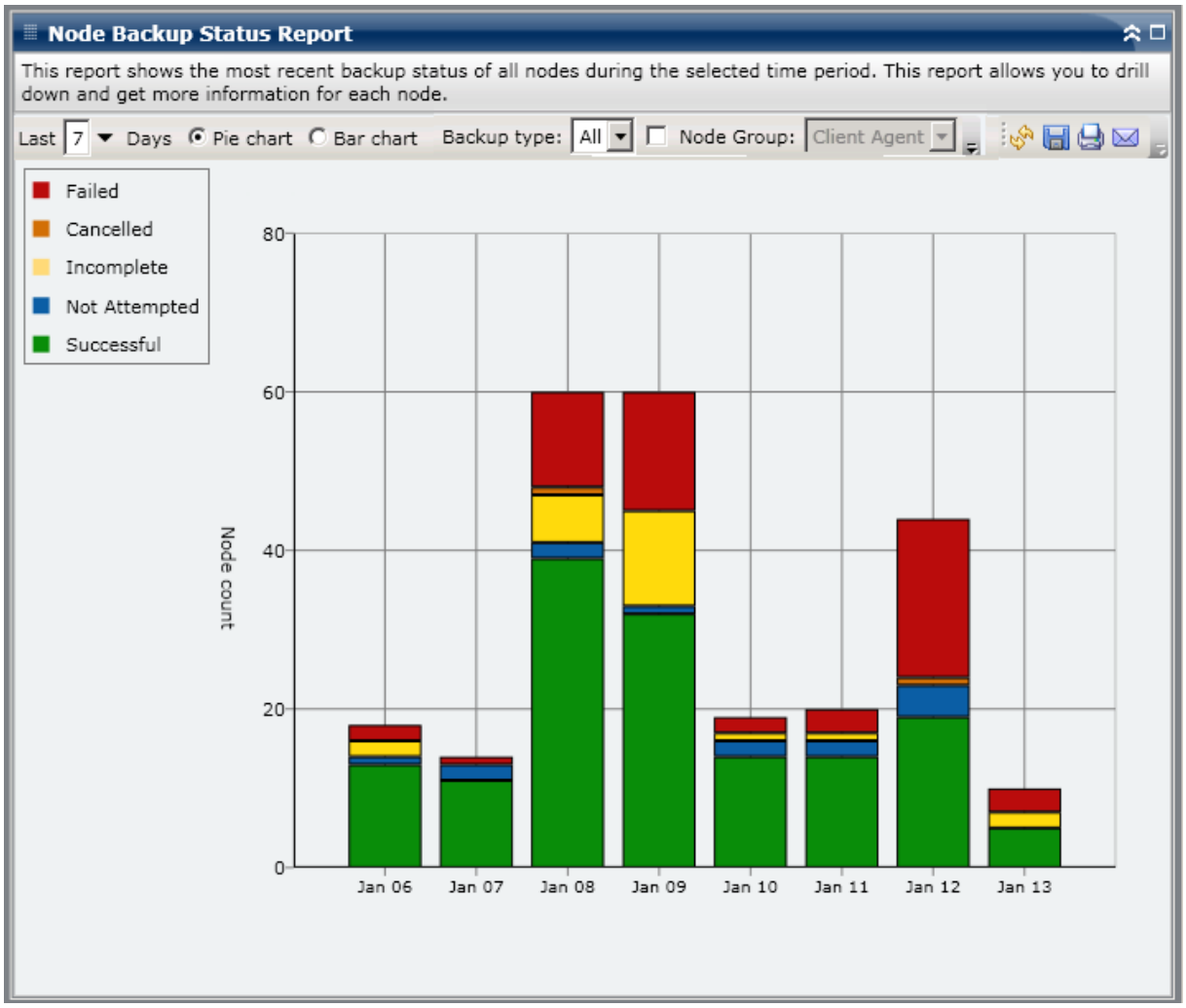
The pie chart provides a high-level overview of nodes that were backed up for all days of the specified time period. The status categories shown in the pie chart represent a percentage of the total number of nodes that were backed up during the last specified number of days, with the most recent backup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

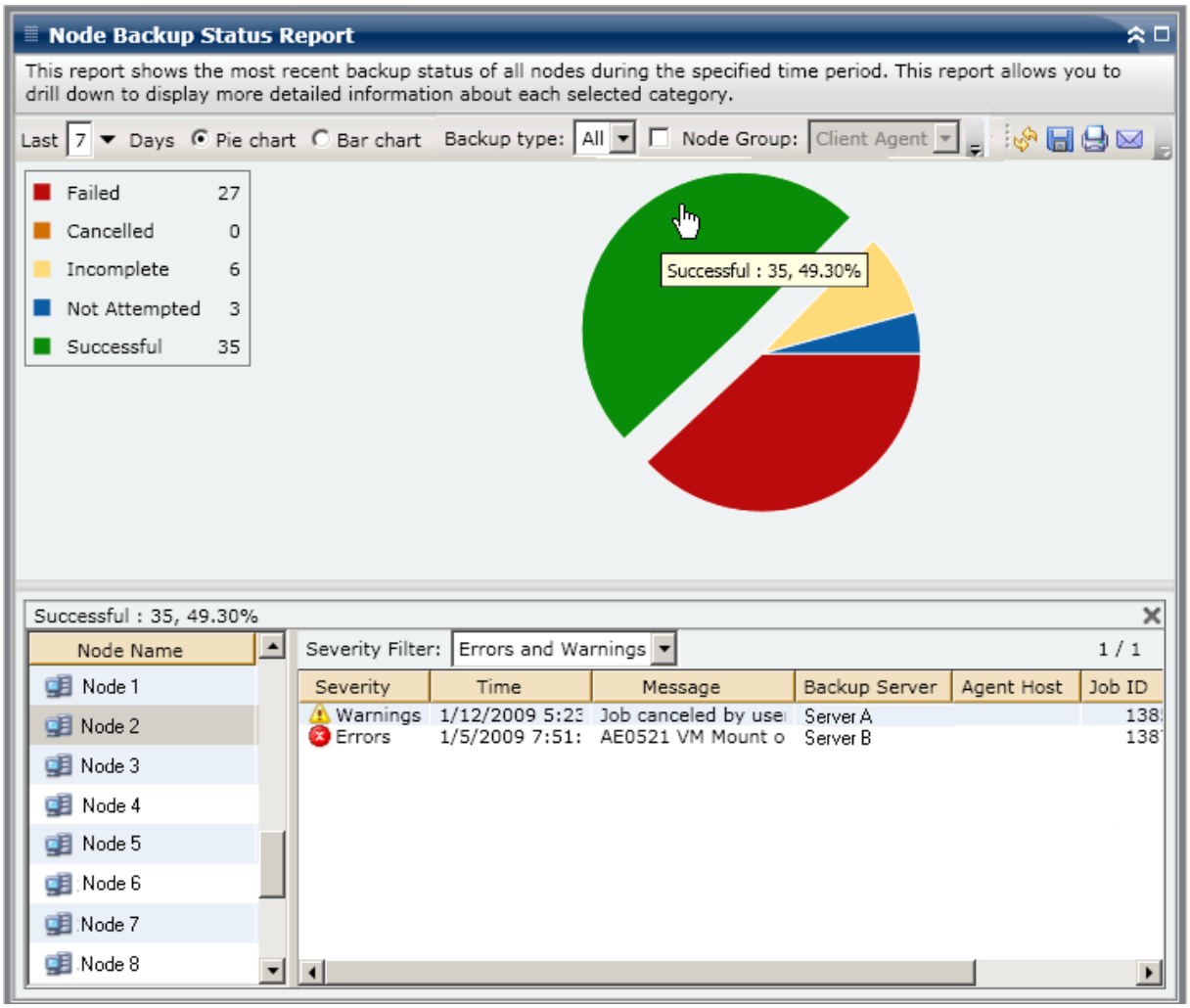


Drill Down Reports

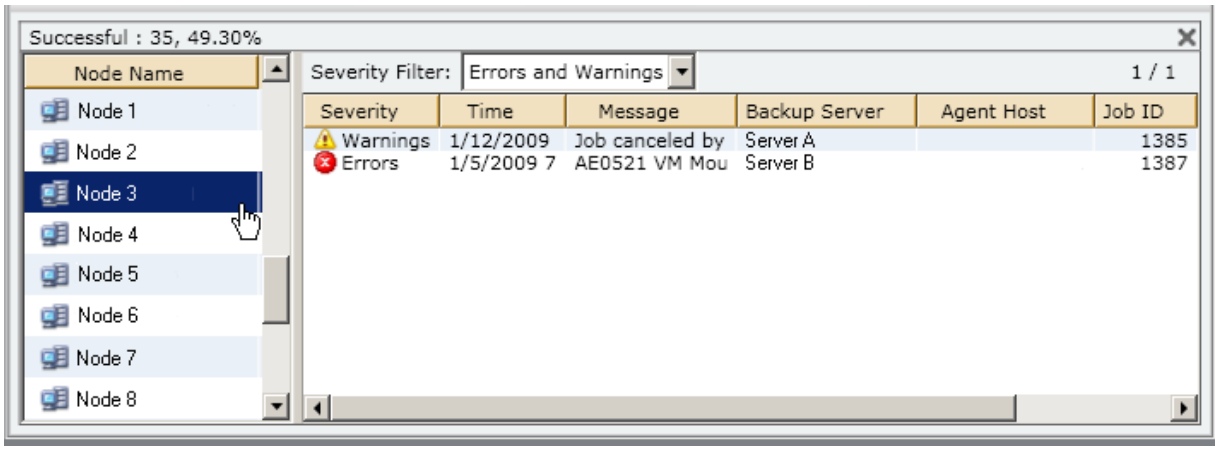
The Node Backup Status Report can be further expanded from the Pie chart view to display more detailed information. You can click on any status category (from either the pie chart view or the bar chart view) to drill down from a report of summary information to a more focused and detailed report about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

Be aware of the following:

- 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.
- 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 62).



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).



Be aware of the following:

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

- Arcserve Backup Disaster Recovery Option
- 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 Arcserve Backup Disaster Recovery Option installed, a warning message is displayed at the top of this report, informing you of this potentially dangerous condition.

Report Benefits

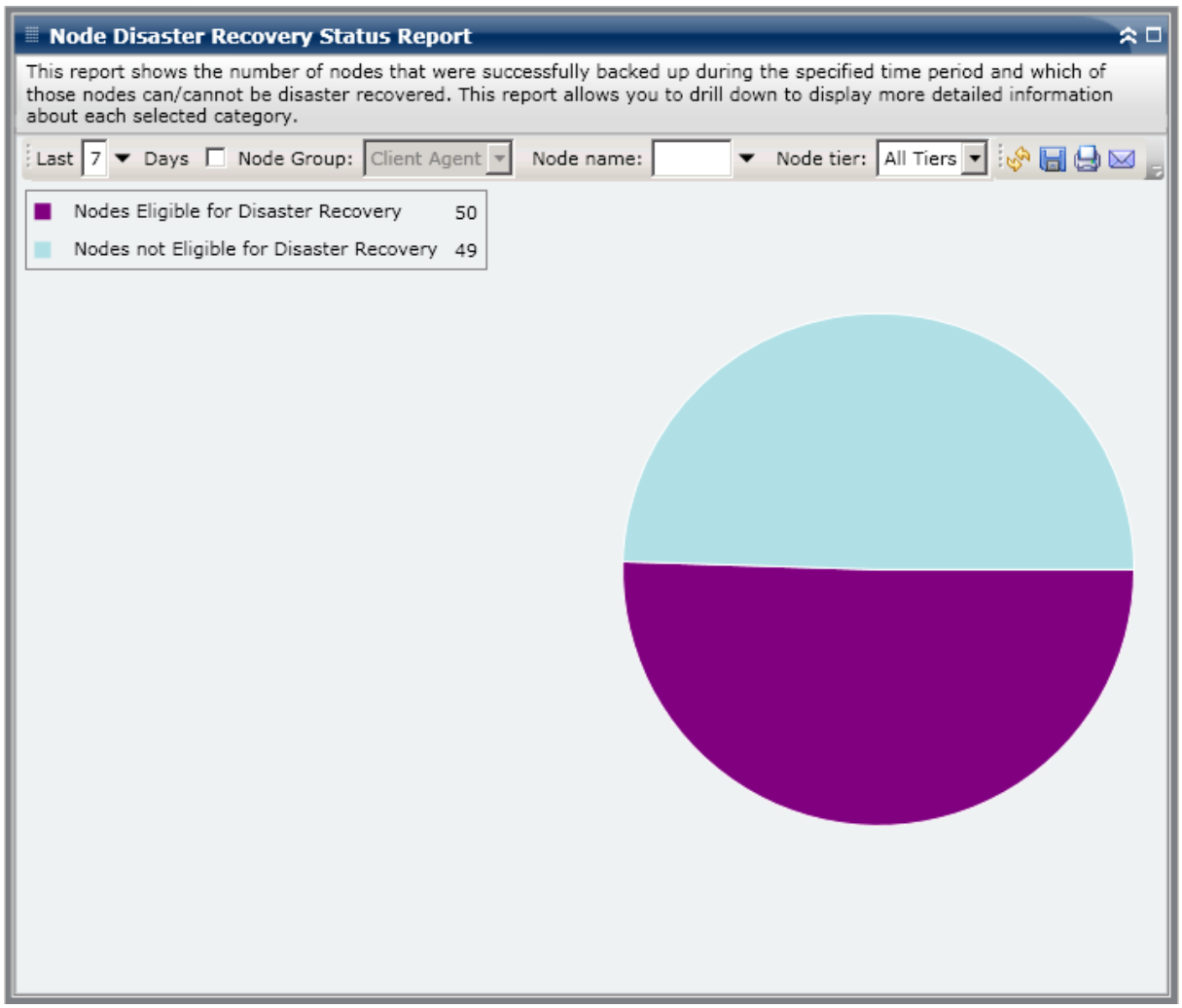
The Nodes Disaster Recovery Status Report is helpful in analyzing and determining which nodes are adequately protected for disaster recovery, and which ones could be potential problem areas.

For example, if this report shows 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 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. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

- 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.

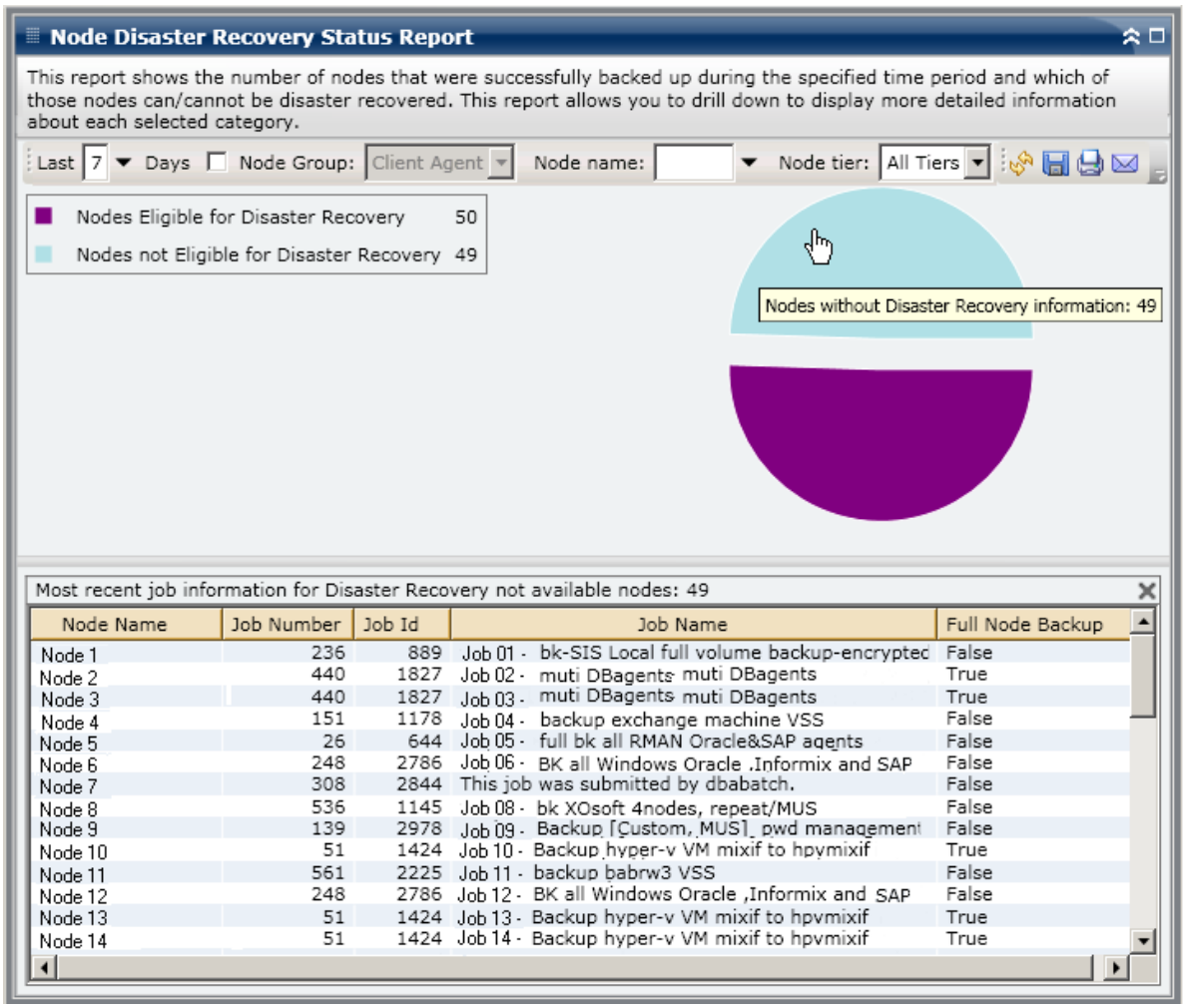


Drill Down Reports

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 62).

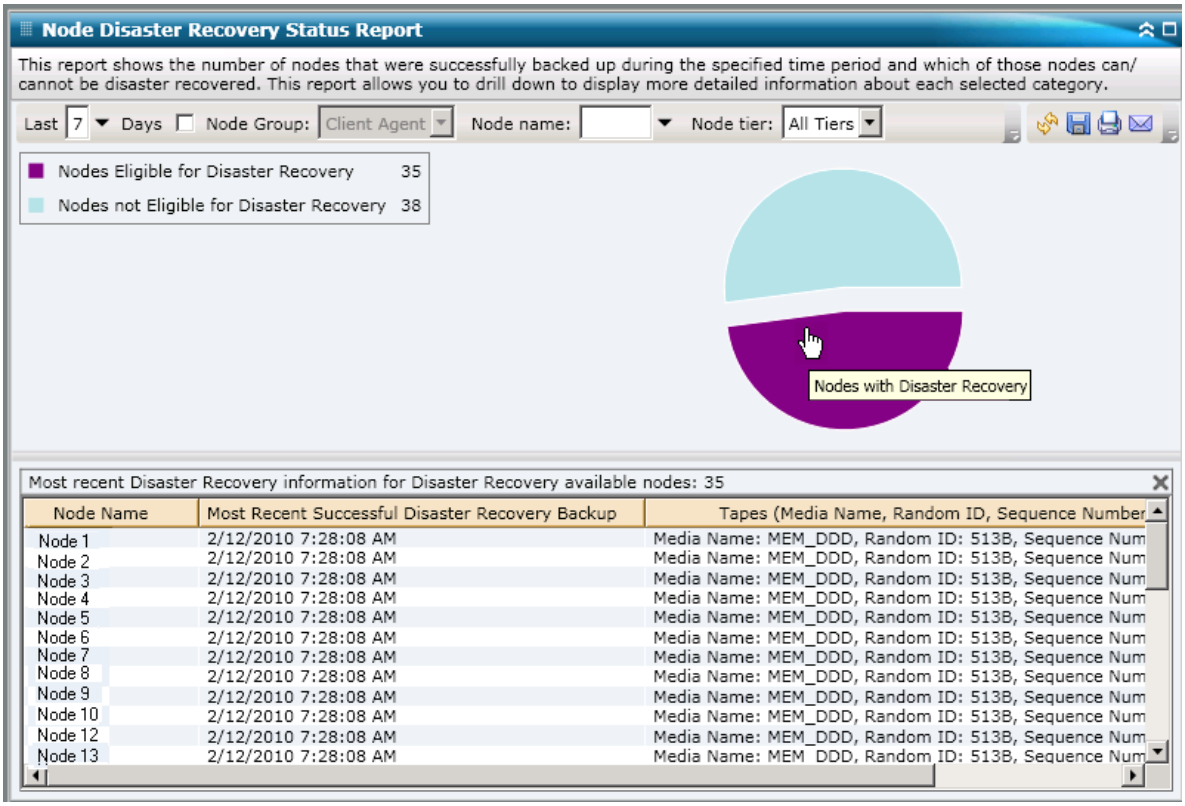
- If you drill down in the Nodes Not Eligible for Disaster Recovery category the corresponding table also displays the job number for the most recent backup job for that node, the Job name, and whether or not the most recent backup job was a Full backup.



Node Name	Job Number	Job Id	Job Name	Full Node Backup
Node 1	236	889	Job 01 - bk-SIS Local full volume backup-encrypted	False
Node 2	440	1827	Job 02 - muti DBagents muti DBagents	True
Node 3	440	1827	Job 03 - muti DBagents muti DBagents	True
Node 4	151	1178	Job 04 - backup exchange machine VSS	False
Node 5	26	644	Job 05 - full bk all RMAN Oracle&SAP agents	False
Node 6	248	2786	Job 06 - BK all Windows Oracle ,Informix and SAP	False
Node 7	308	2844	This job was submitted by dbabatch.	False
Node 8	536	1145	Job 08 - bk XOsoft 4nodes, repeat/MUS	False
Node 9	139	2978	Job 09 - Backup [Custom, MUS]_ pwd management	False
Node 10	51	1424	Job 10 - Backup hyper-v VM mixif to hpvmixif	True
Node 11	561	2225	Job 11 - backup babrw3 VSS	False
Node 12	248	2786	Job 12 - BK all Windows Oracle ,Informix and SAP	False
Node 13	51	1424	Job 13 - Backup hyper-v VM mixif to hpvmixif	True
Node 14	51	1424	Job 14 - Backup hyper-v VM mixif to hpvmixif	True

- If you drill 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 Arcserve Backup or replicated by Arcserve Replication and High Availability)

  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 (High Priority, Medium Priority, and Low Priority). 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, this report can show if you have any High Priority nodes that are not encrypted. If you have non-encrypted High Priority 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 this report shows that you have Low Priority 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.

