CA ARCserve® Central Reporting

User Guide

r16

CA Technologies Product References

This document references the following CA Technologies products:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Contact CA

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Support Links for CA ARCserve Central Applications:

CA Support Online offers a rich set of resources for resolving your technical issues and provides easy access to important product information. With CA Support, you have easy access to trusted advice that is always available. The following links let you access the various CA Support sites that are available:

- **Understanding your Support--**The following link provides information about maintenance programs and support offerings, including terms and conditions, claims, service-level objectives (SLO), and service hours.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registering for Support--**The following link takes you to the CA Support Online registration form which is used to activate your product support.

  https://support.ca.com/prodinfo/supportregistration

- **Accessing Technical Support--**The following link takes you to the One-Stop Product Support page for CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Documentation Changes

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

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

Update 6

- Updated Alert Report View (see page 36). Updated this topic to include two new Event Types: Skip/Merge job waiting in the job queue and Discovery.

Update 4

- Removed the Silent Installation Product Codes subtopic and included the information in the Install CA ARCserve Central Reporting Silently (see page 17) topic.
- Removed graphics from the topic Schedule Reports by Email (see page 88). Added information that describes the tabs.
- Added Change Server Communication Protocol (see page 92). This topic describes how to change the communication protocol used by the CA ARCserve Central Applications components from HTTP to HTTPS and from HTTPS to HTTP using a batch file.

Contents

Chapter 1: Introducing CA ARCserve Central Reporting

This section contains the following topics:

Introduction

CA ARCserve Central Applications combine core data protection and management technologies with an ecosystem of targeted applications that work in unison to facilitate on- and off-premises protection, copy, movement, and transformation of data across global environments.

CA ARCserve Central Applications are easy to use, manage, and install. It provides organizations with automated control of their information to make educated decisions about the access, availability, and security of their data, based on the overall business value.

Among the applications offered by CA ARCserve Central Applications, the reporting feature is managed by CA ARCserve Central Reporting. The reporting application lets you centrally view reports and administer managed devices, settings, and policies that run on or off premise.

CA ARCserve Central Reporting provides an enhanced capability to drill down into each report to display more detailed information.

Reporting Features

CA ARCserve Central Reporting contains the following reporting features:

- Provides a central snapshot overview of your backup infrastructure and your storage resource management (SRM) environment for all registered nodes

- Provides node details including hardware and software with data size trending
- Provides SRM Performance Key Indicator (PKI) that lets you monitor the performance of the agents running in your backup environment

  SRM PKI measures the following performance indicators:

  - CPU usage
  - Memory usage
  - Disk throughput
  - Network input and output

  Note: For more information about enabling and disabling SRM, refer to the CA ARCserve Central Protection Manager guide.
- Provides various report alerts
- Provides Node Backup status
- Provides Node Archive and File Copy Status
- Provides the last successful date and time of the job
- Provides the recovery point that includes encryption and compression status
- Provides Backup size trending
- Provides report filtering capability to limit the data being displayed in the report, based upon specified parameters
- 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 customized schedules for sending reports by email to specified recipients
- Provides central overview for the most recent backup status of your virtual machines
- Provides the ability to view your current time zone

  (The time zone can be viewed at the top right corner of the application.)

How CA ARCserve Central Reporting Works

CA ARCserve Central Reporting provides a list of reports where you can generate data and view the reports as a chart view or table view. For the chart view, it can be pie, bar, or line chart. In addition, some of the reports have an enhanced capability to drill down into the report to display more detailed information.

Start CA ARCserve Central Reporting by clicking the Windows Start menu and selecting All Programs, CA, ARCserve Central Applications, Reporting.

CA ARCserve Central Reporting can also be accessed from a remote computer using the following URL:

http://<CA ARCserve Central Application Server Name>:<Port Number>/reporting/

The CA ARCserve Central Reporting home page appears where you can access any reporting function using the following navigational features:

- **Dashboard**--Provides an overview of all CA ARCserve Central Applications infrastructure and their storage resource management (SRM) environment.
- **Configuration--**Lets you configure the settings for Protection Manager Configuration, Email Configuration, Update Configuration, and Preferences Configuration.
- **View Logs--**Lets you view logs of activities for each individual node. It displays all log messages associated with that node. You can filter the list by specifying the severity of the messages displayed (All, Information, Errors, Warnings, or Errors and Warnings), the type of module (All, Common, Email, Email Scheduler, or Updates), or the node name.