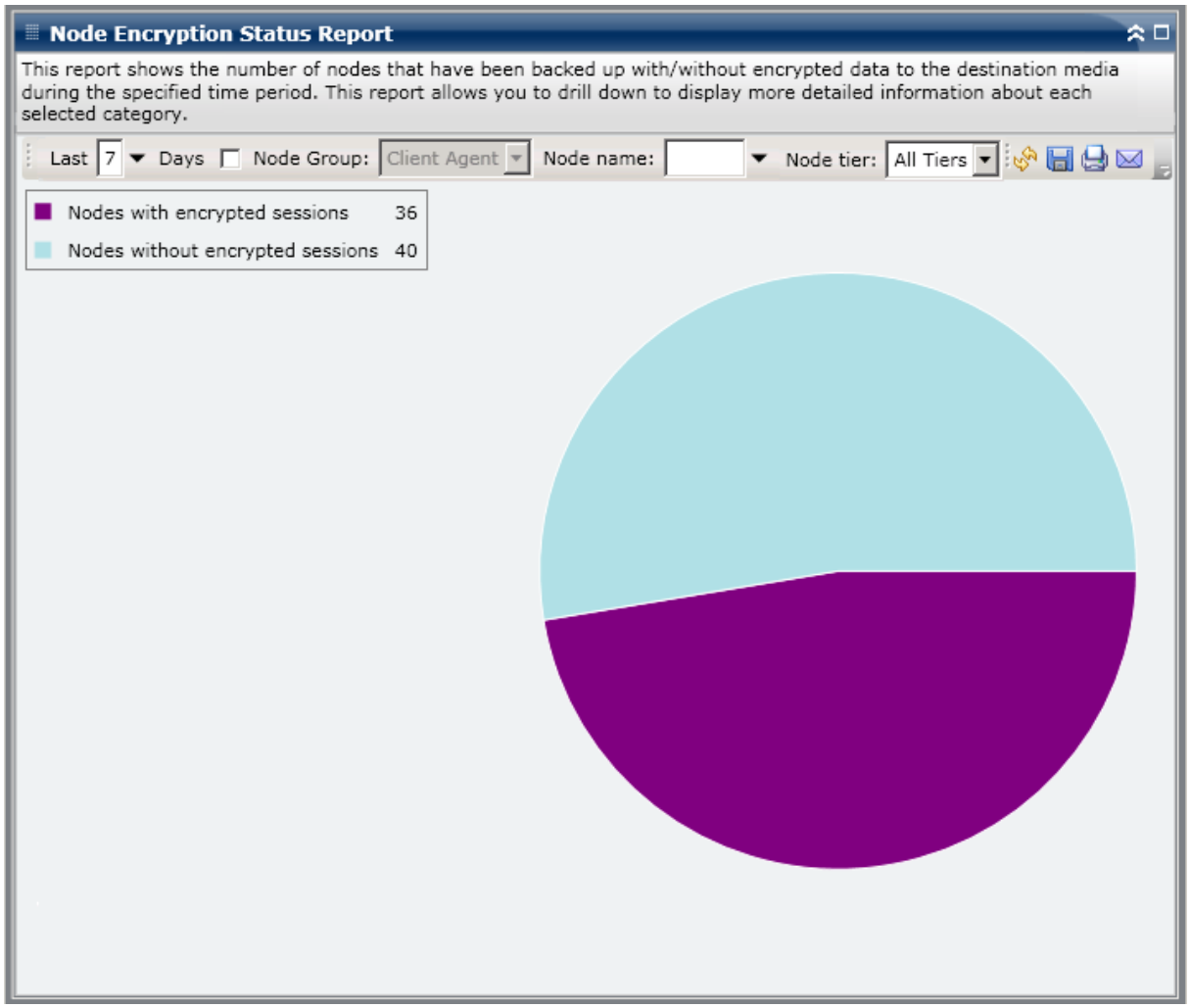
In addition, you can also see if all data on a specific node has been encrypted to ensure both proper security and use of resources.

> 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 (High Priority, Medium Priority, and Low Priority). This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

- 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.



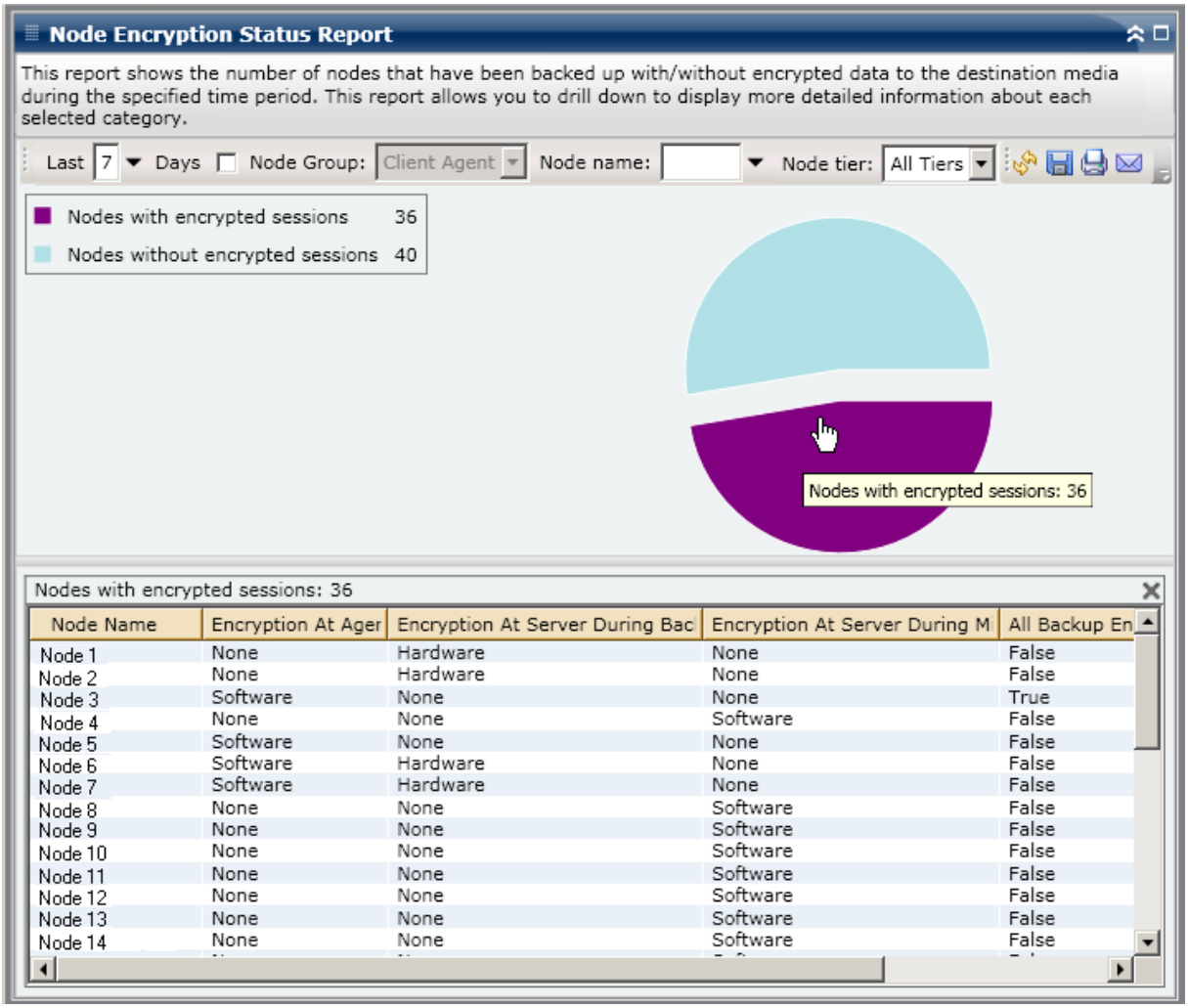
Drill Down Reports

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.

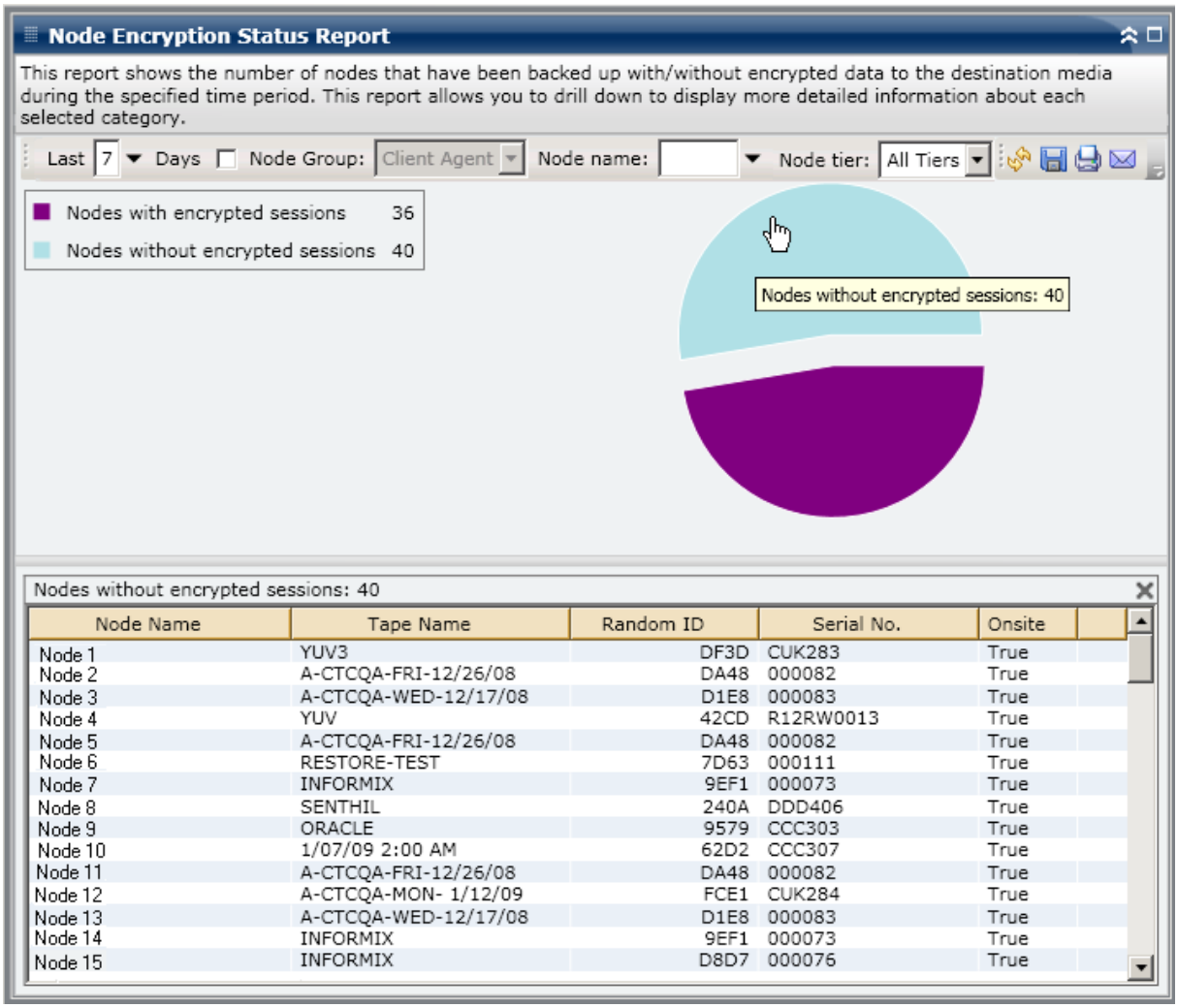
Note: You can select the node name and right-click the mouse button to display a pop-up window with all related node information for the selected node. For more information, see Node Information (see page 62).

- 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 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 Arcserve Backup Database.

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



- 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 Name	Tape Name	Random ID	Serial No.	Onsite
Node 1	YUV3	DF3D	CUK283	True
Node 2	A-CTCQA-FRI-12/26/08	DA48	000082	True
Node 3	A-CTCQA-WED-12/17/08	D1E8	000083	True
Node 4	YUV	42CD	R12RW0013	True
Node 5	A-CTCQA-FRI-12/26/08	DA48	000082	True
Node 6	RESTORE-TEST	7D63	000111	True
Node 7	INFORMIX	9EF1	000073	True
Node 8	SENTHIL	240A	DDD406	True
Node 9	ORACLE	9579	CCC303	True
Node 10	1/07/09 2:00 AM	62D2	CCC307	True
Node 11	A-CTCQA-FRI-12/26/08	DA48	000082	True
Node 12	A-CTCQA-MON- 1/12/09	FCE1	CUK284	True
Node 13	A-CTCQA-WED-12/17/08	D1E8	000083	True
Node 14	INFORMIX	9EF1	000073	True
Node 15	INFORMIX	D8D7	000076	True

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, 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, 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. This report contains filters for Last # Days, # of Recovery Points, Node Group, Node Name, and Node Tier.

The availability of Disaster Recovery is based upon whether or not the 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 Arcserve Backup Disaster Recovery Option, you can use the Node Disaster Recovery Status Report (see page 160).

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 62).

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 7 Days Recovery Points < 5 Node Group: Client Agent

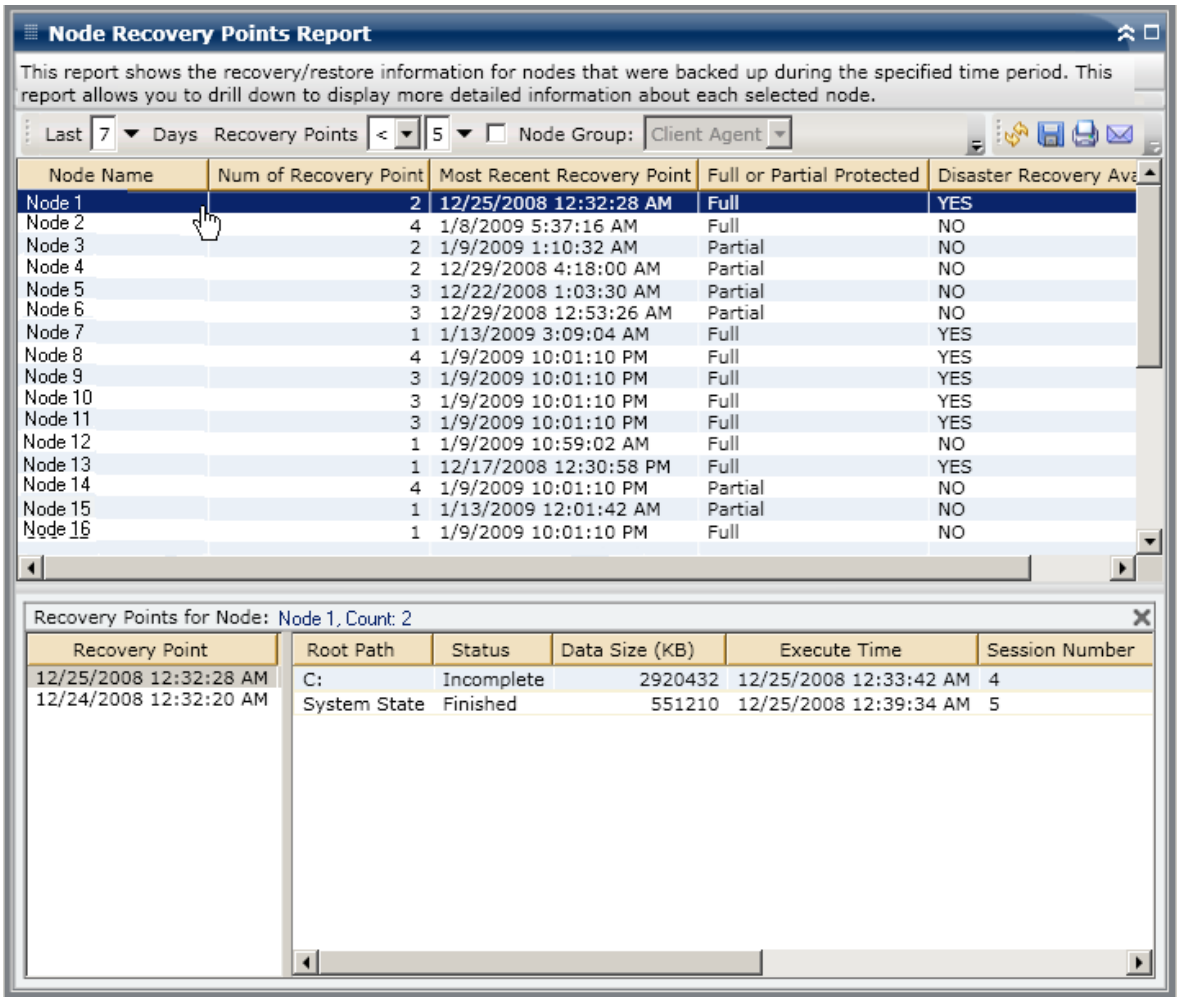
Node Name	Num of Recovery Point	Most Recent Recovery Point	Full or Partial Protected	Disaster Recovery Availa
Node 1	2	12/25/2008 12:32:28 AM	Full	YES
Node 2	4	1/8/2009 5:37:16 AM	Full	NO
Node 3	2	1/9/2009 1:10:32 AM	Partial	NO
Node 4	2	12/29/2008 4:18:00 AM	Partial	NO
Node 5	3	12/22/2008 1:03:30 AM	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 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. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

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 62).

Node Summary Report

This report shows overview information about all nodes (which run a supported Windows operating system) in your backup environment.

Last 7 Days Node Group: Client Agent Node name: Node tier: All Tiers

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) \
Node 2	1	2656	1	2	1024	1	Microsoft(R) \
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) \
Node 6	2	2392	1	3	1024	3	Microsoft(R) \
Node 7	1	2657	1	2	1024	1	Microsoft(R) \
Node 8	1	2259	1	1	512	1	Microsoft(R) \
Node 9	1	1396	4	4	2048	2	Microsoft(R) \
Node 10	1	1396	4	1	2048	2	Microsoft(R) \
Node 11	1	2126	1	1	1024	1	Microsoft(R) \
Node 12	1	2127	1	1	512	1	Microsoft(R) \
Node 13	1	2258	1	1	1024	1	Microsoft(R) \
Node 14	1	996	1	1	512	1	Microsoft(R) \
Node 15	1	2793	1	3	1024	1	Microsoft(R) \
Node 16	1	2660	2	2	511	1	Microsoft(R) \
Node 17	1	2660	1	1	511	1	Microsoft(R) \
Node 18	1	2660	1	1	511	1	Microsoft(R) \
Node 19	1	1994	1	1	511	1	Microsoft(R) \
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) \
Node 23	1	1396	1	2	2048	1	Microsoft(R) \
Node 24	1	2328	2	2	8192	2	Microsoft(R) \
Node 25	1	1995	1	1	511	1	Microsoft(R) \
Node 26	1	1995	7	3	1022	1	Microsoft® W
Node 27	2	2793	1	1	2048	1	Microsoft(R) \
Node 28	1	2793	6	2	2048	1	Microsoft(R) \
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) \
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 in three tier categories: High Priority, Medium Priority, and Low Priority. By default, the High Priority tier is automatically configured to include all Arcserve Backup servers (Primary and Member) and any nodes with Arcserve Backup application agents installed (such as Oracle, Microsoft Exchange, Microsoft SQL Server, Microsoft Sharepoint, etc.), and the Low Priority tier is configured to include all other nodes (having file system agents). (By default, the Medium Priority tier 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 Arcserve Backup Server Admin or from the Backup Manager

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

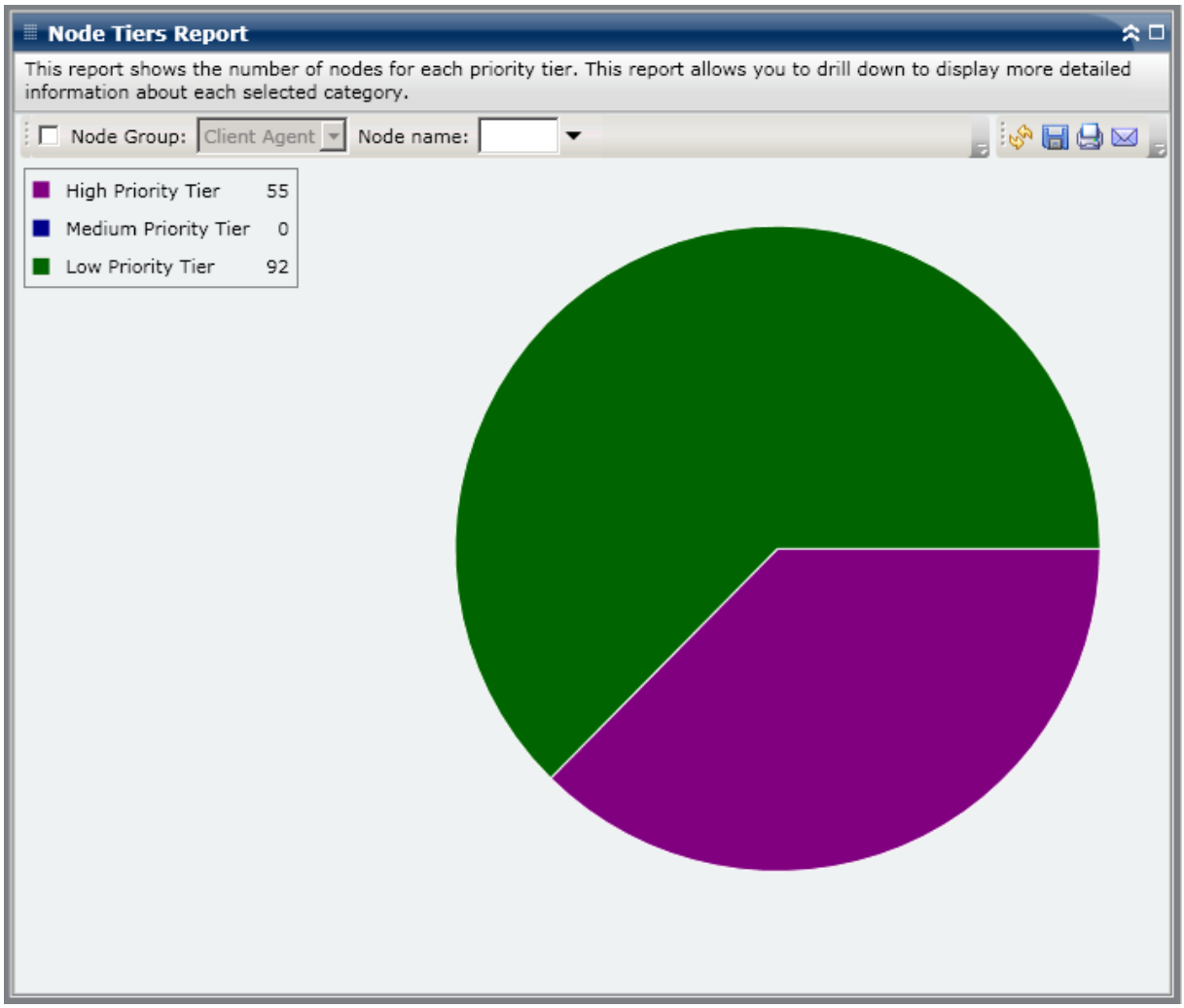
Report Benefits

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 Low Priority tier category, you should then use the Arcserve Backup Server Admin or Arcserve Backup Manager to reassign that node into the High Priority tier category.

Report View

The Node Tiers Report is displayed in a pie chart format, showing the node count for each priority tier. This report contains filters for Node Group and Node Name.



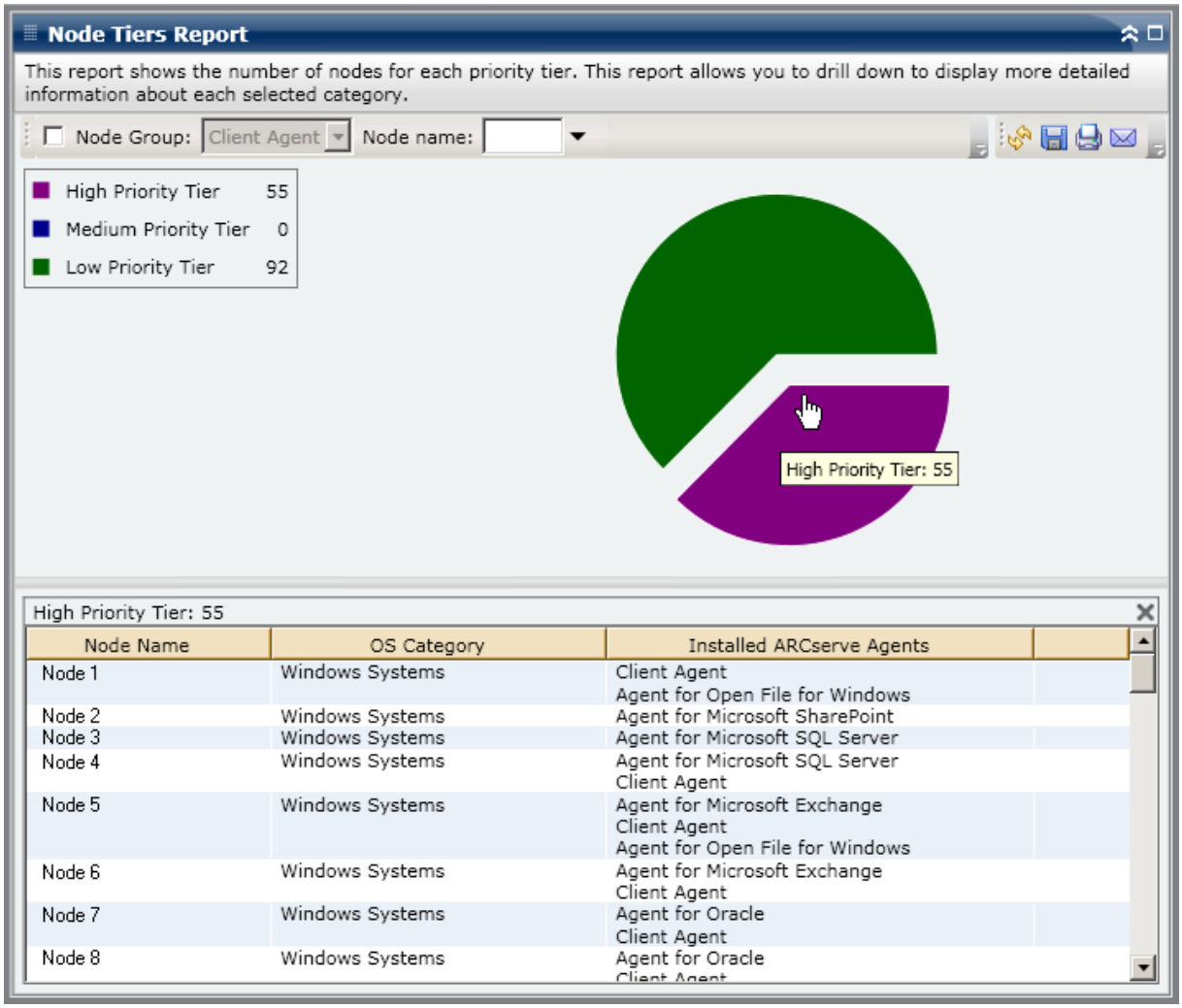
Drill Down Reports

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, Arcserve Replication and High Availability Scenarios, VMware VCB Systems, and Microsoft Hyper-V Systems.

The Installed Arcserve Agents column would include all the 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 62).



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, which indicates 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.

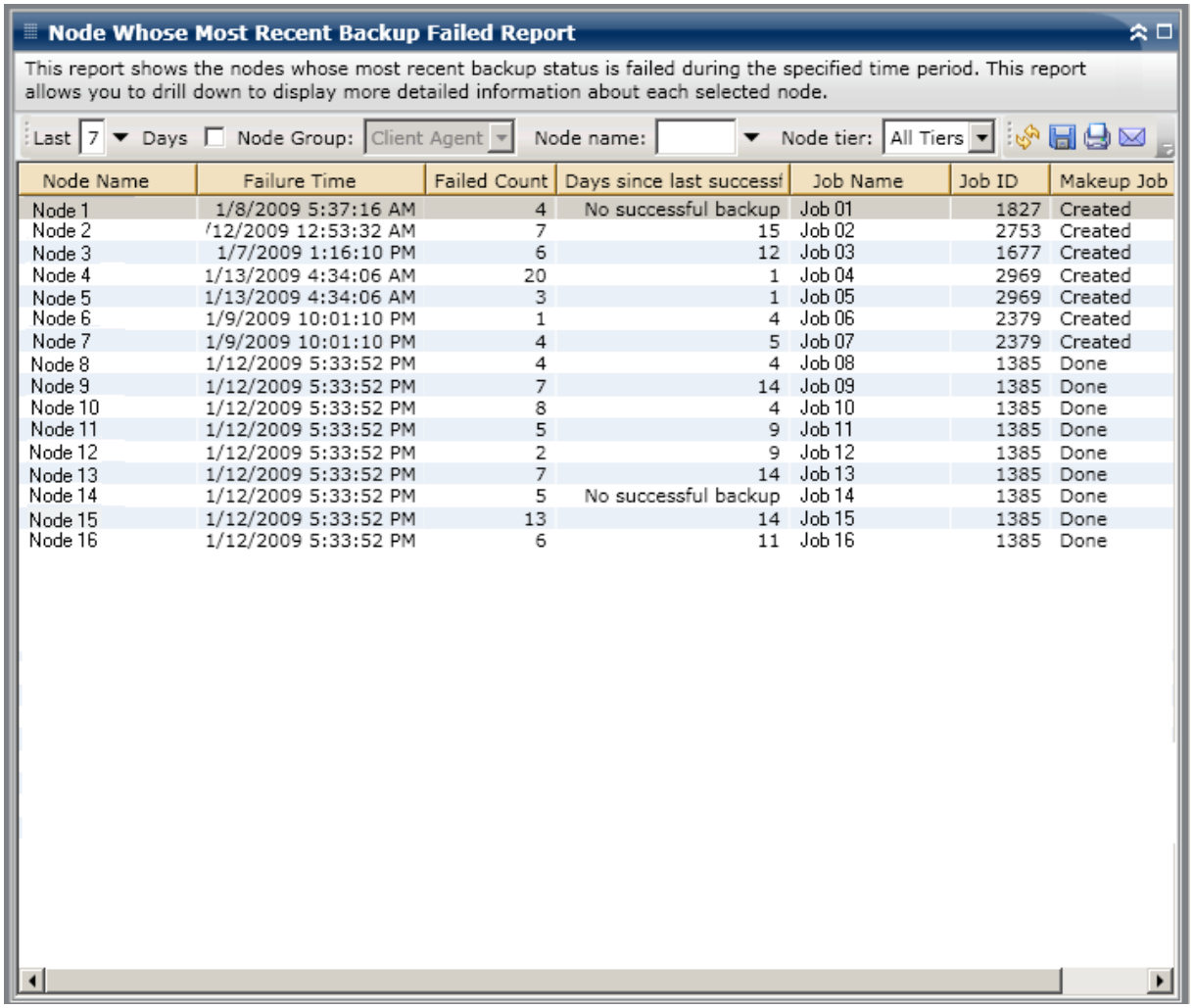
Report View

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). This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

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 62).

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 7 Days Node Group: Client Agent Node name: Node tier: All Tiers

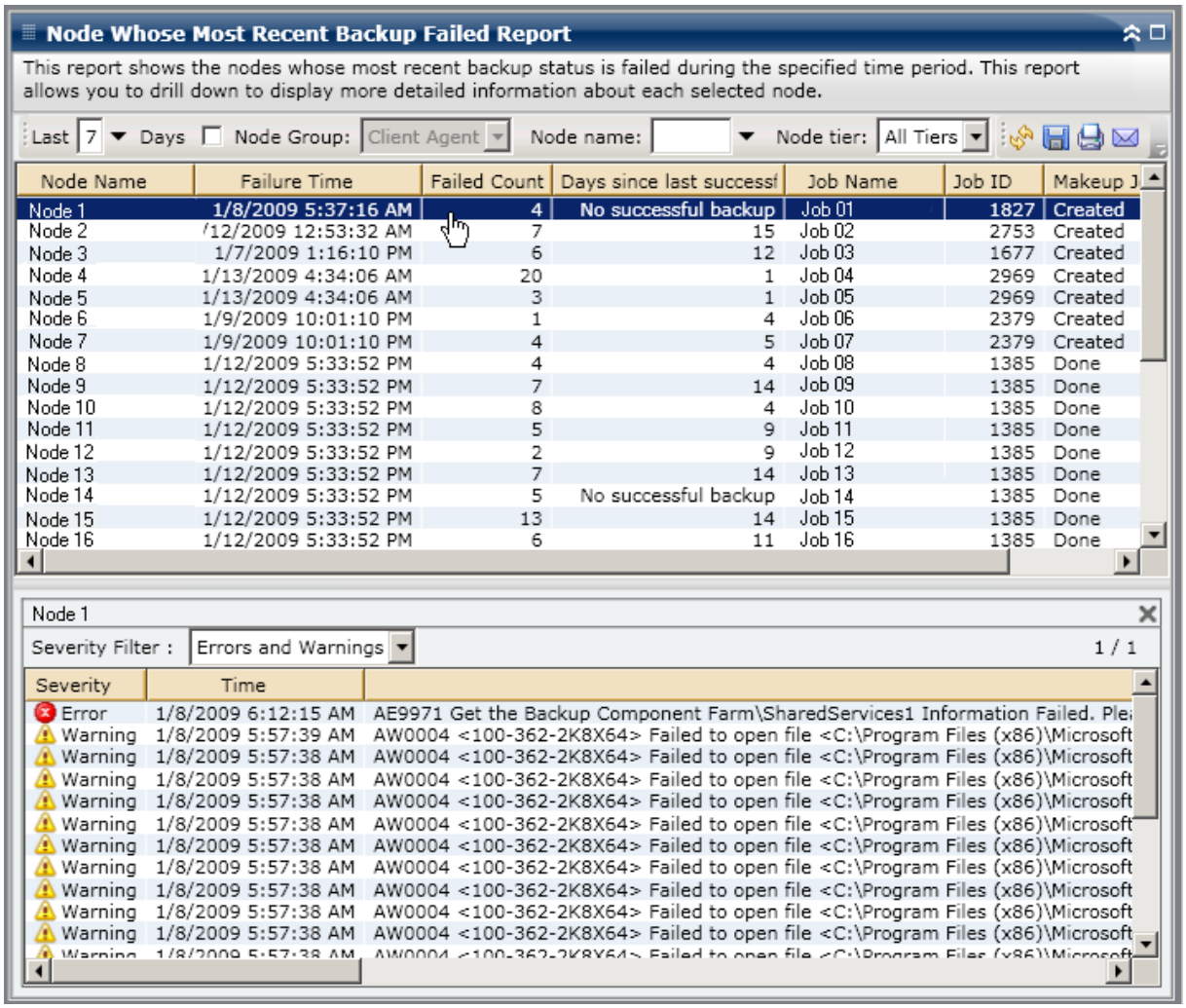
Node Name	Failure Time	Failed Count	Days since last successf	Job Name	Job ID	Makeup Job
Node 1	1/8/2009 5:37:16 AM	4	No successful backup	Job 01	1827	Created
Node 2	/12/2009 12:53:32 AM	7	15	Job 02	2753	Created
Node 3	1/7/2009 1:16:10 PM	6	12	Job 03	1677	Created
Node 4	1/13/2009 4:34:06 AM	20	1	Job 04	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.



OS Report

The OS Report is an SRM-type report that displays the supported Operating System information for all Windows nodes within your 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.

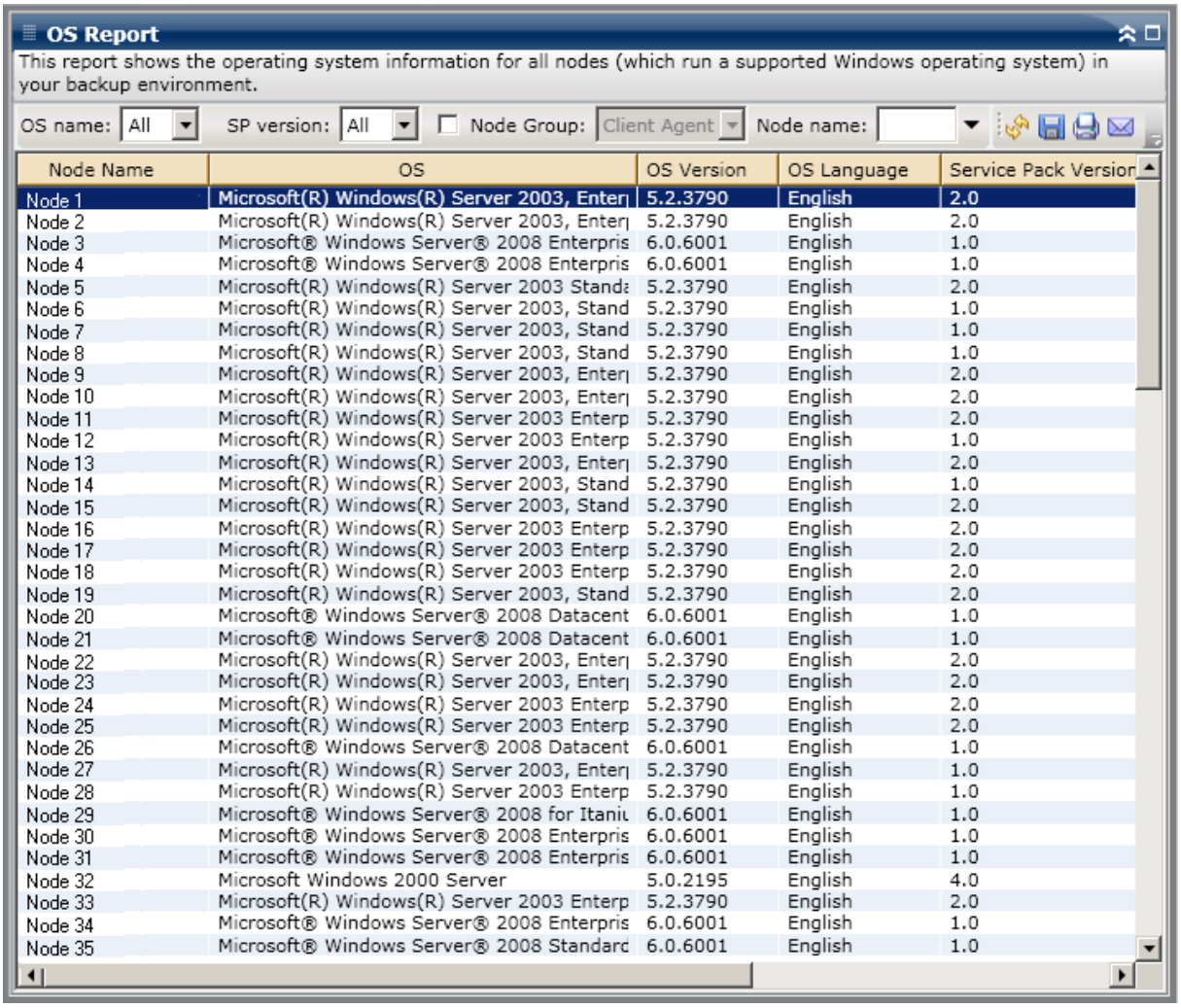
For example, you can correlate this report with the Top Nodes with Fastest/Slowest Backup Throughput Report and identify if a node has slow throughput possibly because of a recent Service Pack applied on the node's operating system. You can also use this report to identify the version and Service Pack 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. This report contains filters for OS Name, SP Version (Service Pack), Node Group, Node Name, and Node Tier.

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 62).



OS Report

This report shows the operating system information for all nodes (which run a supported Windows operating system) in your backup environment.

OS name: All SP version: All Node Group: Client Agent Node name:

Node Name	OS	OS Version	OS Language	Service Pack Version
Node 1	Microsoft(R) Windows(R) Server 2003, Enter	5.2.3790	English	2.0
Node 2	Microsoft(R) Windows(R) Server 2003, Enter	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 Standa	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, Enter	5.2.3790	English	2.0
Node 10	Microsoft(R) Windows(R) Server 2003, Enter	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, Enter	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, Enter	5.2.3790	English	2.0
Node 23	Microsoft(R) Windows(R) Server 2003, Enter	5.2.3790	English	2.0
Node 24	Microsoft(R) Windows(R) Server 2003 Enterp	5.2.3790	English	2.0
Node 25	Microsoft(R) 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, Enter	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 Standarc	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 five categories: Replicated, Disk, Cloud, 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 Arcserve Replication and High Availability and backed up using Arcserve Backup as Arcserve Replication and High Availability 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.

Cloud

Nodes that were backed up to cloud. Cloud backups can usually be recovered within a day.

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.

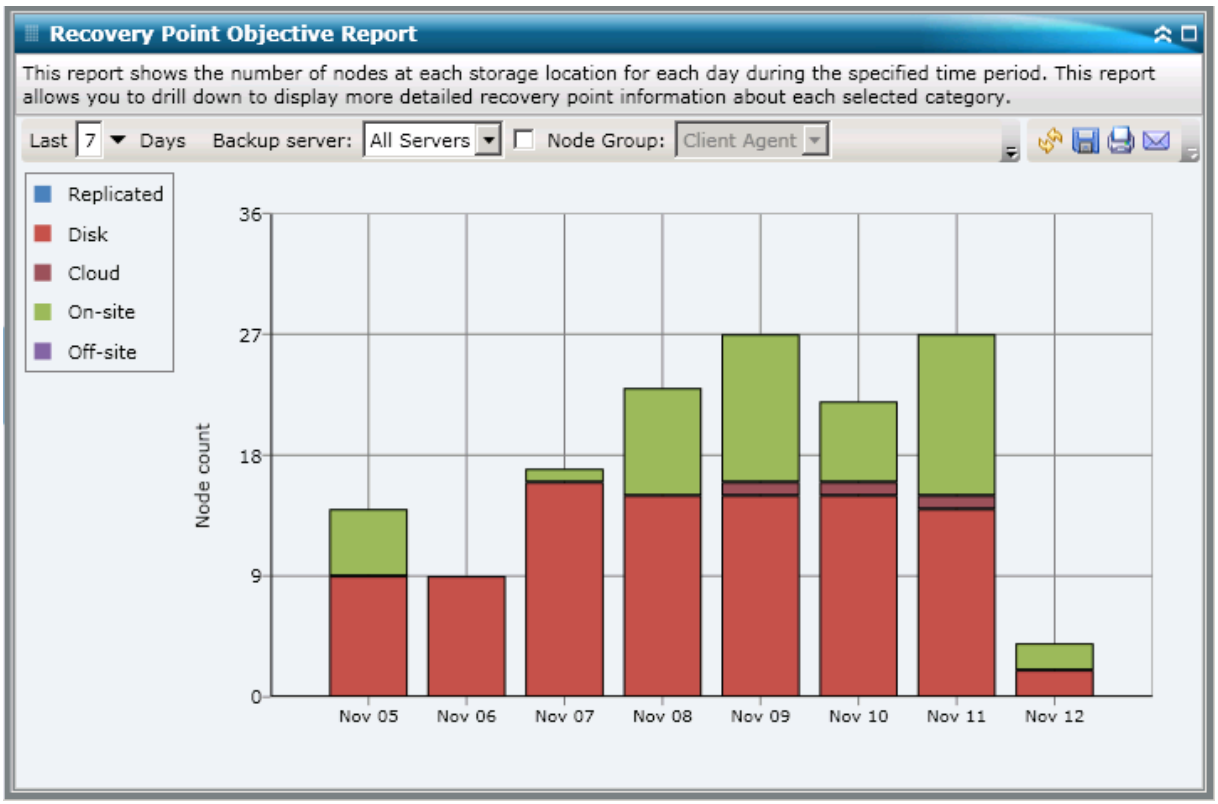
Generally you can use this report to determine how fast you can restore data and how many recovery points (backups) you have taken.

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 backup method to allow a faster recovery of the stored data) to satisfy the various requirements.

Report View

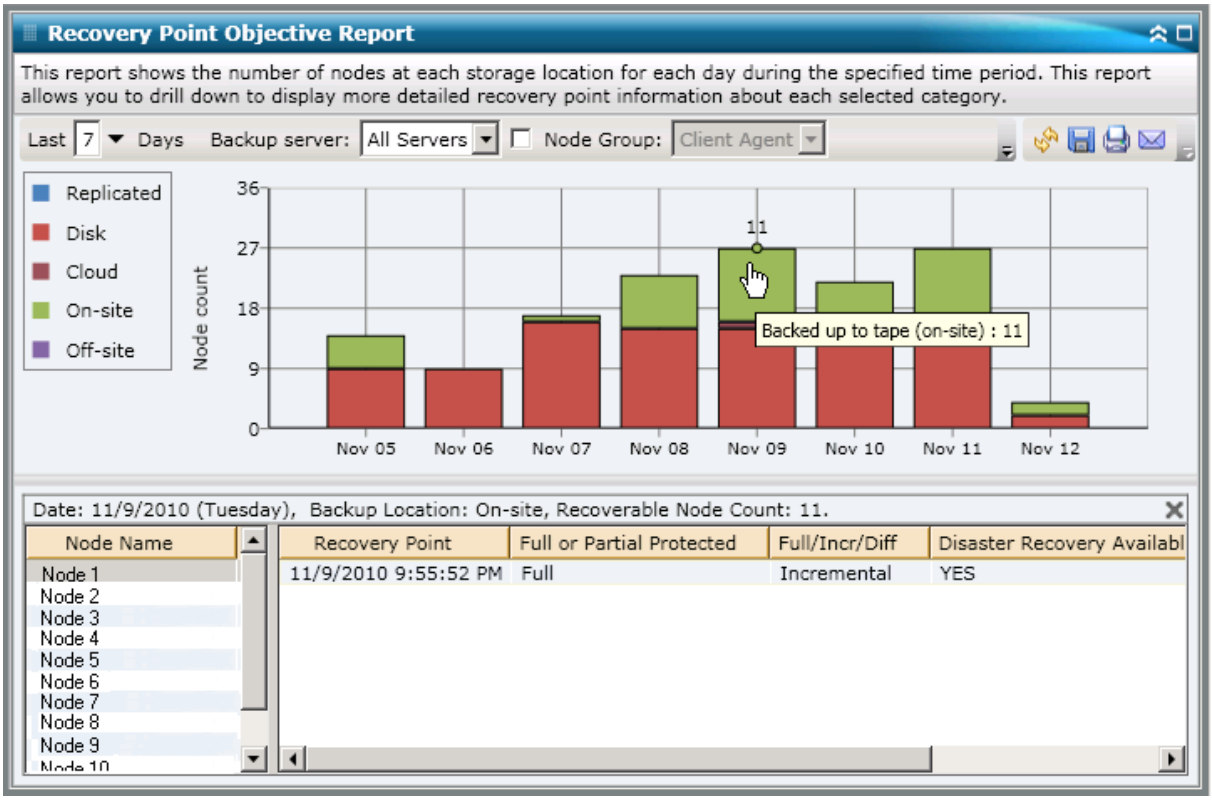
The Recovery Point Objective Report is displayed in a bar chart format, showing the number of nodes that were backed up to the various recovery point locations during the specified time period. The bar chart provides a detailed level view of the nodes that were backed up for the selected server during 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, cloud, tape on-site, and tape off-site). This report contains filters for Last # Days, Backup Server, Node Group, Node Name, and Node Tier.



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 categories 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 62).



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 this report shows 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.