CA ARCserve Central Applications Bookshelf

The topics contained in the CA ARCserve Central Applications Help system are also available as a User Guide in PDF format. The latest PDF version of this guide and Help System can be accessed from the CA ARCserve Central Applications Bookshelf.

The CA ARCserve Central Applications Release Notes files contain information relating to system requirements, operating system support, application recovery support, and other information you may need to know before installing this product. In addition, the Release Notes files contain a list of known issues that you should be aware of before you use CA ARCserve Central Applications. The latest version of the Release Notes can be accessed from the CA ARCserve Central Applications Bookshelf.

Chapter 2: Installing CA ARCserve Central Reporting

This section contains the following topics:

Prerequisite Installation Tasks

Before you install the application, complete the following prerequisite tasks:

- Review the Release Notes. The Release Notes contain a description of system requirements, supported operating systems, and a list of issues known to exist with this release of the application.
- Verify that your system meets the software and hardware requirements that are needed to install the application.
- Verify that your Windows account has administrator privileges or any other equal privileges to install software on the computers where you plan to install CA ARCserve Central Reporting.
- Verify that you have the user names and passwords of the computers where you are installing the application in your possession.
- CA ARCserve Central Reporting application relies on the database configured in CA ARCserve Central Protection Manager. Confirm that the CA ARCserve Central Protection Manager details are correctly configured in order for CA ARCserve Central Reporting to work.

Installation Considerations

Before you install CA ARCserve Central Reporting, review the following installation considerations:

- The CA ARCserve Central Applications installation package installs a module named CA ARCserve Central Applications Server. The server is a module that is common to all applications. The module contains the web service, binaries, and configurations that let the application communicate with each other.

  When you install the application, the installation package installs the CA ARCserve Central Applications Server module before installing the product components. If it becomes necessary to apply a patch to the application, the patch updates the module before updating the product components.

Install CA ARCserve Central Reporting

The installation wizard helps guide you through the process of installing one or more CA ARCserve Central Applications.

Note: Before you install an application, review the Release Notes file and verify that all of the tasks described in Prerequisite Installation Tasks (see page 13) are complete.

To install CA ARCserve Central Reporting

1. Download the CA ARCserve Central Applications installation package to the computer where you want to install the application, and then double-click the Setup file.

   The installation package extracts its contents to your computer and then the Prerequisite Components dialog opens.

2. Click Install on the Prerequisites Components dialog.

   Note: The Prerequisite Components dialog opens only if Setup does not detect that the required prerequisite components are installed on your computer.

   After Setup installs the prerequisite components, the License Agreement dialog opens.

3. Complete the required options on the License Agreement dialog and click Next.

   The Configuration dialog opens.

4. On the Configuration dialog, complete the following:

   - **Components--**Specify the applications that you want to install.

     Note: If you are installing this application using the suite installation package, you can install multiple applications.

   - **Location--**Accept the default installation location or click Browse to specify an alternative installation location. The default location is as follows:

     C:\Program Files\CA\ARCserve Central Applications

   - **Disk Information--** Verify that your hard drive has sufficient free disk space to install the applications.

   - **Windows Administrator Name--**Specify the user name of the Windows Administrator account using the following syntax:

     Domain\User Name

   - **Password--**Specify the password for the user account.

   - **Specify Port Number--**Specify the port number that you want to use to communicate with the web-based user interface. As a best practice, you should accept the default port number. The default port number is as follows:

     8015

     Note: If you want to specify an alternative port number, the available port numbers are from 1024 through 65535. Before you specify an alternative port number, verify that the specified port number is free and available for use. Setup prevents you from installing the application using a port that is not available for use.