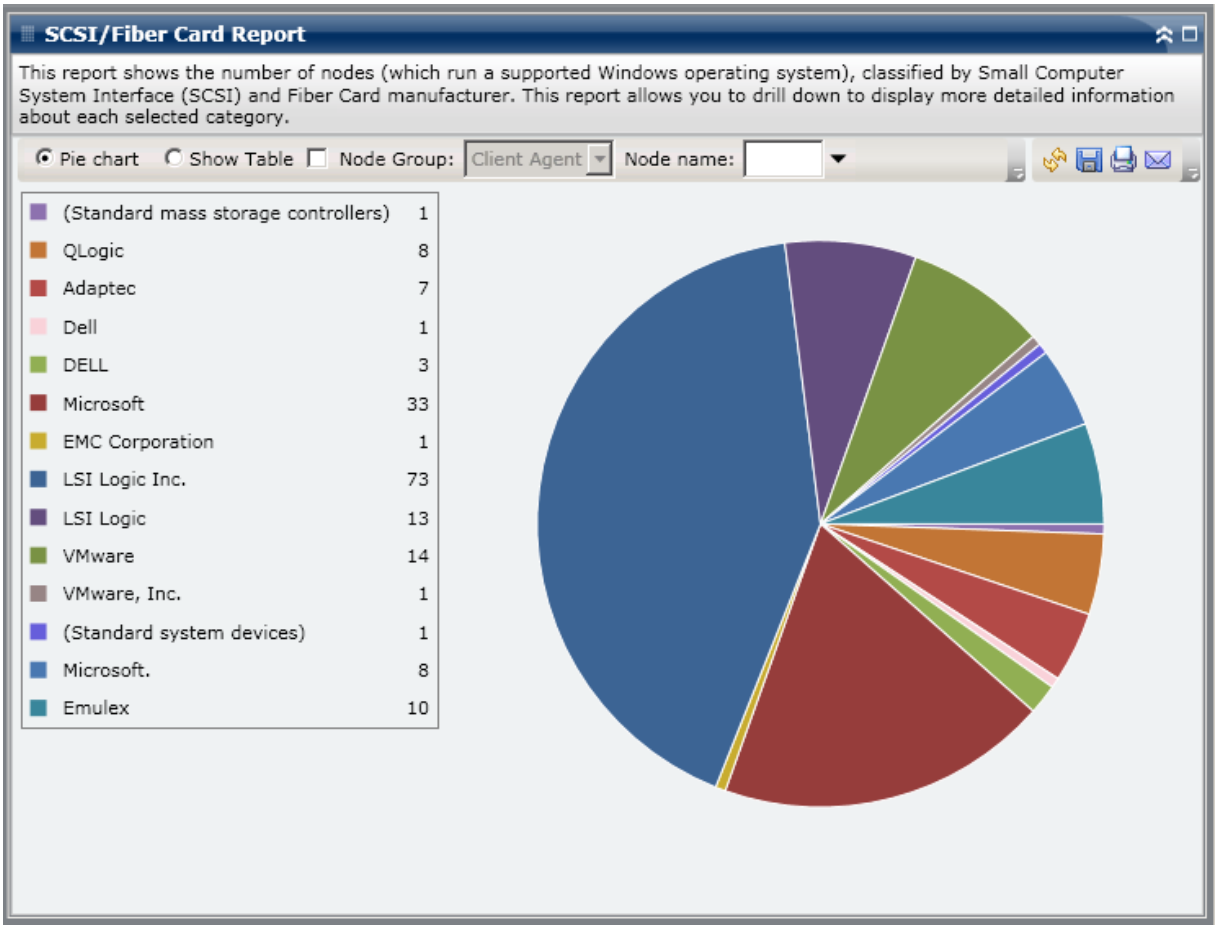
Always look for patterns in behavior to isolate potential problem SCSI or fiber cards and determine if the same SCSI or fiber cards are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The SCSI/Fiber Card Report is displayed in a pie chart or table format. This report contains filters for Node Group, Node Name, and Node Tier.

Pie Chart

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



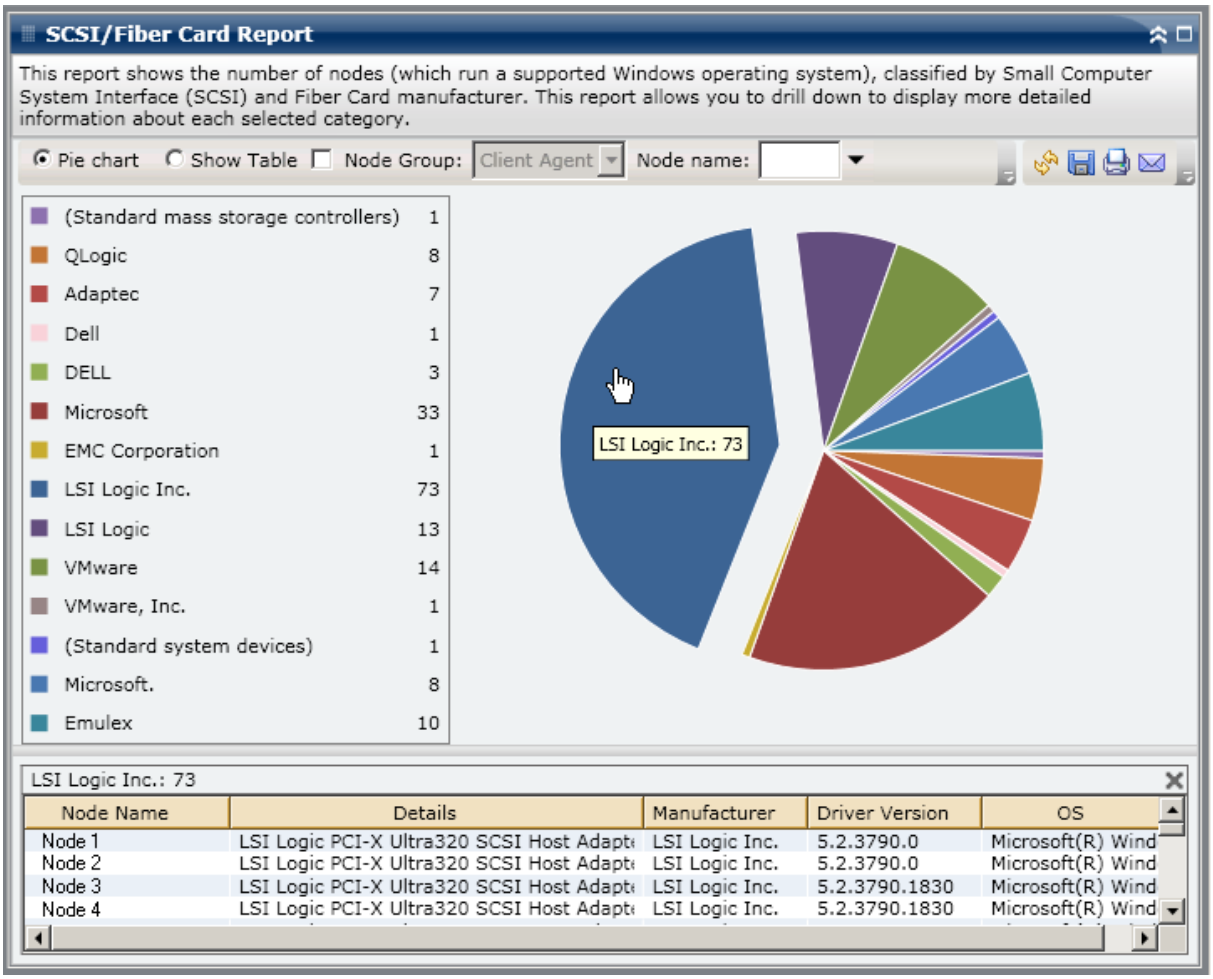
Show Table

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 62).

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.



SRM PKI Utilization Reports

To ensure your servers are efficient and reliable, you need to continually monitor performance to identify possible problems and quickly address bottleneck situations. Dashboard provides four SRM utilization type reports--CPU, Disk Performance, Memory, and Network. These utilization type reports can be used in conjunction with each other to collect different types of data from your Arcserve Backup protected servers during a specified period of time. This collected data can help you analyze server performance and isolate any problem areas.

From these utilization reports, you can perform system management monitoring to determine which servers are being used most and least. For servers with high utilization, you may want to consider some hardware upgrades to relieve bottleneck conditions caused by inefficient hardware. For servers with low utilization, you may want to consider server consolidation or virtualization to maximize your hardware usage. In addition, if you are having backup problems you should also view these utilization reports to determine if the problem could be related to these system-related areas.

Each of these utilization reports can be configured to send alert notifications when specified alert threshold level percentages are exceeded. The performance key indicator (PKI) threshold settings for each of these alerts are configured from the Arcserve Backup Central Agent Admin by accessing the Configure SRM PKI dialog. These alerts can be in the form of various methods of communication and sent to specified people as configured in the Arcserve Backup Alert Manager. For more information about configuring these alert settings, see the *Administration Guide*.

Note: If an alert notification fails to be sent, the failed alert will be included in the agent "AgPkiAlt.log" file, but no retry attempt will be made for the notification. The AgPkiAlt.log file is located in the following directory: X:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent\Log.

SRM PKI Report Benefits

The utilization reports are SRM-type reports that can be used in conjunction with each other to collect different types of data from your Arcserve Backup protected servers. These reports can be used to help you analyze server performance and isolate problem areas.

CPU Utilization Report

The CPU Utilization Report displays the percentage of CPU usage for a Arcserve Backup protected server during a specified period of time. You can use this report to monitor CPU usage and make sure that it does not become overloaded too often. If your CPU usage is too high, your server response time may become very slow or unresponsive and you should consider spreading out (balancing) your load. If your CPU usage is too low, you may want to consider server consolidation or virtualization to maximize your hardware usage.

Disk Performance Report

The Disk Performance Report displays the disk throughput for a Arcserve Backup protected server during a specified period of time. You can use this report to monitor disk throughput and make sure that you are maximizing your disk capability. If your disk throughput is far less than the disk capabilities, you may not need the excessive capabilities of that particular disk and should consider downgrading to a more efficient disk to better match your needs. If your disk throughput is close to the maximum value that your disk can handle, you should consider upgrading to a disk that better matches your needs. Generally a faster disk leads to better performance.

Memory Utilization Report

The Memory Utilization Report displays the percentage of memory in use on your Arcserve Backup protected servers during a specified period of time. Utilization is how much of your memory capacity you are using. The higher the percentage the worse your server performance will be. If your memory utilization continually becomes too high, you need to determine which process is causing this high usage. You can use this report to determine when a application or server upgrade may be necessary.

Network Utilization Report

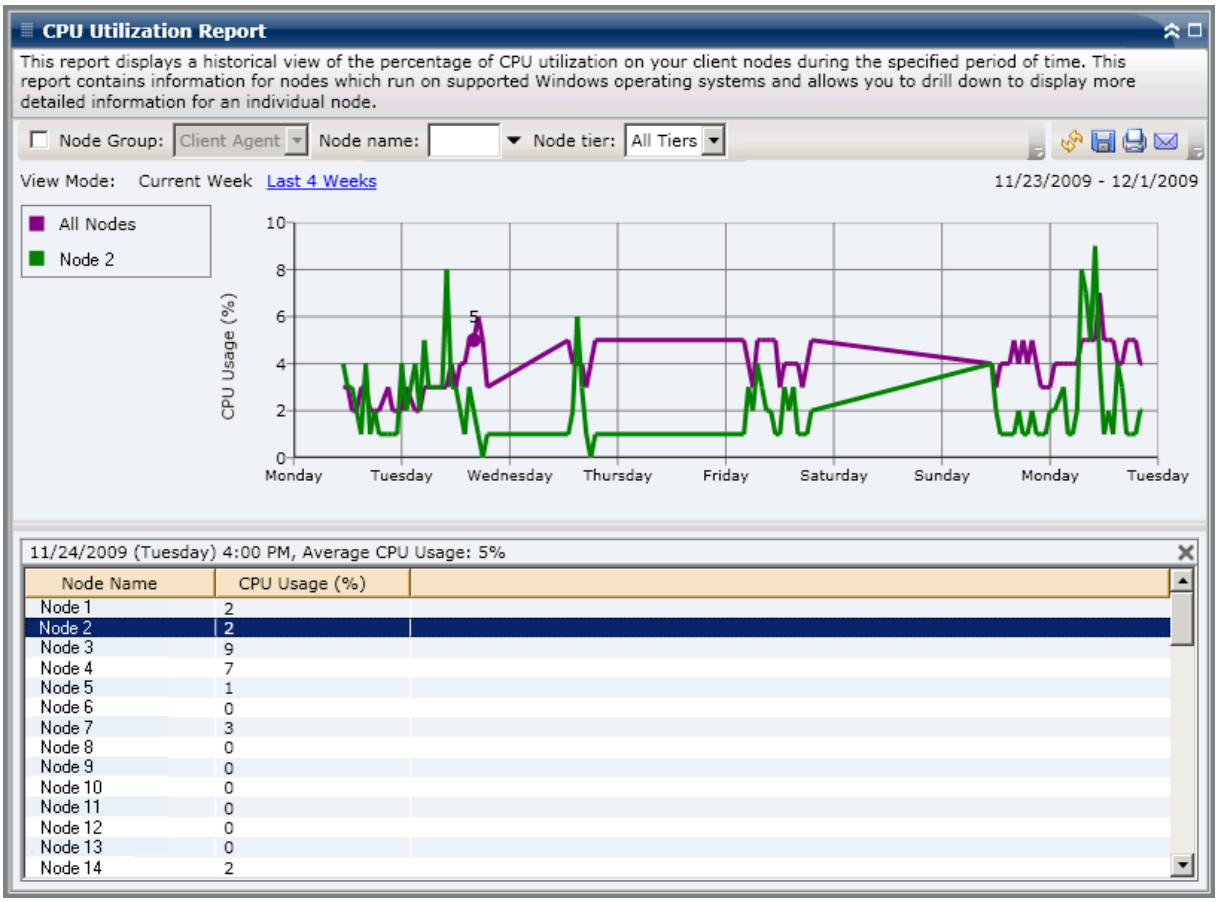
The Network Utilization Report displays the percentage of NIC bandwidth you are currently using on your Arcserve Backup protected servers during a specified period of time. Utilization is how much of your network interface (or NIC) capacity you are using. The higher the percentage the worse your network performance will be. If your network utilization continually becomes too high, you need to determine which process is causing this high usage and remedy the problem.

In addition, if based on your specific network capacity the percentage of your network utilization is too high during backup time, you may need to upgrade your NIC card to handle the higher throughput requirements. If your network utilization is too low, you may want to consider server consolidation or virtualization to maximize your hardware usage.

CPU Utilization Report

The CPU Utilization Report is displayed in graph format showing a historical view of the percentage of CPU usage for the monitored servers during a specified time period (only for nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data for the last 7 days, and the Last 4 Weeks mode displays data for the last 4 weeks. You can use the scroll bar at the bottom of the chart to adjust the time period or click on any sample point along the data line to display more details about that specific sample point. You can also filter the data by node name, node group, or node tier level.

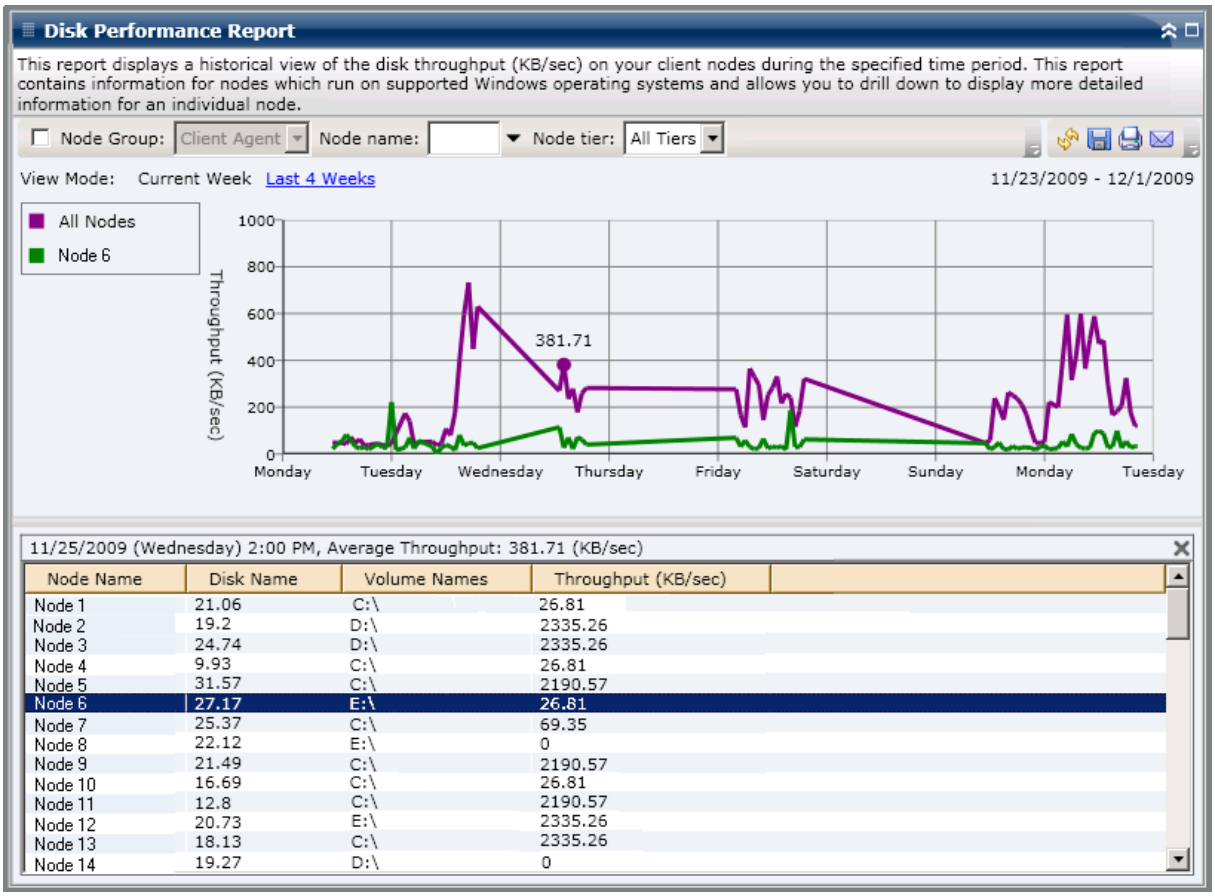
The CPU Utilization Report can be further expanded to display more detailed information. You can click on a sample point on the line chart to show the details of that specific time period. This drill-down report includes the Arcserve Backup protected node names, along with the corresponding percentage of CPU usage for each node. You can also click on the name of an individual node to display the line chart information for that particular node overlaid on the overall line chart.



Disk Performance Report

The Disk Performance Report is displayed in graph format showing the a historical view of disk throughput (speed in KB/sec) for the monitored servers during a specified time period (only for nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data for the last 7 days, and the Last 4 Weeks mode displays data for the last 4 weeks. You can use the scroll bar at the bottom of the chart to adjust the time period or click on any sample point along the data line to display more details about that specific sample point. You can also filter the data by node name, node group, or node tier level.

The Disk Performance Report can be further expanded to display more detailed information. You can click on a sample point on the line chart to show the details of that specific time period. This drill-down report includes the Arcserve Backup protected node names, along with the corresponding disk name, volume names, and throughput. You can also click on the name of an individual node to display the line chart information for that particular node overlaid on the overall line chart.

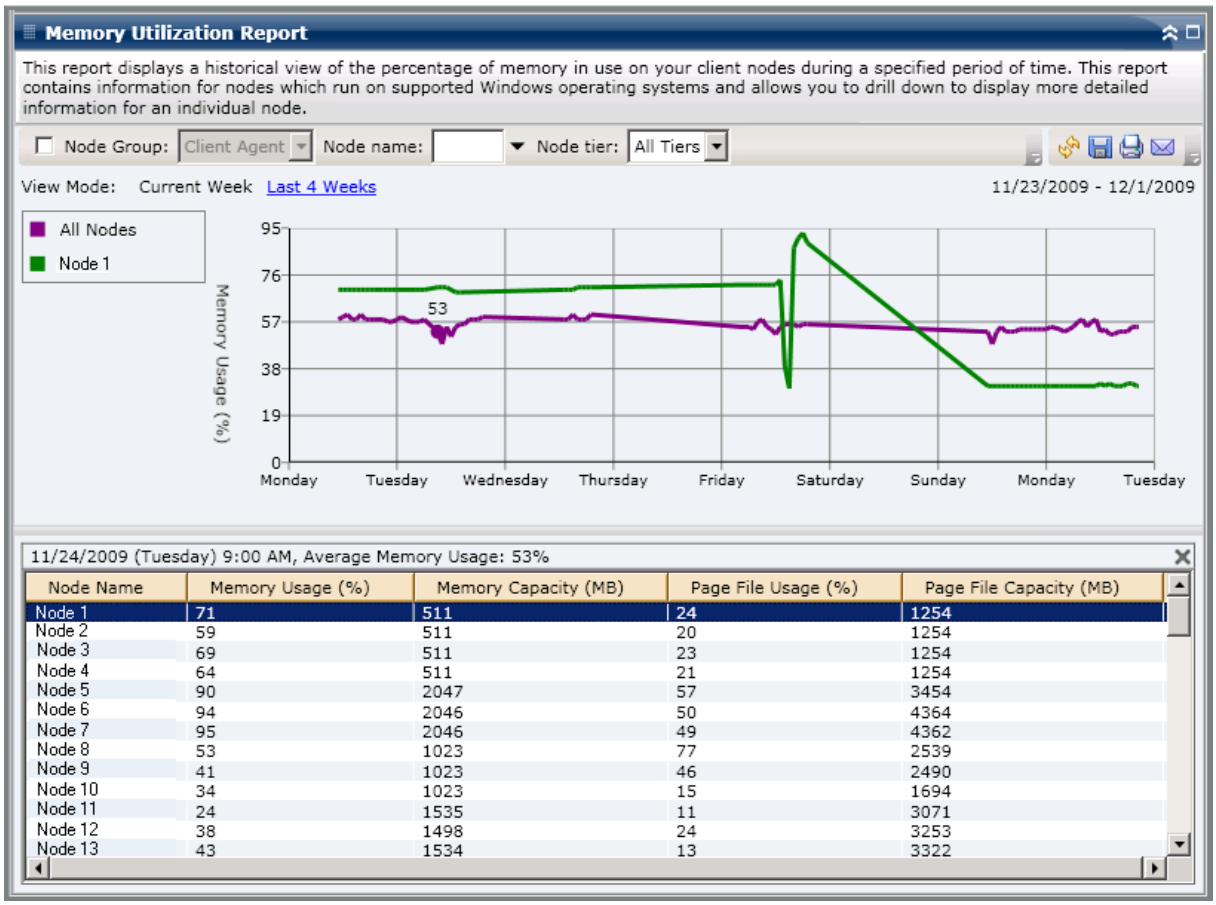


Memory Utilization Report

The Memory Utilization Report is displayed in graph format showing a historical view of the percentage of memory usage for the monitored servers during a specified time period (only for nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data for the last 7 days, and the Last 4 Weeks mode displays data for the last 4 weeks. You can use the scroll bar at the bottom of the chart to adjust the time period or click on any sample point along the data line to display more details about that specific sample point. You can also filter the data by node name, node group, or node tier level.

The Memory Utilization Report can be further expanded to display more detailed information. You can click on a sample point on the line chart to show the details of that specific time period. This drill-down report includes the Arcserve Backup protected node names, along with the corresponding percentage of memory usage, memory capacity, page file usage, and page file capacity for each node. You can also click on the name of an individual node to display the line chart information for that particular node overlaid on the overall line chart.

Note: A page file is a reserved portion of the hard disk drive that is used to temporarily store segments of data. This data is then swapped in and out of your physical memory when there is not enough memory to hold all that the applications are calling for and frees up some physical memory for your applications. A page file can also be referred to as a swap file.



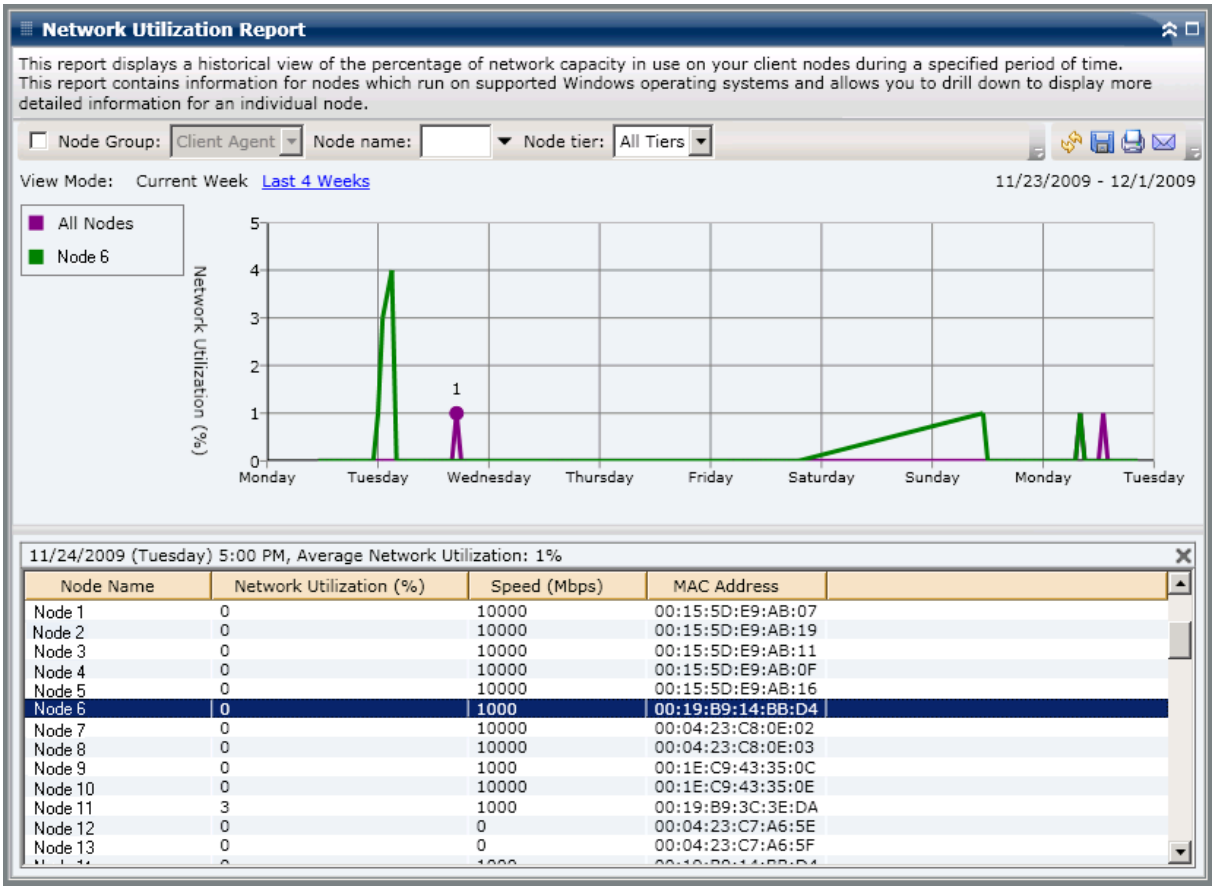
Node Name	Memory Usage (%)	Memory Capacity (MB)	Page File Usage (%)	Page File Capacity (MB)
Node 1	71	511	24	1254
Node 2	59	511	20	1254
Node 3	69	511	23	1254
Node 4	64	511	21	1254
Node 5	90	2047	57	3454
Node 6	94	2046	50	4364
Node 7	95	2046	49	4362
Node 8	53	1023	77	2539
Node 9	41	1023	46	2490
Node 10	34	1023	15	1694
Node 11	24	1535	11	3071
Node 12	38	1498	24	3253
Node 13	43	1534	13	3322

Network Utilization Report

The Network Utilization Report is displayed in graph format showing a historical view of the percentage of network (NIC) usage for the monitored servers during a specified time period (only for nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data for the last 7 days, and the Last 4 Weeks mode displays data for the last 4 weeks. You can use the scroll bar at the bottom of the chart to adjust the time period or click on any sample point along the data line to display more details about that specific sample point. You can also filter the data by node name, node group, or node tier level.

The Network Utilization Report can be further expanded to display more detailed information. You can click on a sample point on the line chart to show the details of that specific time period. This drill-down report includes the Arcserve Backup protected node names, along with the corresponding percentage of network usage, bandwidth speed (in MB/second), and the MAC address for each node. You can also click on the name of an individual node to display the line chart information for that particular node overlaid on the overall line chart.

Note: The MAC (Media Access Control) address is a hardware-unique value assigned by the manufacturer and associated with network adapters or network interface cards (NICs) for identification purposes.



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, this report can show 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.

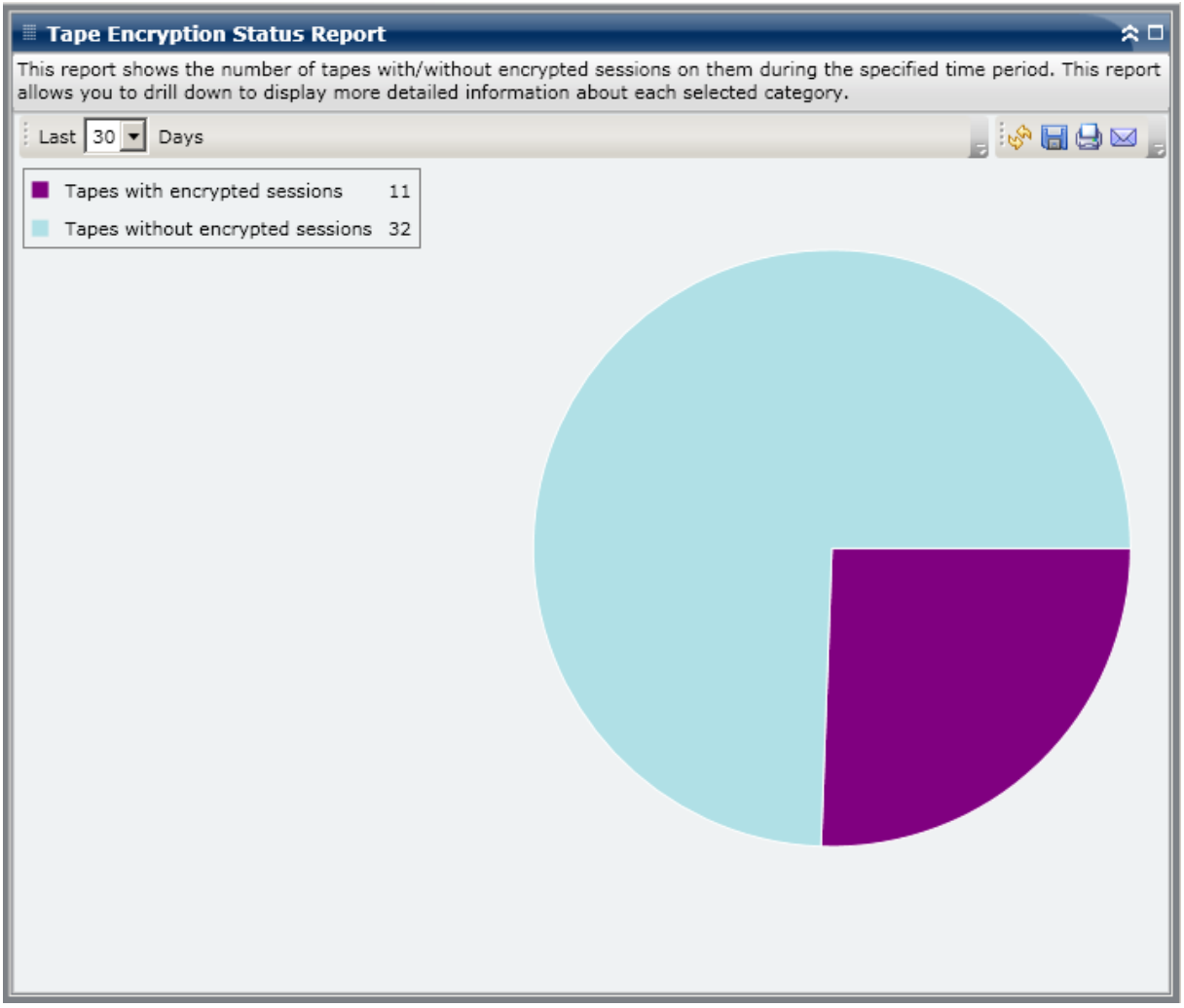
Likewise, from this report you can see if you have non-sensitive data that is being encrypted and therefore not only wasting valuable resources (time and money), but also slowing down your backup efforts.

> For example, if this report shows 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. This report contains a filter for Last # Days.

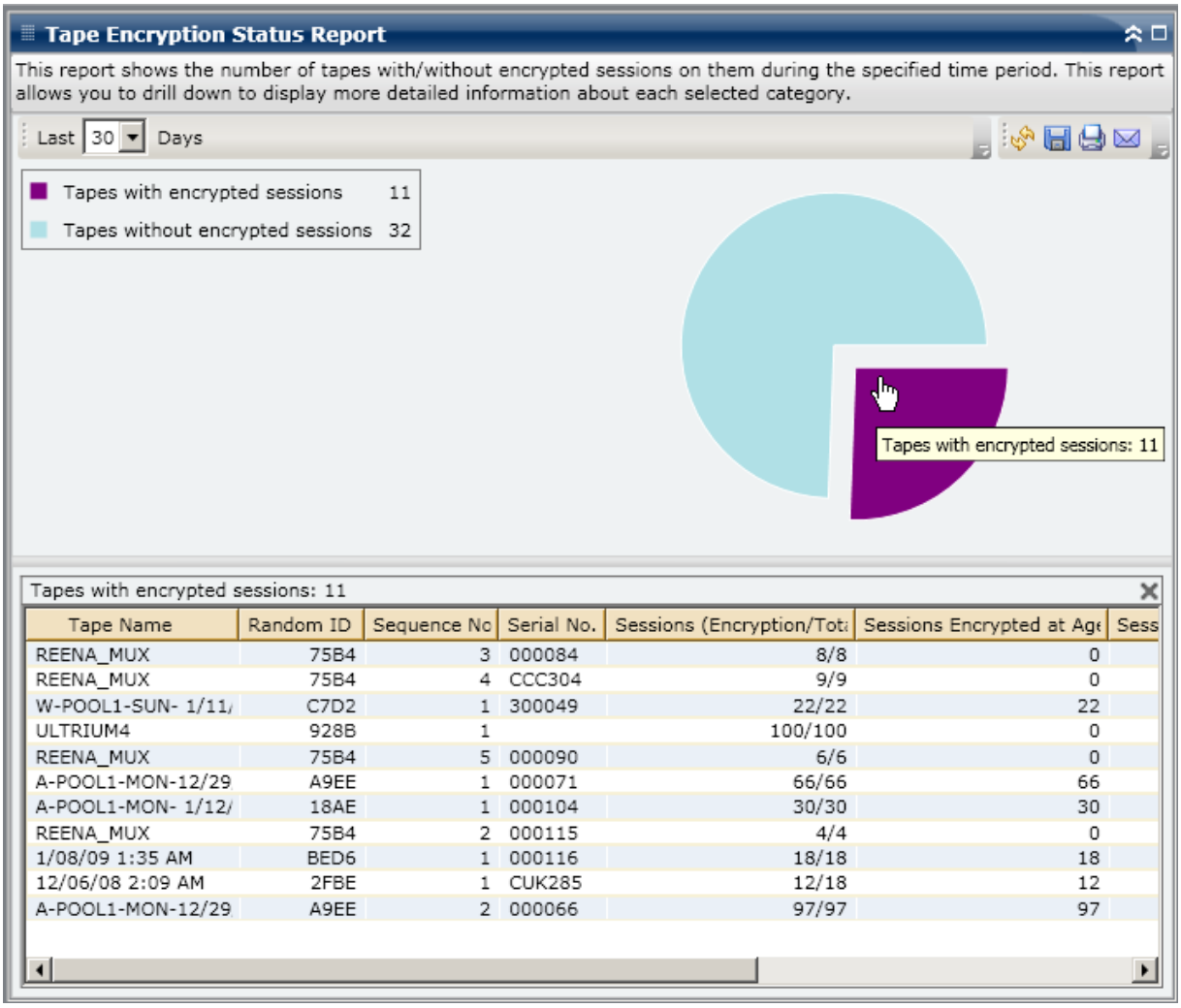
- Tapes with encrypted sessions are defined as tapes that have one or more encrypted backup sessions during the specified time period.
- Tapes without encrypted sessions are defined as tapes that do not have any encrypted backup sessions during the specified time period.



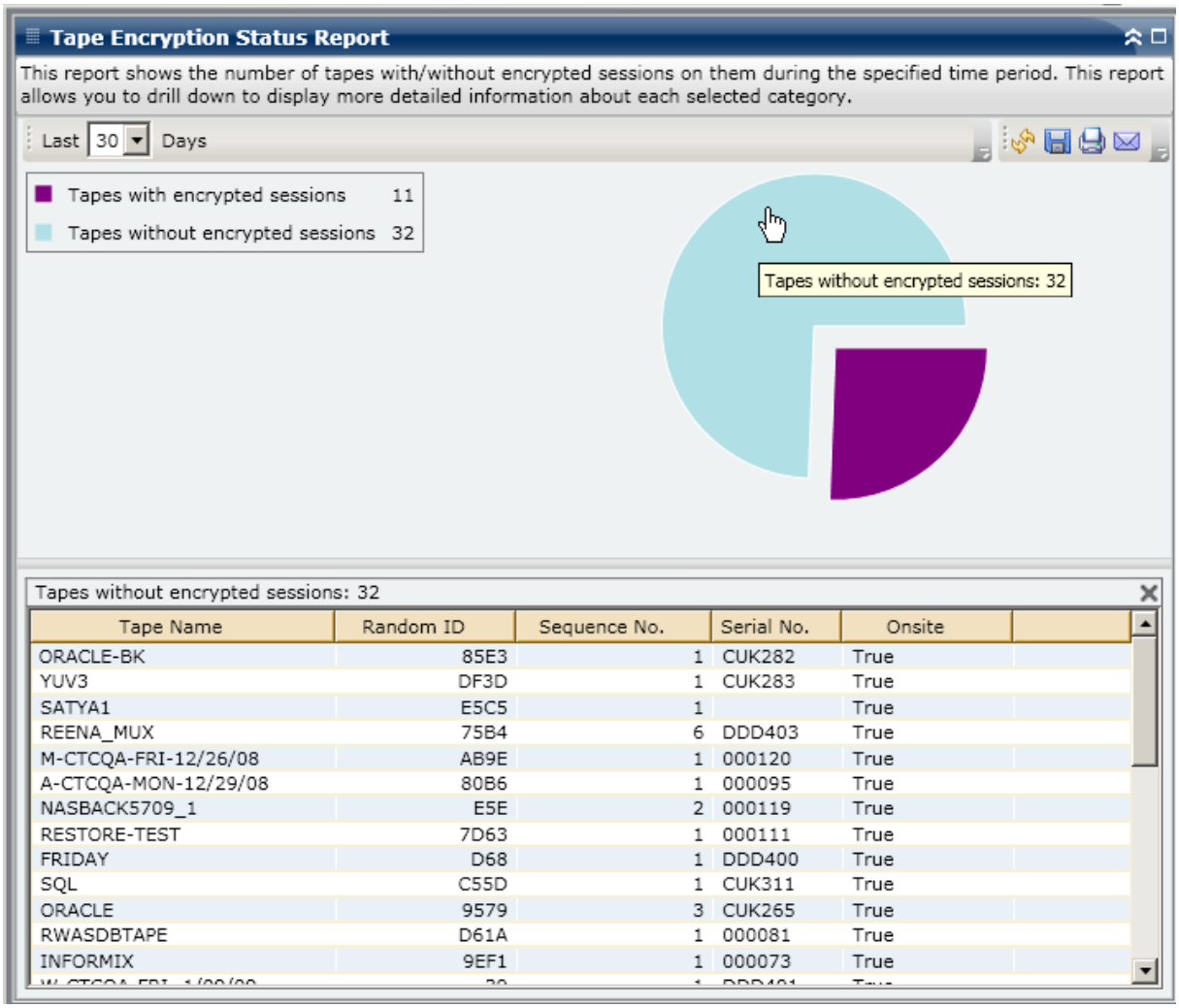
Drill Down Reports

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 drill 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 Arcserve Backup server (using software encryption and hardware encryption).
  - **Password only** - Session information is protected by a session password on the tape.



- If you drill 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.

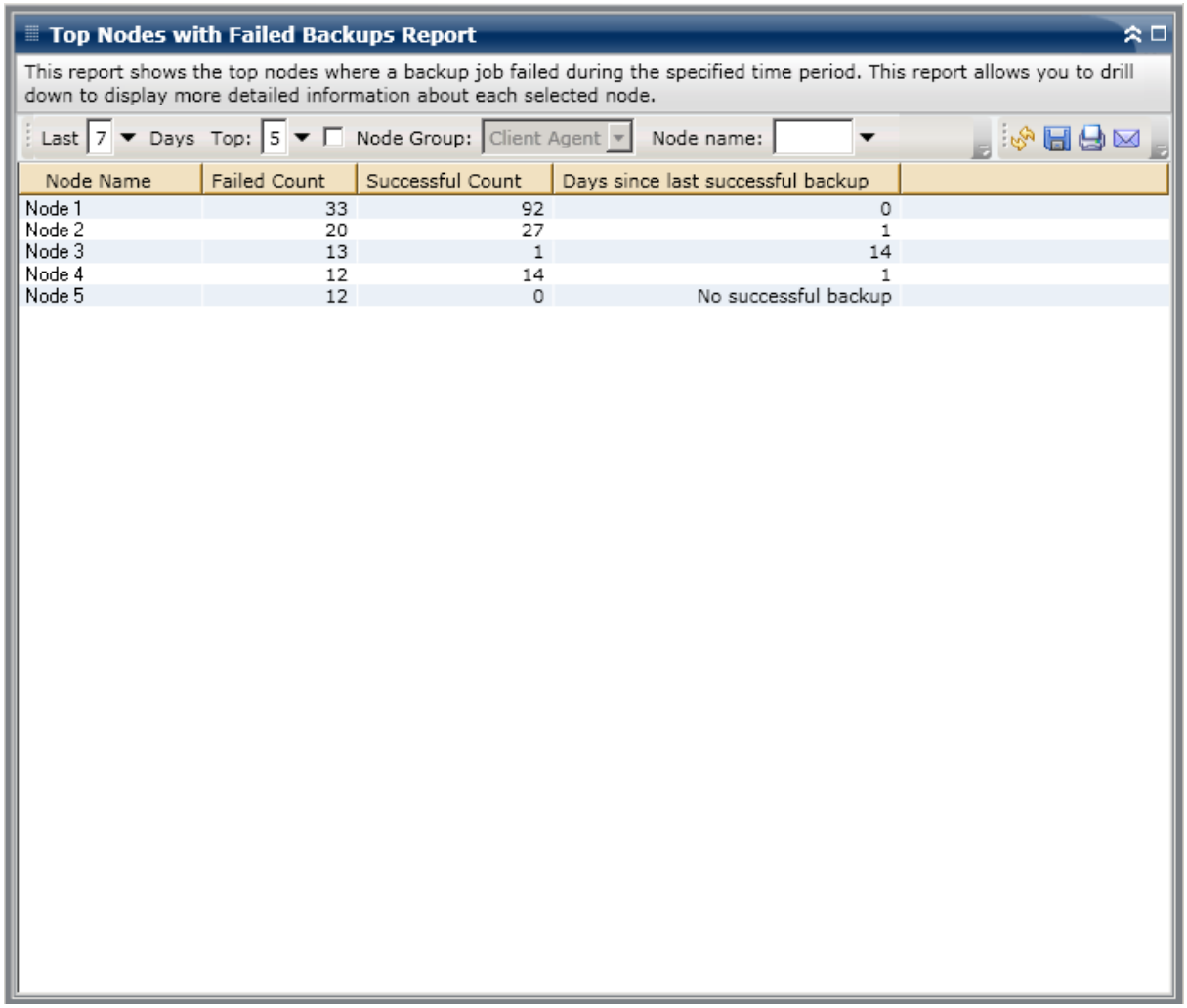
Note: An "N/A" displayed in this field indicates that the data is Not Applicable and means that there has not been a successful backup of this node during the specified time period.

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. This report contains filters for Last # Days, Top # of Failed Nodes, Node Group, Node Name, and Node Tier.

Note: By default, Arcserve Backup only retains Activity Log information for 14 days. If you want 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 62).