   - **Use HTTPS for web communication--**Specify to use HTTPS communication for data transmission. By default, this is not selected.

     Note: HTTPS (secure) communication provides a higher level of security than HTTP communication. HTTPS is recommended communication protocol if you transmit confidential information in your network.

   - **Allow Setup to register CA ARCserve Central Applications services and programs to the Windows Firewall as exceptions--**Verify that the check box next to this option is selected. Firewall exceptions are required if you want to configure and manage CA ARCserve Central Applications from remote computers.

     Note: For local users, you do not need to register firewall exceptions.

   Click Next.

   The Application Settings dialog opens.

5. Complete the following fields on the Application Settings dialog:

   Note: The values specified on the Application Settings dialog let CA ARCserve Central Reporting retrieve information from the computer where CA ARCserve Central Protection Manager is installed to create reports.

   - **CA ARCserve Central Protection Manager Server--**Specify the Host Name of the computer where the Protection Manager application is installed.
   - **User Name--**Specify the User Name that is required to log in to the computer where the Protection Manager application is installed.
   - **Password--**Specify the password for the user.
   - **Port--**Specify the port number that you must use to communicate with the CA ARCserve Central Protection Manager user interface.
   - **Connection type--**Select the connection type based on the connection configured in CA ARCserve Central Protection Manager:
     - **HTTP--**Specifies an unsecured connection.
     - **HTTPS--**Specifies a secured connection.
   - **I will configure this later--**Lets you configure the application settings after the installation process is complete.

   Click Next.

   After the installation process is complete, the Installation Report dialog opens.

6. The Installation Report dialog summarizes the installation. If you want to check for updates to the application now, click Check for updates and then click Finish.

The application is installed.

Uninstall CA ARCserve Central Reporting

You can uninstall the application using Programs and Features located in Windows Control Panel.

To uninstall CA ARCserve Central Reporting

1. From the Windows Start menu, click Start and click Control Panel.

   Windows Control Panel opens.

2. From Windows Control Panel, click the drop-down list next to View by and then click Large icons or Small icons.

   The icons for the Windows Control Panel applications appear in a grid layout.

3. Click Programs and Features.

   The Uninstall or change a program window opens.

4. Locate and click the application that you want to uninstall.

   Right-click the application and click Uninstall on the pop-up menu.

   Follow the on-screen instructions to uninstall the application.

The application is uninstalled.

Install CA ARCserve Central Reporting Silently

CA ARCserve Central Applications lets you install CA ARCserve Central Reporting silently. A silent installation eliminates the need for user interaction. The following steps describe how to install the application using Windows Command Line.

To install CA ARCserve Central Reporting silently

1. Open the Windows Command Line on the computer where you want to start the silent installation process.
2. Download the CA ARCserve Central Applications self-extracting installation package to your computer.

   Start the silent installation process using the following Command Line syntax:

   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR> -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"

Usage:

s

Lets you run the executable file package in silent mode.

v

Lets you specify additional command line options.

q

Lets you install the application in silent mode.

-Path:<INSTALLDIR>

(Optional) Lets you specify the target installation path.

Example:

-Path:\"C:\Program Files\CA\ARCserve Central Applications\"

Note: If the value for INSTALLDIR contains a space, enclose the path with backslashes and quotation marks. Additionally, the path cannot end with a backslash character.

-Port:<PORT>

(Optional) Lets you specify the port number for communication.

Example:

-Port:8015

-U:<UserName>

Lets you specify the user name to use to install and run the application.

Note: The user name must be an administrative account or an account with administrative privileges.

-P:<Password>

Lets you specify the password for UserName.

-Products:<ProductList>

(Optional) Lets you specify CA ARCserve Central Applications to install silently. If you do not specify a value for this argument, the silent installation process installs all components of CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

All CA ARCserve Central Applications

ALL

Note: The following examples describe the syntax that is required to install one, two, three, or all CA ARCserve Central Applications silently:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

The application is installed silently.

Uninstall CA ARCserve Central Reporting Silently

CA ARCserve Central Applications lets you uninstall CA ARCserve Central Reporting silently. A silent uninstallation eliminates the need for user interaction. The following steps describe how to uninstall the application using Windows Command Line.

To uninstall CA ARCserve Central Reporting silently

1. Log in to the computer where you want to uninstall the application.

   Note: You must log in using an administrative account or an account with administrative privileges.

2. Open the Windows Command Line and execute the following command to start the silent uninstallation process:

   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>

   Or,

   <INSTALLDIR>%\Setup\uninstall.exe /q /ALL

   Example: The following syntax lets you uninstall CA ARCserve Central Reporting silently.

   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

   Usage:

   <INSTALLDIR>

   Lets you specify the directory where the application is installed.

   Note: Execute the syntax that corresponds with the architecture of the operating system on the computer.

   <ProductCode>

   Lets you specify the application to uninstall silently.

   Note: The silent uninstallation process lets you install one or more CA ARCserve Central Applications. Use the following product codes to uninstall CA ARCserve Central Applications silently:

   CA ARCserve Central Host-Based VM Backup

   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

   CA ARCserve Central Protection Manager

   {CAED05FE-D895-4FD5-B964-001928BD2D62}

   CA ARCserve Central Reporting

   {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

   CA ARCserve Central Virtual Standby

   {CAED4835-964B-484B-A395-E2DF12E6F73D}

The application is uninstalled silently.

Chapter 3: Getting Started With CA ARCserve Central Reporting

The following sections describe how to configure CA ARCserve Central Reporting.

This section contains the following topics:

Configure the CA ARCserve Central Protection Manager Server

The CA ARCserve Central Protection Manager Configuration module lets you connect to the CA ARCserve Central Protection Manager machine and port to retrieve database information for your reports.

Follow these steps:

1. Log in to the CA ARCserve Central Reporting server and click Configuration on the Navigation bar to open the Configuration screen.
2. From the Configuration panel, click CA ARCserve Central Protection Manager Configuration.
3. Complete the following fields:
   - **CA ARCserve Central Protection Manager Server**

     The following fields default to the values configured in the CA ARCserve Central Protection Manager server:

- **Machine Name**--The Host Name of the computer where CA ARCserve Central Protection Manager is installed.
- **User Name**--The User Name that is required to log on to the computer where CA ARCserve Central Protection Manager is installed.
- **Password**--The password for the user.
- **Port**--The port number that you must use to communicate with the CA ARCserve Central Protection Manager Web Service.
- **HTTPS**--This option is checked or unchecked based on the connection configured in the CA ARCserve Central Protection Manager server.

- **Detect Port and Protocol Automatically**--Lets you obtain the CA ARCserve Central Protection Manager Port and Protocol of the Protection Manager database and populates the fields above.

  Note: This option is enabled only if the remote registry access of the CA ARCserve Central Protection Manager server is allowed.

  To verify if the remote registry is allowed or not, go to the CA ARCserve Central Protection Manager server where CA ARCserve Central Protection Manager is installed, navigate to services.msc, verify that the 'Remote Registry' service has started and set to 'Automatic'.

- **Test--**Lets you verify that the access information for the CA ARCserve Central Protection Manager is correct.

4. Click Save.

Be aware of the following:

- The access information for the CA ARCserve Central Protection Manager database is stored on the CA ARCserve Central Reporting server which will then connect to this database and display its data in the reports.
- If the port, protocol, credentials, or database settings are changed in CA ARCserve Central Protection Manager, then it is required that you update the CA ARCserve Central Reporting configuration settings to match what was changed in CA ARCserve Central Protection Manager.
- If CA ARCserve Central Protection Manager and CA ARCserve Central Reporting applications are installed on the same server and are using the default settings during the installation, it is not required to configure the CA ARCserve Central Protection Manager server.

Configure Email Settings

You can configure email settings for use with your application to send alerts automatically under conditions you specify.

Follow these steps:

1. Log in to the application.

   From the Navigation bar on the home page, click Configuration to open the Configuration screen.