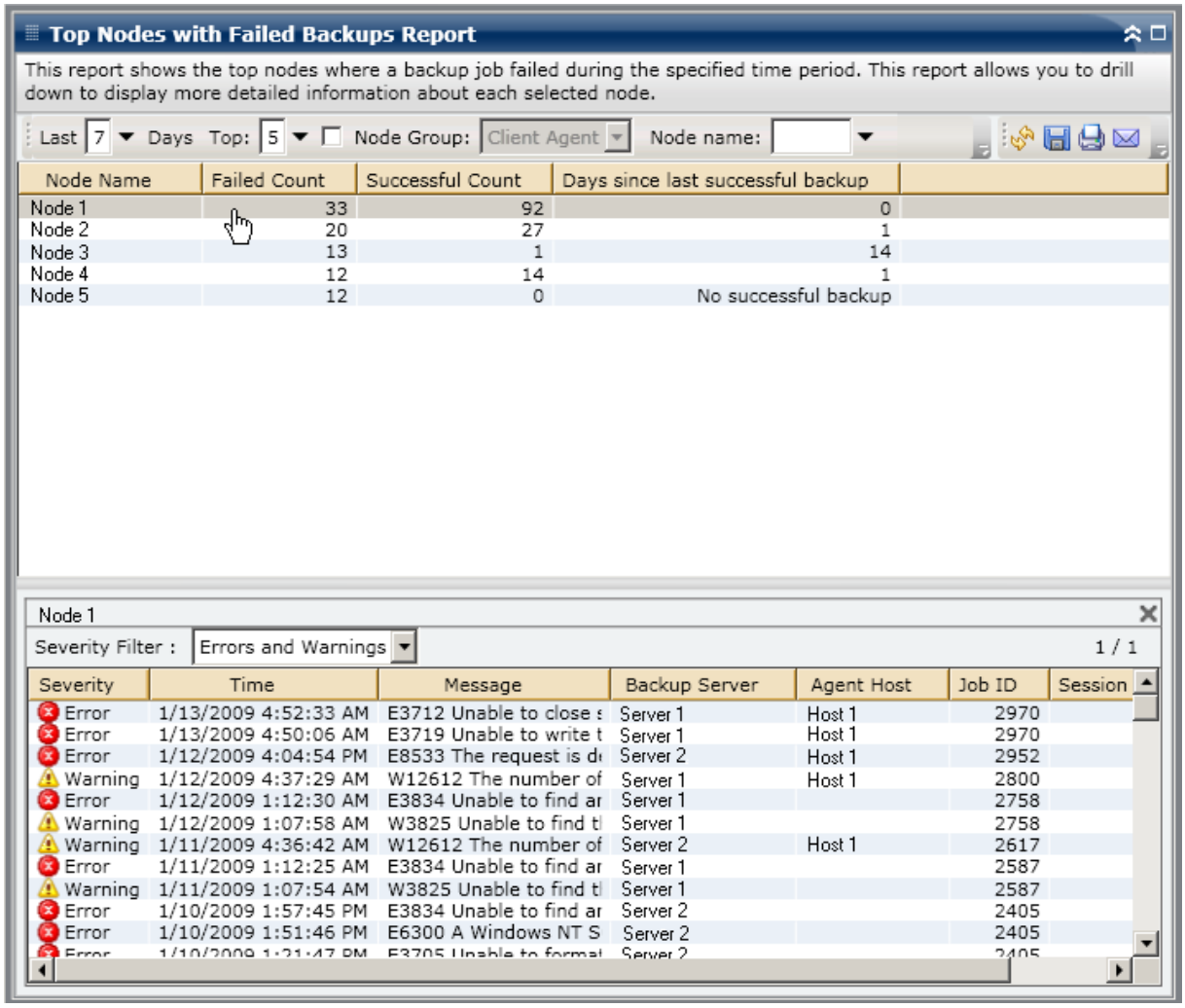
Node Name	Failed Count	Successful Count	Days since last successful backup
Node 1	33	92	0
Node 2	20	27	1
Node 3	13	1	14
Node 4	12	14	1
Node 5	12	0	No successful backup

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 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.

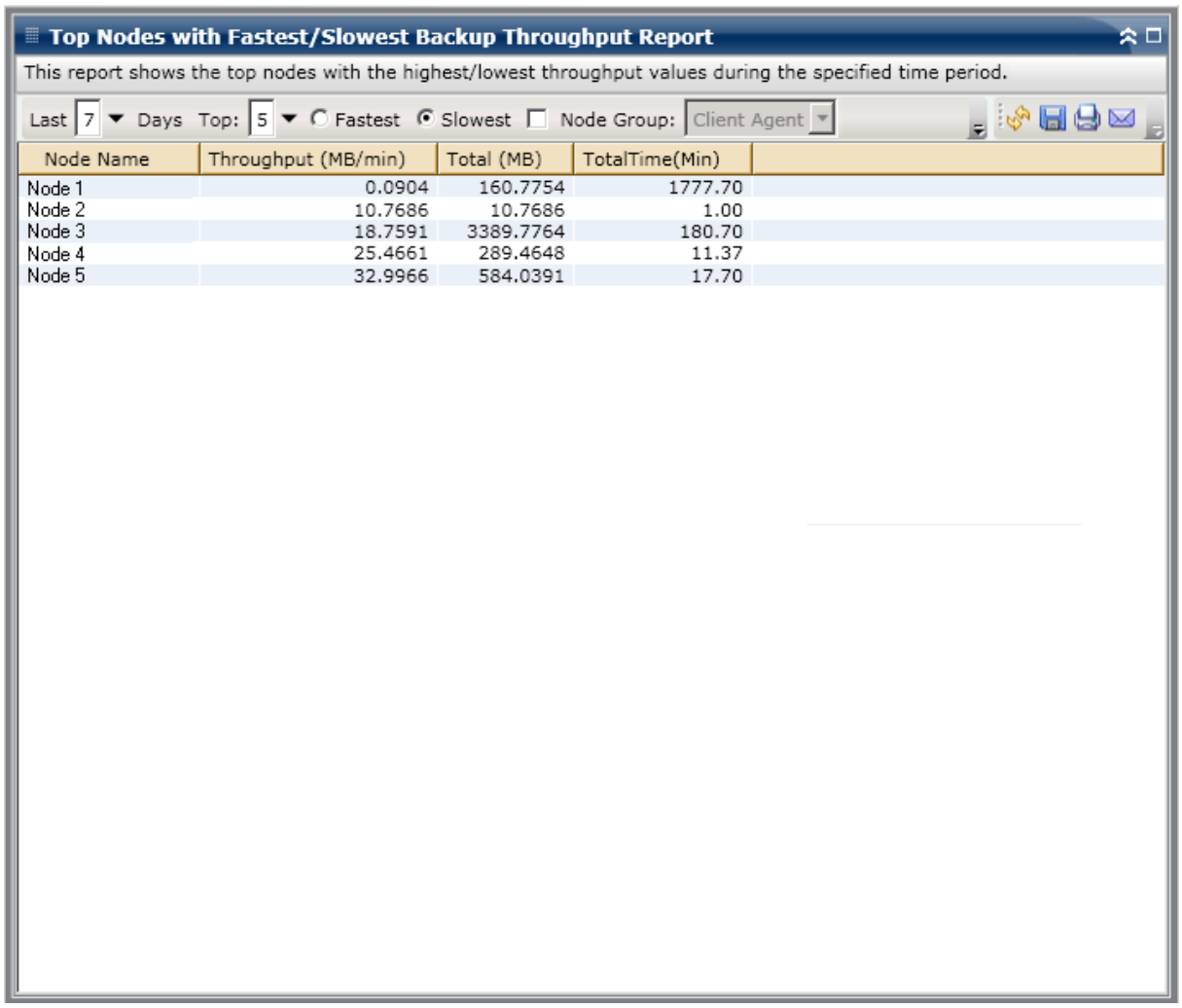
You can also use the fastest throughput values as reference points to analyze why these nodes are performing well. You can compare the slower nodes to the faster nodes to determine if you actually have a problem or if both sets of values are similar, maybe the slower nodes are not performing poorly. 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). This report contains filters for Last # Days, Top # of Fastest/Slowest Nodes, Node Group, Node Name, and Node Tier.

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 62).



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

Top Nodes with Most Unchanged Files Report

The Top Nodes with Most Unchanged Files Report is an SRM-type report that lists the top specified number of nodes with the largest unchanged file count or unchanged file size during the last specified number of days.

Report Benefits

The Top Nodes with Most Unchanged Files Report is helpful in analyzing and determining which nodes contain the largest number or size of files that have not changed during the selected time period. This report makes it easy for you to decide what to archive and what not to archive. Generally from this report, you would focus your attention on the nodes with the largest quantity or largest size values during the filtered time period and try to determine how many files and how much data could be archived so that the disk space could be reclaimed.

Report View

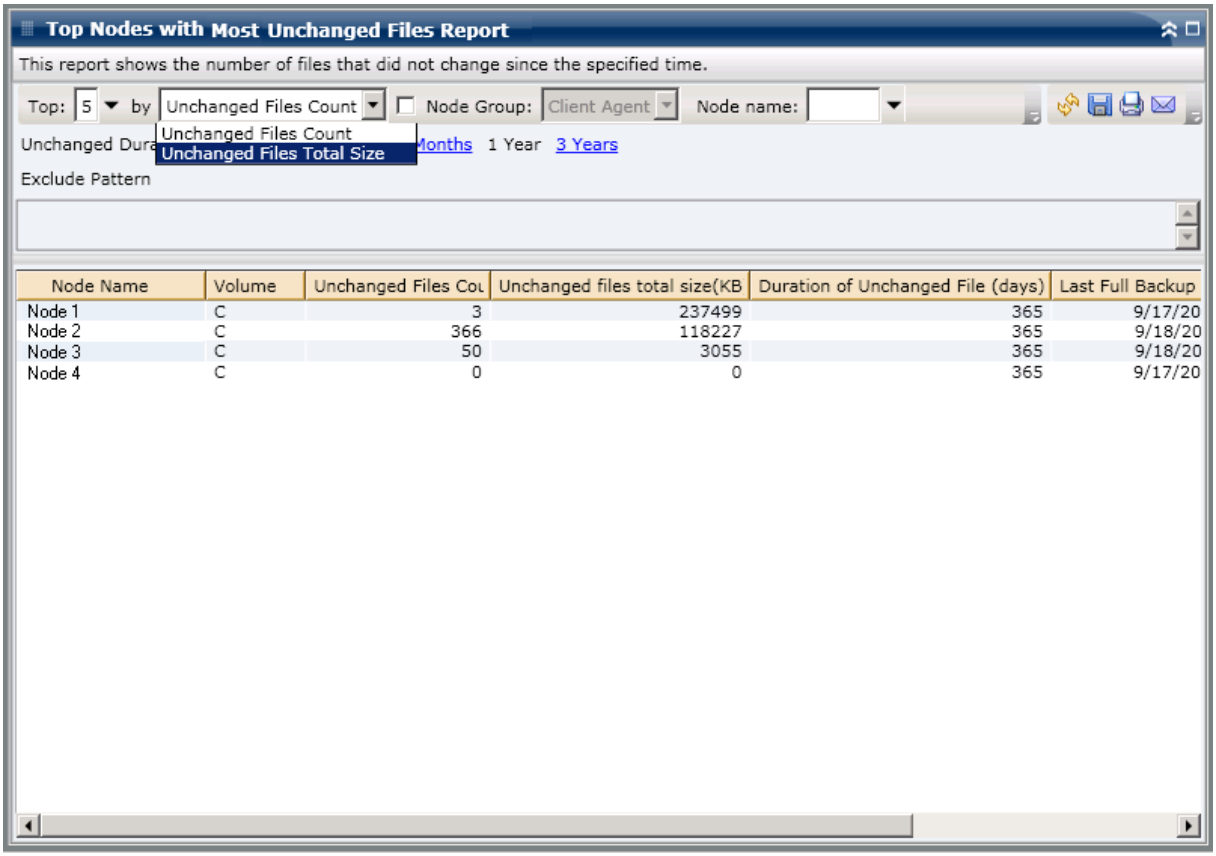
The Top Nodes with Most Unchanged Files Report is displayed in a table format, listing the nodes with the largest unchanged files. You can specify to filter this report to display either the most Unchanged Files Count or the largest Unchanged Files Total Size (default). This report also contains filters for Node Group, Node Name, and Node Tier.

The report consists of two main parts:

- The upper part of the report displays the exclude pattern filters which are used to determine which files (matching the pattern) to exclude from the query processing. The details for these pattern filters are specified from the Central Agent Admin window. For more information about the Central Agent Admin, see the *Administration Guide*.

  You can also select the duration time to filter the report display, with the available pre-defined duration time periods being 1 month, 3 months, 6 months, 1 year, or 3 years.

- The lower part of the report displays the top node listings that match the specified filters and includes such information as Node Name, Volume, Unchanged Files Count, Unchanged Files Total Size, Duration of Unchanged Files, and the Last full Backup Time.



Total Archive Size Report

The Total Archive Size Report displays the total size of data archived by Arcserve Backup within your domain. This report helps you perform capacity management and resource planning for your archive environment.

Report Benefits

The Total Archive Size Report lets you analyze the data capacity requirements for all nodes within your domain and can be used in various budget planning as well as operational planning to ensure that you have the capabilities to archive this data. This report displays the total size of the data archived and is based upon the size of all successful archives of each node, and not the total capacity of the node itself.

For example, if the total capacity of your node is 500 GB and your image for that node is 400 GB, this report will display the total size as 400 GB and your archive schedule should be based upon archiving it up to 400 GB.

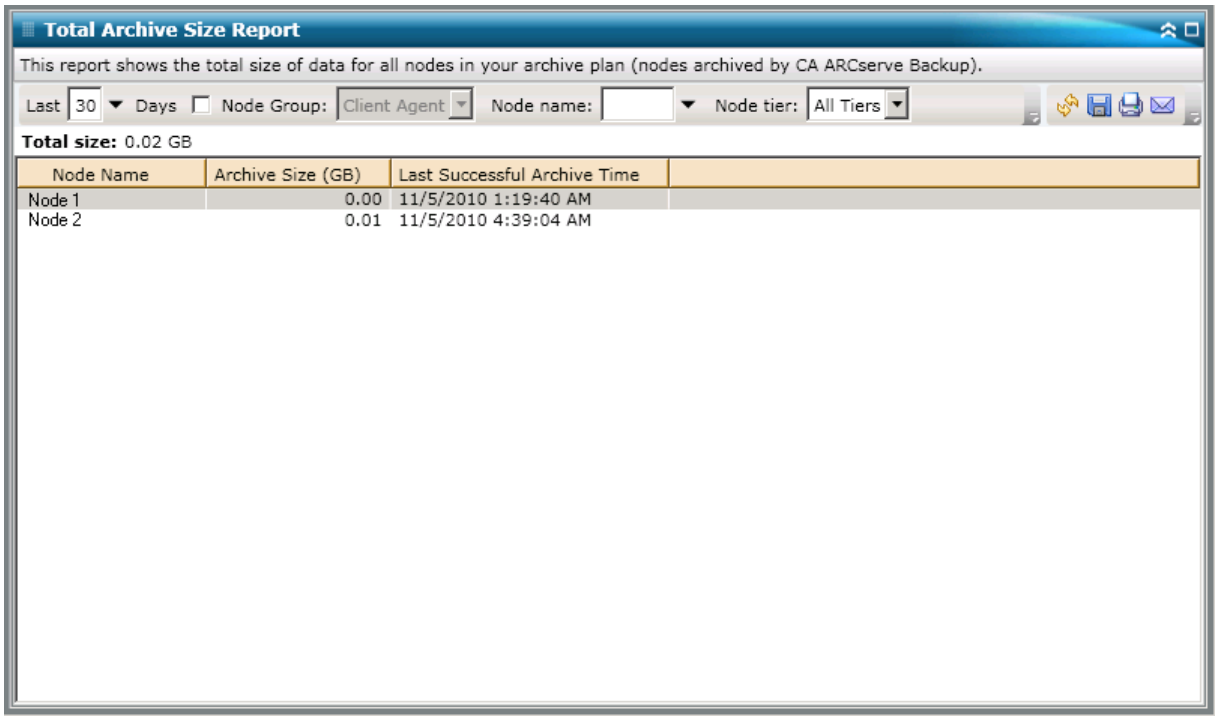
You can use this report to help manage your archive resources, including determining if you have adequate time capabilities to perform your scheduled archives and if you have an adequate number of tapes or disk space required to store this data.

You can also use this report to see the size of the data for the machines you archive. You can then plan or adjust your archive schedule for the nodes to meet your window requirement and device capability.

Report View

The Total Archive Size Report is displayed in table format listing Node Name, Backup Size, and the date and time of the last successful archive. The Total size value displayed is the combined size for all displayed nodes. This report contains filters for Last # Days, Node Group, Node Name, and Node Tier.

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 62).



Total Protection Size Report

The Total Protection Size Report displays the total size of data protected by Arcserve Backup within your backup domain. This report helps you perform capacity management and resource planning for your backup environment.

Report Benefits

The Total Protection Size Report lets you analyze the data capacity requirements for all nodes within your backup domain and can be used in various budget planning as well as operational planning to ensure that you have the capabilities to protect this data. This report displays the total size of the data protected and is based upon the size of your most recent successful full backup of each node, and not the total capacity of the node itself.

For example, if the total capacity of your node is 500 GB and your backup image for that node is 400 GB, this report will display the total protection size as 400 GB and your backup schedule should be based upon backing up 400 GB.

You can use this report to help manage your backup resources, including determining if you have adequate time capabilities to perform your scheduled backups and if you have an adequate number of tapes or disk space required to store this backed up data.

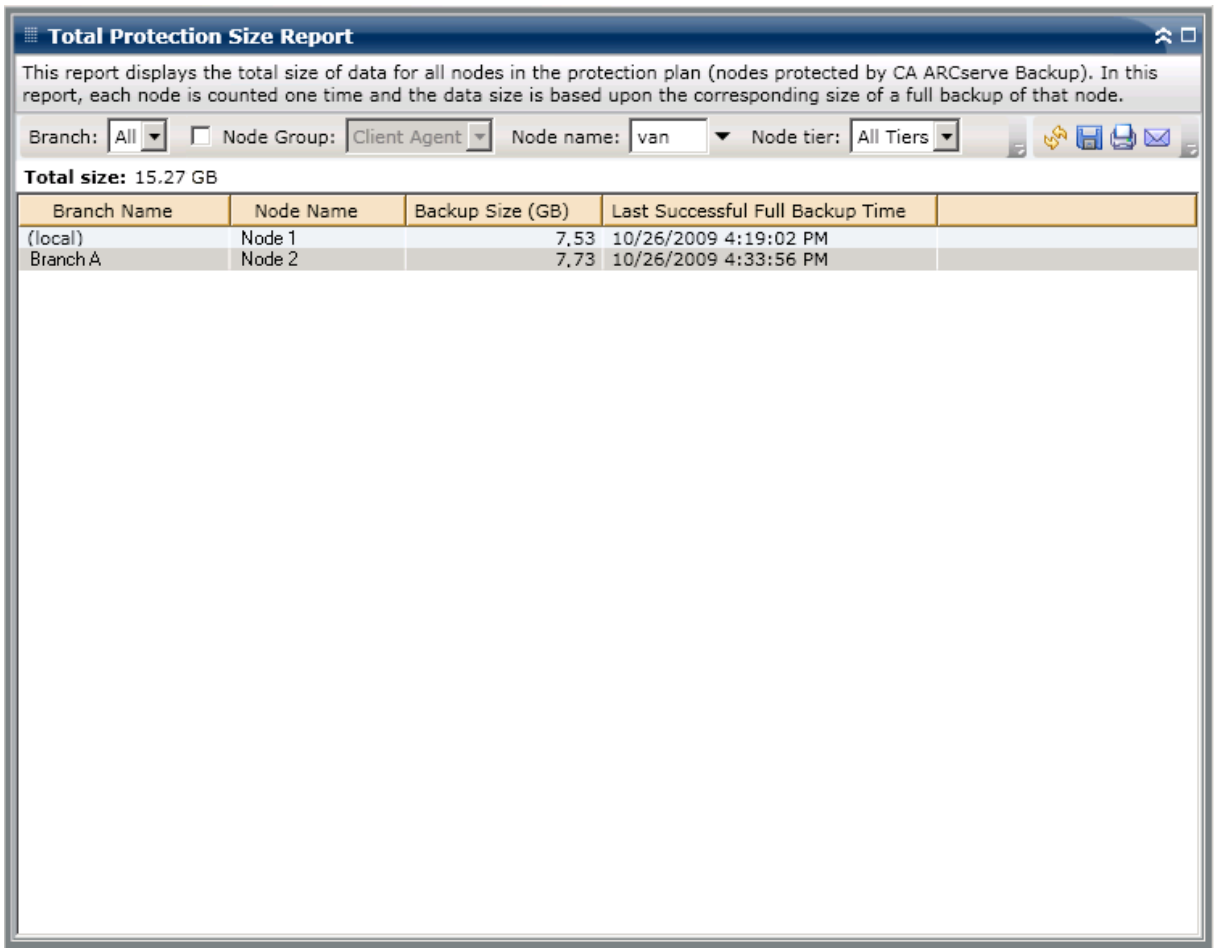
For example, if this report shows that a specific node contained 10 TB of data that is being backed up and your current backup window is limited to 10 hours each day. You can then quickly determine if you have adequate resource capabilities to back up 1 TB of data every hour and if necessary, take the appropriate planning actions to either improve your backup rate or increase your backup window.

You can also use this report to see the size of the data for the machines you protect. You can then plan or adjust your backup schedule for the nodes to meet your backup window requirement and device capability.

Report View

The Total Protection Size Report is displayed in table format listing Node Name, Backup Size, and the date and time of the last successful backup. The Total size value displayed is the combined size for all displayed nodes. This report contains filters for Backup Type, Node Group, Node Name, and Node Tier.

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 62).



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.

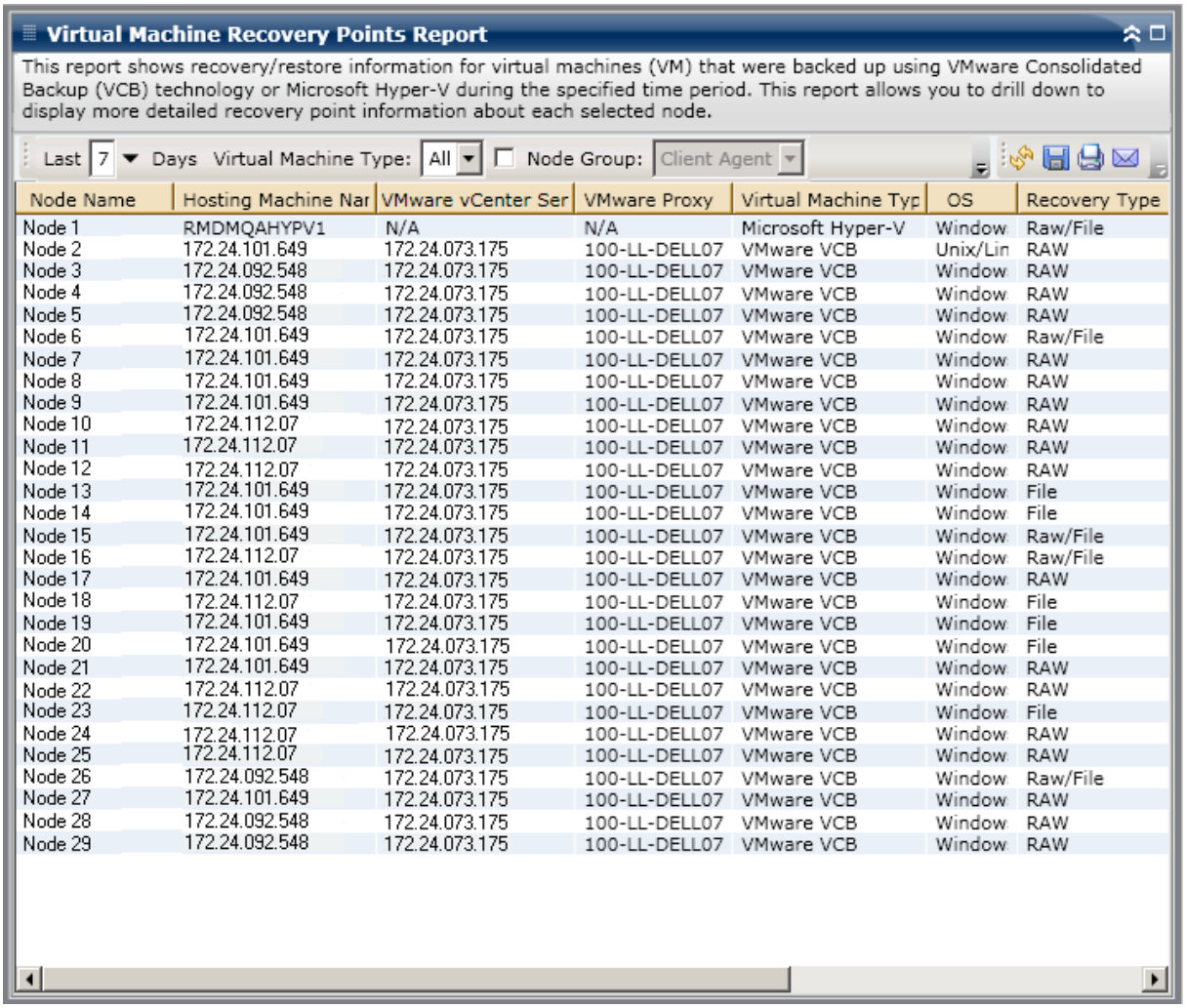
For example, a VM that contains high-priority data should have five recovery points taken to be adequately protected. If from this report, you discover that this specific high-priority VM only contains two recovery points, you should investigate the reason, and modify your backup schedule as necessary 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. This report contains filters for Last # of Days, Virtual Machine Type, Node Group, Node Name, and Node Tier.