2. From the Configuration panel, click Email Configuration to display the Email Configuration options.

3. Complete the following fields:

   - **Service**--Specify the type of email service from the drop-down. (Google Mail, Yahoo Mail, Live Mail or Other).
   - **Mail Server**--Specify the host name of the SMTP server that you want CA ARCserve Central Applications to use to send email.
   - **Requires Authentication**--Select this option when the mail server that you specified requires authentication. The Account Name and Password are required.
   - **Subject**--Specify a default email subject.
   - **From**--Specify the email address the email is being sent from.
   - **Recipients**--Specify one or more email addresses, separated by a semicolon(;), the email is being sent to.
   - **Use SSL**--Select this option if the mail server you specified requires secure connection (SSL).
   - **Send STARTTLS**--Select this option if the mail server you specified requires STARTTLS command.
   - **Use HTML format**--Lets you send the email messages in HTML format. (selected by default)
   - **Enable Proxy Settings**--Select this option if there is a proxy server and then specify the proxy server settings.

4. Click Test Email to verify that the mail configuration settings are correct.

5. Click Save.

   Note: You can click Reset to revert to the previously saved values.

The email configuration is applied.

Configure Update Schedules

The application lets you set up a schedule that automatically downloads product updates from a CA Server or a local software staging server.

To configure update schedules

1. Log in to the application.
2. Click Configuration on the Navigation bar to open the Configuration screen.
3. From the Configuration panel, click Update Configuration.

   The update configuration options appear.
4. Select a Download Server.
   - **CA Server**--Click Proxy Settings for the following options:
     - **Use browser proxy settings--**Lets you use the credentials that provided for the browser proxy settings.

       Note: The Use browser proxy settings option affects Internet Explorer and Chrome.
     - **Configure proxy settings**--Specify the IP Address or Host Name of the proxy server and the port number. If the server you specified requires authentication, click Proxy server requires authentication and provide the credentials.

       Click OK to return to Update configuration.
   - **Staging Server--**If you select this option, click Add Server to add a staging server to the list. Enter its host name and Port number and click OK.

     If you specify multiple staging servers, the application tries to use the first server listed. If connection succeeds, the remaining servers listed are not used for staging.
5. (Optional) Click Test Connection to verify the server connection and wait until the test completes.
6. (Optional) Click Automatically check for updates, and then specify the day and time. You can specify a daily or weekly schedule.

Click Save to apply the Update configuration.

Configure Proxy Settings

CA ARCserve Central Applications let you specify a proxy server to communicate with CA Support to check for and download available updates. To enable this capability, you specify the proxy server that you want to communicate in behalf of the CA ARCserve Central Applications server.

Follow these steps:

1. Log in to the application and click Configuration on the Navigation bar.

   The Configuration options appear.

2. Click Update Configuration.

   The update configuration options display.

3. Click Proxy Settings.

   The Proxy Settings dialog opens.

4. Click one of the following options:

   - **Use browser proxy settings--**Lets the application detect and use the same proxy settings that are applied to the browser to connect to the CA Technologies server for update information.

     Note: This behavior applies to only Internet Explorer and Chrome browsers.

   - **Configure proxy settings--**Lets you define an alternative server that the application will use to communicate with CA Support to check for updates. The alternative server (proxy) can help ensure security, increased performance, and administrative control.

     Complete the following fields:

     - **Proxy Server--**Specify the host name or IP address of the proxy server.
     - **Port--**Specify the port number that the proxy server will use to communicate with the CA Support website.
     - **(Optional) Proxy server requires authentication--**If the login credentials for the proxy server are not the same as the credentials for the CA ARCserve Central Applications server, click the check box next to Proxy server requires authentication and specify the User Name and Password that is required to log in to the proxy server.

       Note: Use the following format to specify the user name: <domain name>/<user name>.

   Click OK.

The proxy settings are configured

Configure Social Networking Preferences

CA ARCserve Central Applications let you manage the social networking tools that can help you manage each application. You can generate news feeds, specify links to popular social networking websites, and select video source websites.

To configure social networking preferences

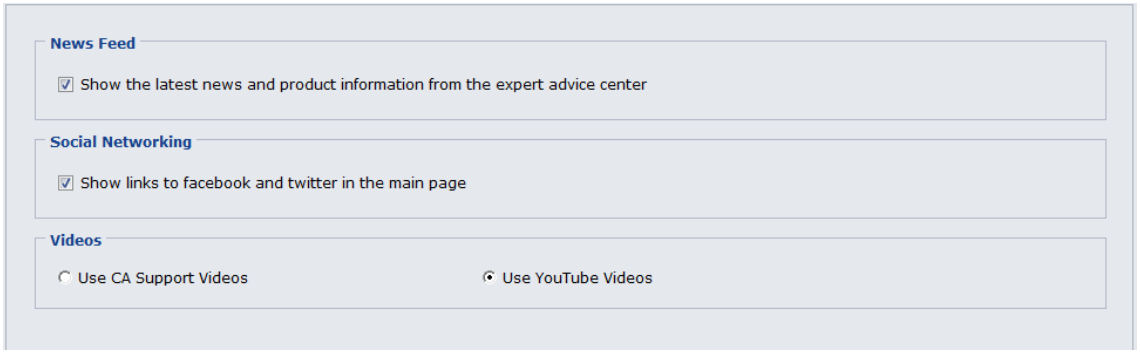
1. Log in to the application.

   From the Navigation bar on the home page, click Configuration.

   The Configuration screen displays

2. From the Configuration panel, click Preferences Configuration.

   The Preferences options appear.



3. Specify the options that you require:

   - **News Feed**--Lets the application display RSS feeds about CA ARCserve Central Applications and CA ARCserve D2D related news and product information (from the Expert Advice Center). The feeds appear on the home page.
   - **Social Networking**--Lets the application display icons on the home page for access to Twitter and Facebook for CA ARCserve Central Applications and CA ARCserve D2D related social networking websites.
   - **Videos**--Lets you select the type of video to view your CA ARCserve Central Applications and CA ARCserve D2D products. (Use YouTube Videos is the default video.)

   Click Save.

   The Social Networking options are applied

4. From the Navigation bar, click Home.

   The Home Page displays.

5. Refresh your browser window.

   The Social Networking options are applied.

Modify the Administrator Account

CA ARCserve Central Applications let you modify the user name, password, or both for the administrator account after you install the application. This administrator account is used only for the default display user name on the login screen.

Note: The user name specified must be a Windows administrative account or an account that has Windows administrative privileges.

Follow these steps:

1. Log in to the application and click Configuration in the Navigation bar.

   The configuration options appear.

2. Click Administrator Account

3. The Administrator account settings appear.

4. Update the following fields, as required:

   - User Name
   - Password

   Click Save

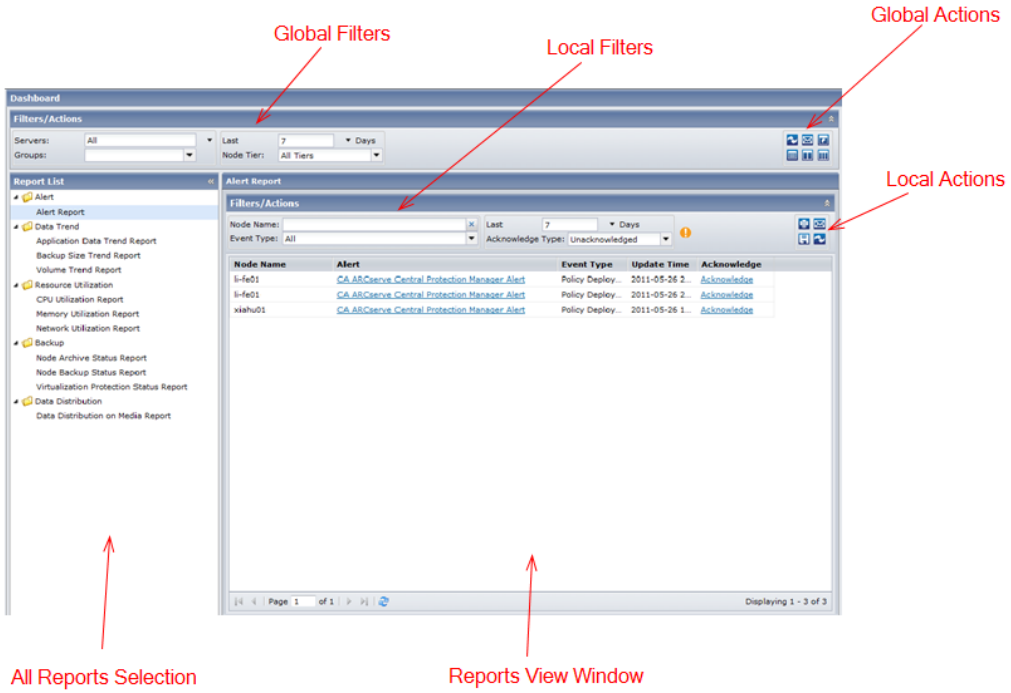
The administrator account is modified.