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 62).



Virtual Machine Recovery Points Report

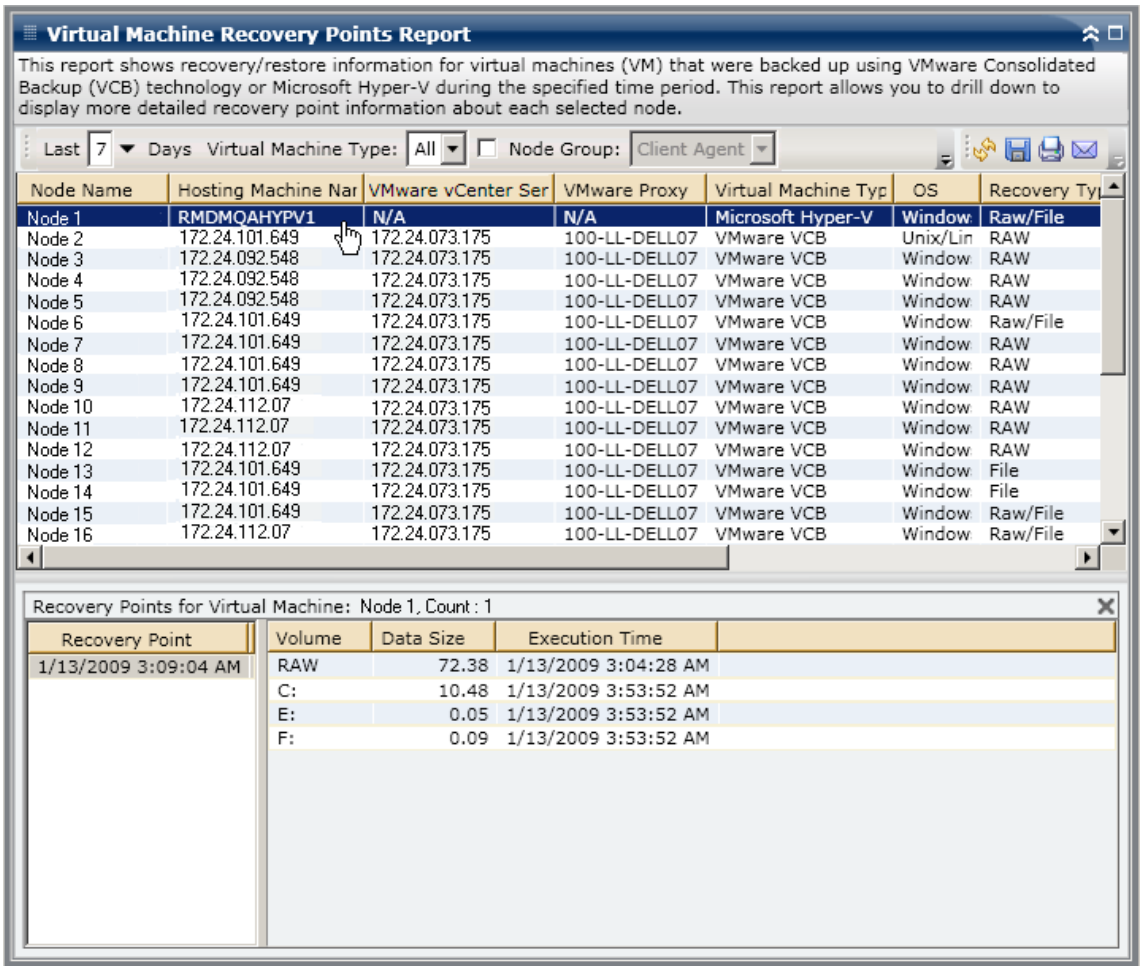
This report shows recovery/restore information for virtual machines (VM) that were backed up using VMware Consolidated Backup (VCB) technology or Microsoft Hyper-V during the specified time period. This report allows you to drill down to display more detailed recovery point information about each selected node.

Last 7 Days Virtual Machine Type: All Node Group: Client Agent

Node Name	Hosting Machine Nar	VMware vCenter Ser	VMware Proxy	Virtual Machine Typ	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 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's 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.

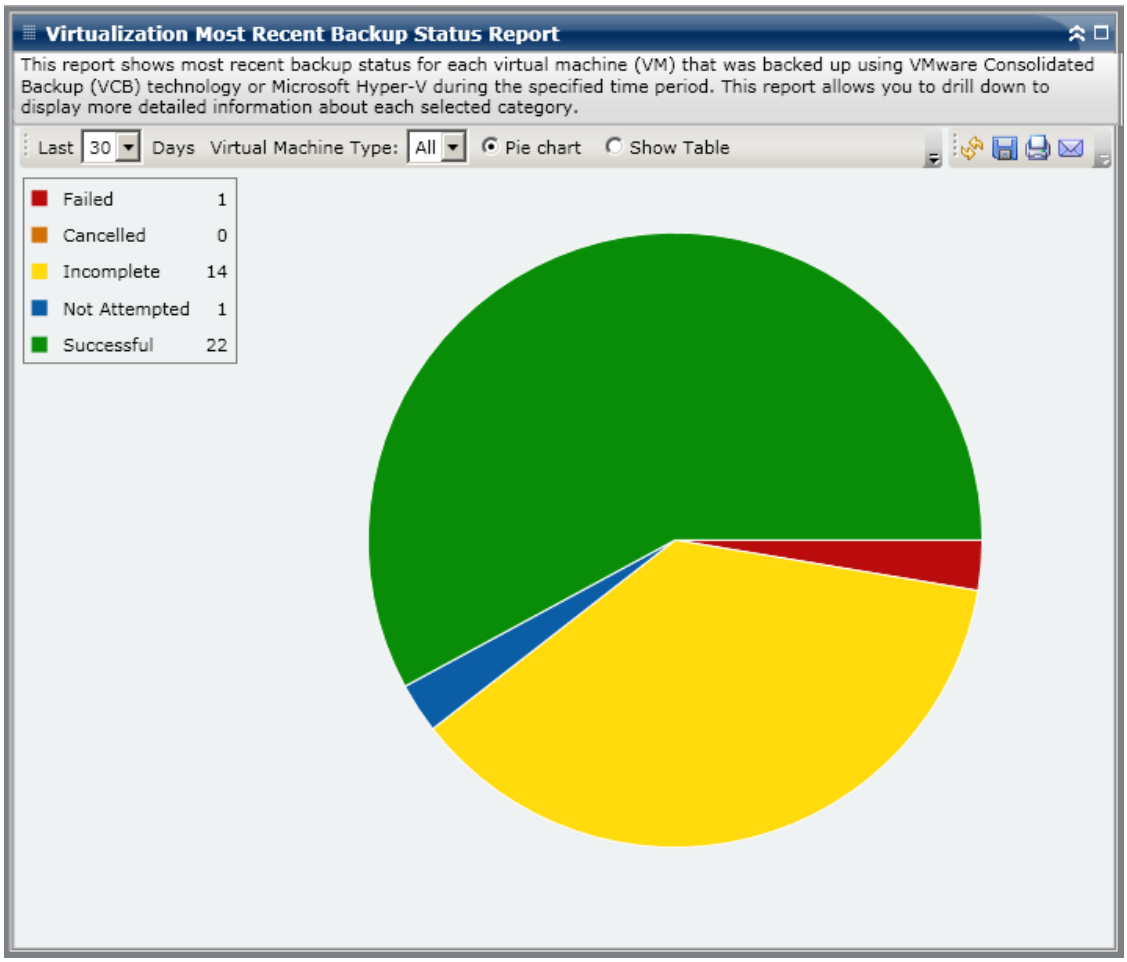
Always look for patterns in behavior to isolate potential problem jobs and determine if the same jobs are failing frequently. It is important to analyze the results from all fields of this report when attempting to determine problem backup jobs.

Report View

The Virtualization Most Recent Backup Status Report is displayed in a pie chart or table format. This report contains filters for Last # of Days, Virtual Machine Type, Node Group, Node Name, and Node Tier.

Pie Chart

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



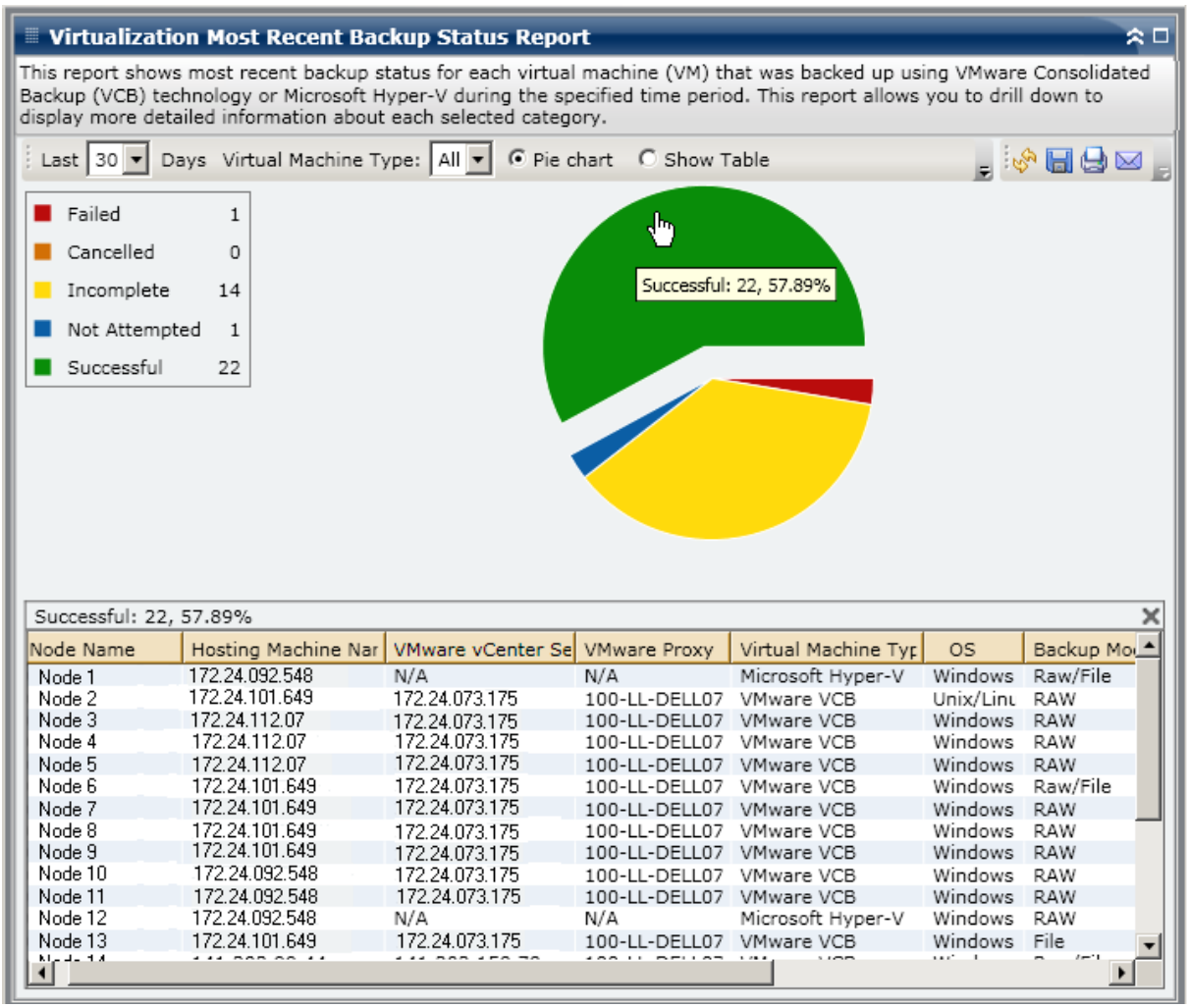
Show Table

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 vCenter Server, 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 62).

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 this report shows 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.

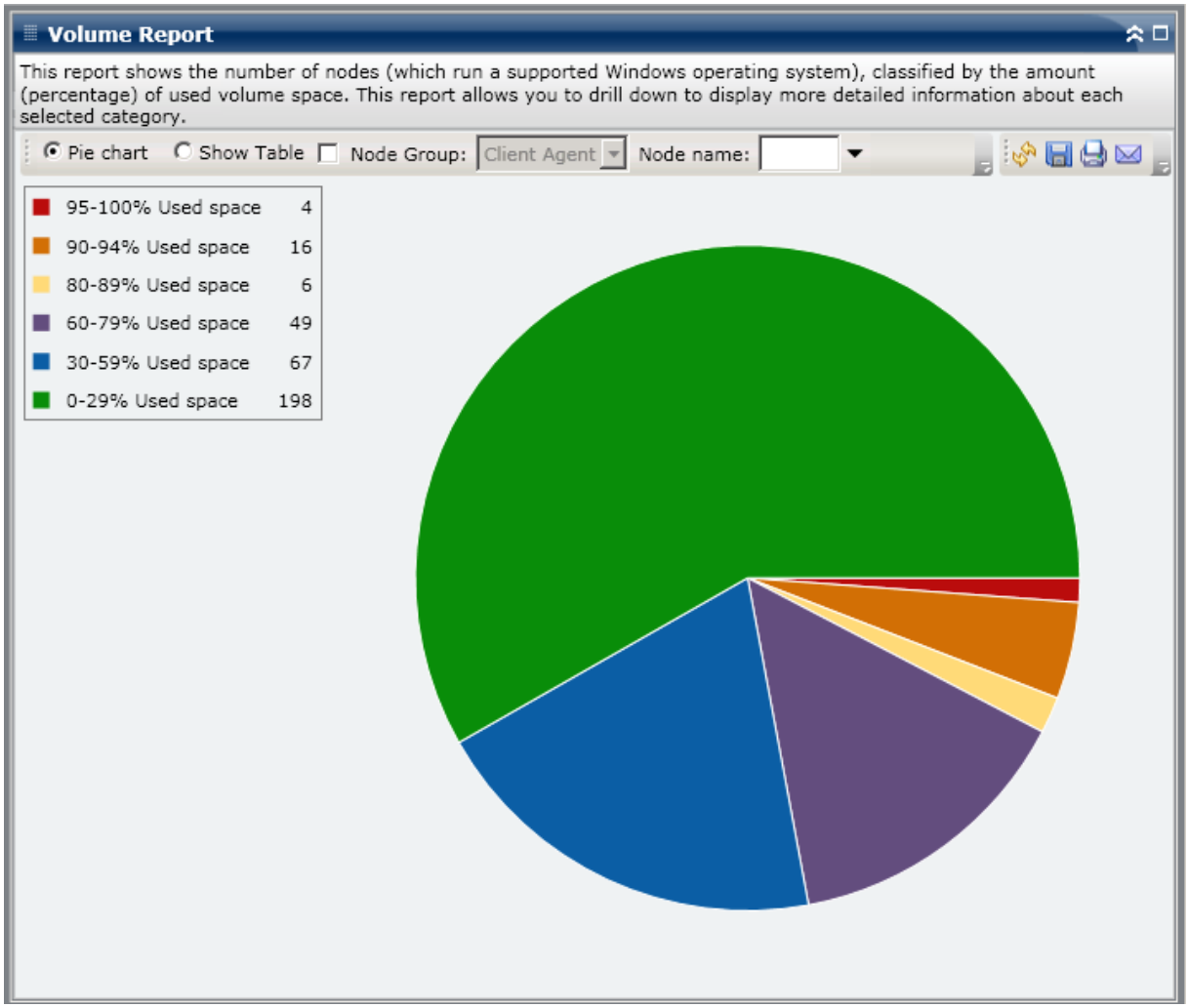
It is important to analyze the results from all fields of this report when attempting to determine problem nodes.

Report View

The Volume Report is displayed in pie chart or table format. This report contains filters for Node Group, Node Name, and Node Tier.

Pie Chart

The pie chart shows the amount of volume space used in preconfigured percentage categories.



Show Table

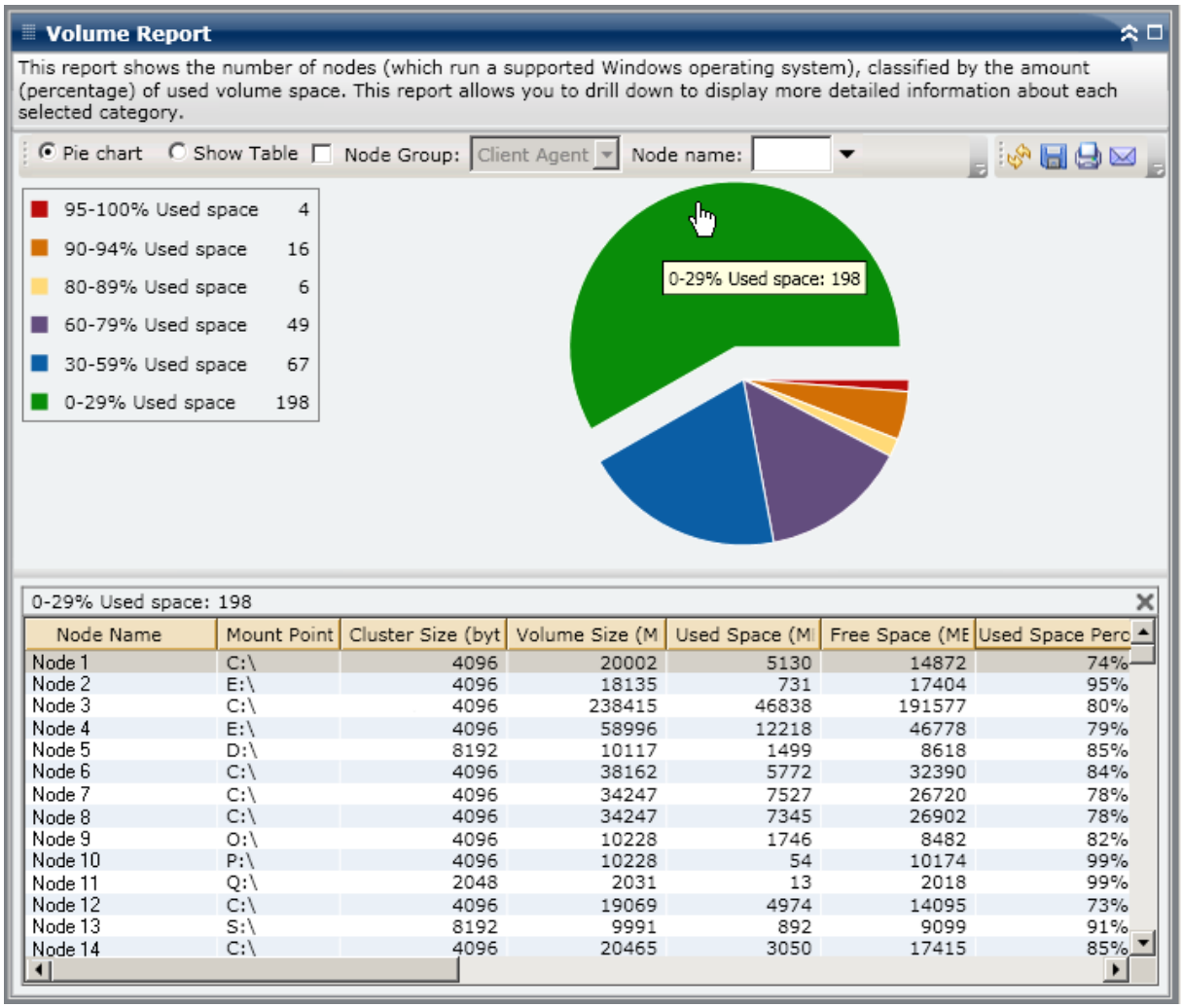
If you select Show Table, the Volume Report displays more detailed information in table format, listing the Node Name, OS, Mount Point, Cluster Size, Volume Size, Free Space, Free Space Percentage, Volume Type, Disk Name, Compressed, File System Type, and Total Fragmentation for all of the allocated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

Note: For Total Fragmentation data, because Windows XP systems are not supported, this column will display N/A. In addition, some FAT32 volumes may not provide fragmentation data and will also display N/A in this column.

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 62).

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.



Volume Trend Report

The Volume Trend Report is an SRM-type report that displays the data size in use for each volume in a historical view and then projects the growth trend for these volumes so that you can anticipate and prepare for future volume space requirements. This report displays the information for nodes which run a supported Windows operating system and allows you to drill down to display more detailed information for a single node.

Report Benefits

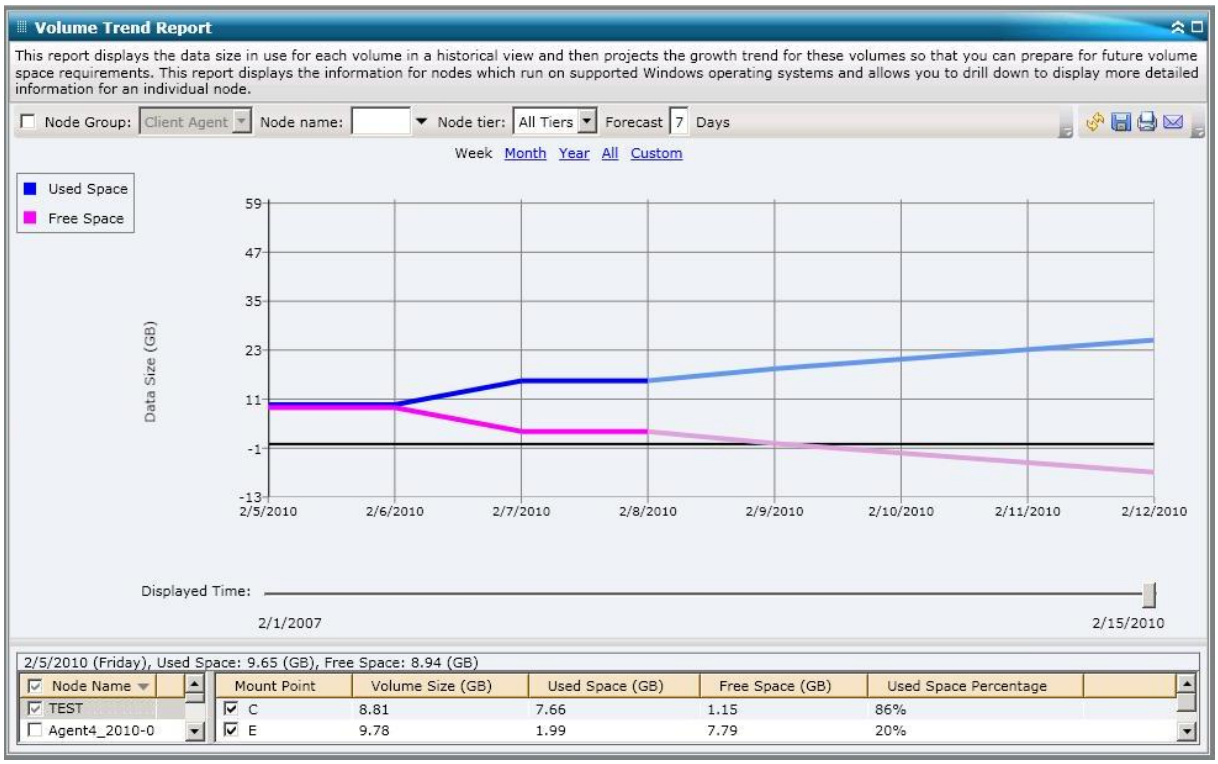
The Volume Trend Report is helpful in analyzing the current (and historical) size of data in use for each volume. In addition, this report is also helpful in determining the future volume size needs based upon anticipated growth trends. With this information, you can then predict volume space requirements for a future time period and take actions accordingly to ensure you are properly protected.

Report View

The Volume Trend Report is displayed in graph format showing the used space and free space capacity (in GB) for each volume, along with the anticipated trends during a future time period. The report lets you specify the view mode (Week, Month, Year, All, and Customized Time Range) for the displayed time period. You can use the scroll bar at the bottom of the chart to adjust the time period being displayed or click on any sample point along the data line to display more details about that specific sample point. This report contains filters for Node Group, Node Name, and Node Tier. You can also filter the data by individual volumes and the forecasted time range.

This report lets you easily see the projected trends in capacity for each volume to help you plan for your future needs. The data from each volume category (Used Space and Free Space) is displayed as a separate line with a separate color and the projected data for that volume category is displayed in a lighter color.

The Volume Trend Report can be further expanded to display more detailed information. You can click on a sample point along the line chart to show the details of that time period. This drill-down report includes the node names, along with the associated mounting points, volume size, used space, free space, and used space percentage. You can also select different volume combinations to display their accumulated size trends.



Chapter 7: Troubleshooting Dashboard

This section contains the following topics:

Troubleshooting Overview (see page 225)
Dashboard Troubleshooting (see page 225)

Troubleshooting Overview

When a problem is detected, Dashboard will display a pop-up message to help you identify and quickly resolve the problem.

Dashboard Troubleshooting

This section explains the most common Dashboard troubles, along with the reason and solution.

Email notifications not being sent

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

1. Verify the Arcserve Backup services are running and restart if necessary. For more information about 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 24).
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 Arcserve 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 Arcserve Backup Dashboard does not display any data, perform the following troubleshooting procedure:

Note: Dashboard can only monitor and report on nodes that have 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 Arcserve Backup r12.5 agent.
2. Verify the Arcserve Backup services are running and restart if necessary. For more information about 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 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 Arcserve support.

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

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

1. If you have not restored the Arcserve Backup Database, make sure that you specify to include the "Preserve current ARCserve Domain Memberships" option as follows to avoid this problem:

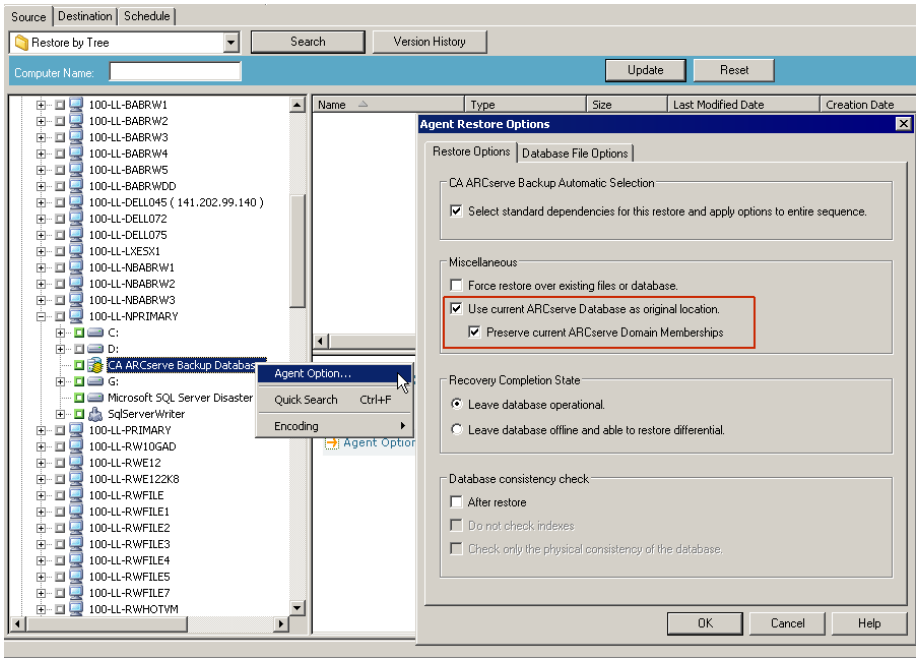
   a. From the Restore Manager, select the Arcserve Backup Database to be restored.

   b. Right-click and from the pop-up menu, select Agent Option.

      The Agent Restore Options dialog appears.

   c. Right-click and from the pop-up menu, select Agent Option.

   d. 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 Arcserve Backup Database (and if the "Preserve current ARCserve Domain Memberships" option is not selected), you need to enter the Arcserve Backup Database credentials using Server Configuration Wizard as follows:
   a. Close 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 Arcserve Backup Manager, and launch Dashboard.

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

If the 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 Arcserve Backup. During the installation of 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 Arcserve 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 Arcserve Backup. During the installation of 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 Arcserve 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 Arcserve Backup is aware that this node exists.
   b. Check if 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 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 Arcserve Technical Support for investigation.

   For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Arcserve 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 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 Arcserve Backup server.

SRM probe dialog displays "Service not ready" message

This is because the SRM Prober 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 an SRM probe again.
2. If the problem persists, contact Arcserve support for online technical assistance and a complete list of locations, primary service hours, and telephone numbers.

Chapter 8: Troubleshooting Global Dashboard

This section contains the following topics:

Troubleshooting Overview (see page 233)
Global Dashboard Troubleshooting (see page 233)

Troubleshooting Overview

When a problem is detected, Global Dashboard generates a message to help you identify and resolve the problem. These messages are contained in the Global Dashboard activity logs.

There are two types of activity logs for Global Dashboard. The Central Primary Server activity log displays errors that are encountered during the receiving of data by the central site. The Branch Primary Server activity log displays errors that are encountered during the transmitting of data by the branch site.

- To view the Central Primary Server activity log, access the Central Manager and click "Log Messages" to display the corresponding central site messages.
- To view the Branch Primary Server activity log, access the Branch Manager and click "Show More…" to open the Alert and Error Message window and display the corresponding branch site messages.

In addition, when an incorrect action is attempted, Global Dashboard will generally display a pop-up message to help you identify and quickly resolve the problem.

Global Dashboard Troubleshooting

This section explains the most common Global Dashboard troubles, along with the reason and solution.

"System Out Of Memory Exception" error occurred

In the Branch Manager UI, you receive the following message in the log: System.OutOfMemoryException

Reason:

During incremental data synchronization, there is large number of records to synchronize from the branch site to the central site. If the system memory on the Branch Primary Server is low, this error may occur.

Action:

- At the central site, access the Arcserve Backup home directory and open the CentralConfig.xml file from the GlobalDashboard folder.
- Locate the "<MaxTransactEveryTime>800</MaxTransactEveryTime>" parameter and reduce the value of transactions from 800 (default) to lower number (perhaps 400).
- Save the changes and restart Arcserve Central Remoting Server service at the central site.

"Broken database schema for branch site" error occurred

At the the Branch Manager UI, you receive the following warning message:

"Database schema for this Branch Primary Server was broken and needs full data synchronization. Do you want to perform a full data synchronization now?"

Reason:

You have initialized, restored, or changed the Arcserve Backup database on the branch site.

Action:

- Click Yes to perform the full data synchronization and specify the details for the Central Primary Server.
- If problem persists, uninstall and reinstall Global Dashboard from your branch site.

"Central Primary Server is busy" error occurred

During full synchronization of data from the branch site to the central site, you receive the following warning message:

"Central Primary Server is busy. Click Retry to attempt to register again or click Cancel to cancel the installation process."

Reason:

The Central Primary Server is currently unable to accept a connection from this branch site. This could be because of any of the following conditions:

- Insufficient resources (CPU, memory, or so on) on the Central Primary Server.
- The specified value for the maximum concurrent connections parameter is set too low on the Central Manager.
- The SQL Server on the central site entered into a deadlock condition.

Action:

- Wait for few minutes and click Retry.
- If the problem persists, at the central site change the value of Maximum Concurrent Connections to a higher value and then at the branch site click Retry in the warning message. For more information about the Maximum Concurrent Connection settings, see Understanding Central Manager (see page 66).

General Error During Full Data Synchronization

During full synchronization of data from a branch site to the central site, you receive the following error message:

"General Error! Contact the central administrator!"

Reason:

SQL Server service is not running on the central site during the full data synchronization process.

Action:

Ensure that the SQL Server service and all Arcserve Backup services are running at the central site, then reattempt to perform a full data synchronization from the branch site.

"Attempt to start Data synchronization service failed!" error occurred

At the Branch Manager UI, you receive the following warning message:

"Attempt to start Data synchronization service failed!"

Reason:

When a Branch site has a newer version of Arcserve Backup than the corresponding Central Primary Server or the Central Primary Server is not online.

Action:

- Verify that the Central Primary Server is online.
- Verify that the status of the "CA ARCserve Dashboard Sync Service" is not "Disabled". If so, change the status to "Automatic" on the branch site and then perform a full data synchronization.
- Verify that the version of Arcserve Backup for the Central Primary Server is the same or a newer version than the Branch Primary Server.
- If problem persists, uninstall and reinstall Global Dashboard from your branch site.

"Branch name already exists" error occurred

During full synchronization of data from the branch site to the central site, you receive the following warning message:

"Branch name [name of branch] already exists in the Central Primary Server. The following name [name of branch_1] is suggested to be used as the new Branch name. Do you want to continue with the new Branch name?"

Reason:

- You inadvertently assigned a duplicate branch site name.
- You tried to reinstall Global Dashboard from the branch site and then attempted a full data synchronization to the old central site.

Action:

- Assign a different name to the duplicate branch site name.
- At the central site, open the Central Manager UI and delete the duplicate branch site name that was registered earlier. For more information about deleting branch names, see Understanding Central Manager (see page 66).
- At the branch site, click No in the warning message and manually initiate a full data synchronization again by clicking 'Synchronize' button in Branch Manager UI. For more information, see Manually Synchronize Data (see page 90).

"Service Communication Failure" occurred

When you launch Global Dashboard, you receive the following error message:

"Communication with the Arcserve Backup Server can be established, but unable to communicate with CA ARCserve Communication Foundation (Global) Service. Please make sure that the CA ARCserve Communication Foundation (Global) Service is up and running."

Reason:

- At the central site, the Arcserve Communication Foundation (Global) Service is not running
- At the central site, the SQL Server service is not running.
- You are trying to connect to the Central Primary Server through a remote Arcserve Backup Manager and a network connectivity problem exists.

Action:

- Verify all services are running.
- Verify a valid network connection exists between the Central Primary Server and the remote Arcserve Backup Manager.

"Central Site Connection Failure" occurred

While attempting data synchronization, you receive the following message:

"A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond"

Reason:

The network connection from the central site is broken.

Action:

- Verify proper network connection at the central site. If a broken network connection is discovered and fixed, Global Dashboard will then attempt to automatically recover and immediately perform an incremental data synchronization.
- If the problem persists, notify the central site administrator to resolve the network problem.

ASDB Connection Failure

When you try to open a report you receive the following error message, but you know the SQL Service is running and the Arcserve Backup database (ASDB) is online:

"Unable to connect to ASDB Database. Please make sure that SQL SERVICE is running and ASDB database is ONLINE"

Reason:

Microsoft SQL server is reusing the cached query plan, but the query plan is poor.

Action:

On the central database machine, open SQL Server Management Studio and run the following command:

dbcc freeproccache

Synchronization Fails Due to Insufficient Free Disk Space

Valid on Windows platforms.

Symptom:

The process of synchronizing the Central Primary Server with Branch Primary Servers fails. Arcserve Backup displays a message indicating that the branch configuration file is damaged and to reinstall the Branch Primary Server.

Solution:

The process of synchronizing the Central Primary Server with Branch Primary Servers fails when there is insufficient free disk space on Central Primary servers. The lack of free disk space prevents Arcserve Backup from saving the Central Primary Server and Branch Primary Server configuration files.

To correct this problem, free disk space on the Central Primary Server and then configure Dashboard using Server Configuration Wizard. The corrective action is as follows:

1. Log in to the Arcserve Backup Central Primary Server and delete the following configuration file:

   `$BAB_HOME\GlobalDashboard\Config.xml`

2. Open Windows Server Manager (Windows Server 2008) or Windows Computer Management (Windows Server 2003).

   Stop the following service:

   `Arcserve Dashboard Sync Service`

3. Delete unnecessary files from the Central Primary Server to free disk space.
4. Start Arcserve Backup Server Configuration Wizard by clicking Start, All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

   On the Select Options dialog, click Configure Global Dashboard and then click Next.

   Note: If you cannot start Server Configuration Wizard, open Branch Manager by clicking Start, All Programs, CA, ARCserve Backup, and click Branch Manager.

   The Select which Primary Server type you want to configure dialog opens.
5. Click Configure as the Central Primary Server and click Next.

   Follow the prompts and complete the required fields to complete the configuration.
6. (Optional) After the configuration is complete, open Windows Server Manager (Windows Server 2008) or Windows Computer Management (Windows Server 2003) and verify that Arcserve Dashboard Sync Service is running.

You should now be able to synchronize the Central Primary Server with Branch Primary Servers successfully.

Glossary

Branch Primary Server

A server that synchronizes and transmits dashboard-related information to the designated Central Primary Server.

branch view

Displays the dashboard-related information for only the local server, without any other branch site details or global dashboard options.

Central Primary Server

The central hub interface for storing synchronized dashboard-related information received from associated Branch Primary Servers.

Dashboard

A user interface tool that provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment.

Dashboard Group

A collection of one or more Dashboard reports.

data synchronization

The process of transmitting dashboard-related information from a branch site database to the central site database so that the central database contains (and reports) the same information as each of the registered branch databases.

Global Dashboard

A user interface tool that provides you a single snapshot overview of dashboard information for multiple Arcserve Backup primary servers, both in your main office and in remote offices, all from a central location.

global view

Displays the dashboard-related information for the local server and also for any or all branch sites.

node tier

Specifies the priority level category (high, medium, or low) for filtering displayed information of monitored nodes.

SRM Prober

A data-collection utility that when invoked, probes or communicates with all machines in your storage environment to collect SRM-related data for the SRM-type reports.

Index

A

add a Dashboard Group • 59
add new branch group • 86
add new email schedule • 25
advanced settings
    Central Primary Server Port • 80
    DB Connection Timeout • 80
    Maximum Concurrent Connections • 80
    understanding • 80
Agent Distribution Report • 100
    drill down reports • 103
    report benefits • 101
    report view • 102
agent upgrade alert • 64
Application Data Trend Report • 104
    report benefits • 105
    report view • 105
Arcserve Backup Dashboard
    email reports • 24
    global options • 19
    graphical displays • 15
    groups • 57
    GUI • 14
    introduction • 11
    report types • 98
    reports • 98
    report-specific options • 31

B

Backup Data Location Report • 106
    drill down reports • 108
    report benefits • 107
    report view • 108
Backup Server Load Distribution Report • 109
    report view • 110
bar chart overview • 15
Branch Configuration dialog • 76
branch groups
    add new branch group • 86
    delete branch group • 87
    modify branch group • 87
Branch Primary Server • 36
branch site
    Branch Configuration dialog • 76
    configure • 71, 76
    delete • 71, 76
    refresh • 71, 76
    resume • 71, 76
    save • 71, 76
    services • 38
    status • 71, 76
    suspend • 71, 76
branch site configuration • 49

C

Central Manager
    advanced settings • 80
    branch management • 71, 76
    definition • 36
    log messages • 78
    understanding • 66, 71, 76, 78, 80
Central Primary Server • 36
central site configuration • 46
collapse report view • 15
configure
    branch site • 49
    central site • 46
    general • 44, 46, 49
configure email reports • 24
configure SRM • 33
CPU Report • 116
    drill down reports • 119
    report benefits • 117
    report view • 118
CPU Utilization Report • 189
    report benefits • 190
    report view • 191
cursor overview • 15
customize reports • 18

D

Dashboard Groups • 57
    add • 59
    delete • 61
    modify • 60
Data Distribution on Media Report • 120
    drill down reports • 122
    report benefits • 120
    report view • 121

data exporting • 202
data sorting • 202
data synchronization
    automatic • 89
    definition • 36
    manual • 90
    retry attempts • 76
    retry interval • 76
    schedule time • 76
data synchronization service • 81
db connection timeout • 80
Deduplication Benefits Estimatie Report • 122
    report benefits • 122
    report view • 124
Deduplication Status Report • 124
    drill down reports • 127
    report benefits • 125
    report view • 126
delete a Dashboard Group • 61
delete branch group • 87
Disk Protection Report • 189
    report benefits • 190
    report view • 192
Disk Report • 128
    drill down reports • 130
    report benefits • 128
    report view • 128
drill down reports • 99
    Agent Distribution Report • 103
    Backup Data Location Report • 108
    CPU Report • 119
    Data Distribution on Media Report • 122
    Deduplication Status Report • 127
    Disk Report • 130
    Job Archive Status Report • 133
    Job Backup Status Report • 139
    Media Assurance Report • 145
    Memory Report • 148
    Network Report • 151
    Node Archive Status Report • 154
    Node Backup Status Report • 159
    Node Disaster Recovery Report • 163
    Node Encryption Status Report • 166
    Node Recovery Point Report • 171
    Node Tiers Report • 176
    Node Whose Most Recent Backup Failed Report • 180
    Recovery Point Objective Report • 185
    SCSI/Fiber Card Report • 189
    Software Installed on Client Node Report • 116
    Tape Encryption Status Report • 198
    Top Nodes with Failed Backups Report • 203
    Virtual Machine Recovery Point Report • 214
    Virtualization Most Recent Backup Status Report • 218
    Volume Report • 222
    Volume Trend Report • 222, 223

E

email scheduling • 19, 24
email scheduling status • 30
expand report view • 15

F

failed node backups • 202
fastest backup nodes • 205
features • 13, 36
flow diagram • 40

G

Global Dashboard Branch Site Configuration dialog • 81
Global Dashboard Console
    definition • 36
Global Dashboard services • 38
global options • 19
graphical displays • 15
GUI • 14

H

how it works • 40

I

installation
    preinstallation considerations • 43
Introduction • 11, 35

J

Job Archive Status Report • 131
    drill down reports • 133
    report benefits • 131
    report view • 132
Job Backup Status Report • 135
    drill down reports • 139
    report benefits • 136
    report view • 136

L

License Report • 141
report benefits • 141
report view • 142
log messages • 24, 78

M

manually configure branch site • 90
manually synchronize data • 90
maximum concurrent connections • 80
Media Assurance Report • 143
drill down reports • 145
report benefits • 143
report view • 143
Memory Report • 145
drill down reports • 148
report benefits • 146
report view • 147
Memory Utilization Report • 189
report benefits • 190
report view • 193
messages • 78
modify a Dashboard Group • 60
modify branch group • 87

N

Network Report • 149
drill down reports • 151
report benefits • 149
report view • 149
Network Utilization Report • 189
report benefits • 190
report view • 195
Node Archive Status Report • 151
drill down report • 154
report benefits • 152
report view • 152
Node Backup Status Report • 155
drill down reports • 159
report benefits • 156
report view • 156
Node Encryption Status Report • 164
drill down reports • 166
report benefits • 165
report view • 165
node information window • 62
Node Recovery Point Report • 168
drill down reports • 171
report benefits • 169
report view • 170
Node Summary Report • 172
report benefits • 173
report view • 174
node tiers • 61
Node Tiers Report • 175
drill down reports • 176
report benefits • 175
report view • 176
Node Whose Last Backup Failed Report • 178
drill down reports • 180
report benefits • 178
report view • 178

O

options • 31
OS Report • 181
report benefits • 181
report view • 182
overall • 11

P

pie chart overview • 15
pki reports • 189, 190, 191, 192, 193, 195
port number • 80
preinstallation considerations • 43

R

Recovery Point Objective Report • 183
drill down reports • 185
report benefits • 183
report view • 185
report types • 98
backup environment • 98
drill down • 99
SRM • 99
reports • 98
Agent Distribution Report • 100
Application Data Trend Report • 104
Backup Data Location Report • 106
Backup Server Load Distribution Report • 109
collapse view • 13
CPU Report • 116
CPU Utilization • 190
Data Distribution on Media Report • 120
Deduplication Benefits Estimate Report • 122

Deduplication Status Report • 124
Disk Protection Report • 190, 192
expand view • 13
Fiber Card Report • 186
Job Archive Status Report • 131
Job Backup Status Report • 135
License Report • 141
Media Assurance Report • 143
Memory Report • 145
Memory Utilization Report • 190, 193
Network Report • 149
Network Utilization Report • 190, 195
Node Archive Status Report • 151
Node Backup Status Report • 155
Node Encryption Status Report • 164
Node Recovery Point Report • 168
Node Summary Report • 172
Node Tiers Report • 175
Node Whose Most Recent Backup Failed Report • 178
OS Report • 181
Recovery Point Objective Report • 183
reports, Disk Report • 128
Software Installed on Client Node • 113, 116
SRM PKI • 189, 190, 191, 192, 193, 195
Tape Encryption Status Report • 196
Top Nodes with Failed Backups Report • 200
Top Nodes with Fastest/Slowest Backup Throughputs Report • 204
Top Nodes with Largest Unchanged Files Report • 206
Total Archive Status Report • 207
types • 98
Utilization Reports • 189, 190
Virtual Machine Recovery Point Report • 211
Virtualization Most Recent Backup Status Report • 215
Volume Report • 218
Volume Trend Report • 222, 223
retry attempts • 76
retry interval • 76
ROBO • 35

S

scheduling emails • 19, 24
SCSI/Fiber Card Report • 186
drill down reports • 189
report benefits • 187
report view • 187
services • 38
slowest backup nodes • 205
Software Installed on Client Node Report • 113, 116
drill down report • 116
report benefits • 113
report view • 113
SRM PKI reports • 189, 190, 191, 192, 193, 195
SRM probe settings • 33
SRM prober • 33
SRM reports • 99
synchronize data
automatic • 89
manual • 90
retry attempts • 76
retry interval • 76
schedule time • 76
services • 38

T

Tape Encryption Status Report • 198
drill down reports • 198
report benefits • 197
report view • 197
throughputs • 205
time zone • 71, 76
Top Nodes with Failed Backups Report • 200
drill down reports • 203
report benefits • 201
report view • 202
Top Nodes with Fastest/Slowest Backup Throughputs Report • 204
report benefits • 204
report view • 205
Top Nodes with Largest Unchanged Files Report • 206
report benefits • 206
report view • 206
Total Archive Status Report • 207
report benefits • 208
report view • 209
tracking email schedule status • 30

U

understanding
Central Manager • 66, 71, 76, 78, 80

V

Virtual Machine Recovery Point Report • 211
drill down reports • 214
report benefits • 212
report view • 213
Virtualization MostRecent Backup Status Report • 215
drill down reports • 218
report view • 216
reports benefit • 215
Volume Report • 218
drill down reports • 222
report benefits • 219
report view • 219
Volume Trend Report • 223
report benefits • 223
report view • 223