Chapter 4: Using CA ARCserve Central Reporting

This section contains the following topics:

Understanding the Dashboard Screen

The Dashboard screen is accessed from the Navigation bar on the left panel of the CA ARCserve Central Reporting application. You can view details of your protected environment in a single central view of status roll-ups and summary reports. With each of the reports you can expand and drill down into specific computers, which can help you determine the root causes of problems.



The Dashboard screen lets you filter your reports in two perspectives: Global and Local.

- **Global Filters**--Lets you specify the filter to display for all reports.
  - **Servers**
    - **All** (default)--Displays results on all nodes registered with the CA ARCserve Central Protection Manager server.
    - **CA ARCserve Backup**--Select All or specific CA ARCserve Backup nodes registered with the CA ARCserve Central Protection Manager server for you to select.
    - **CA ARCserve D2D**--Select All or specific CA ARCserve D2D nodes registered with the CA ARCserve Central Protection Manager server for you to select.

- **Groups**

  The Groups filter displays application types and names of CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups. This selection is applied to all reports listed in the Report List.

- **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 (*default*), and 30 days) to select from. You can also manually enter a value in this field.

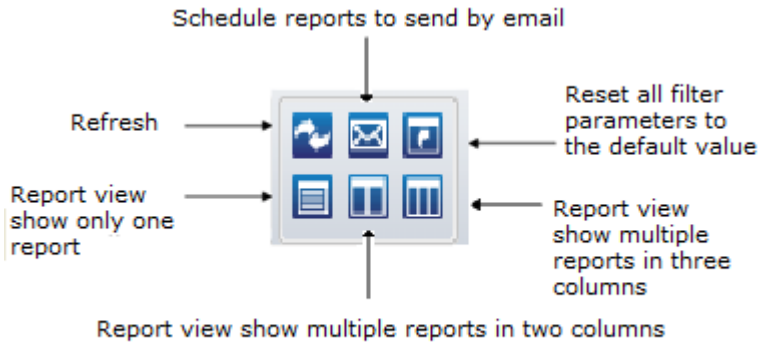
- **Node Tier**

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

  Note: The Node Tier for CA ARCserve D2D nodes is Medium Priority.

- **Global Actions**--Lets you select one of the following icons to apply to all reports. For more details on these icons, see the Reporting Tasks (see page 87) section.



- **Local Filters**--Lets you specify the filter for the selected report. For more details on each filter, see the desired report in the CA ARCserve Central Reporting Types (see page 35) section.
- **Local Actions**--Lets you select one of the following icons to apply to the selected report. For more details on the icons, see the Reporting Tasks (see page 87) section.

- **Reports View Window**--Displays the results for the selected report.

  Note: All reporting data is obtained from CA ARCserve Central Protection Manager where each node is registered and synchronized. For more details, see section on 'What You Can Do With Nodes' in the *CA ARCserve Central Protection Manager User Guide*.

- **All Reports Selection Panel**--Displays the types of reports CA ARCserve Central Reporting has to offer. For more information on each report, see CA ARCserve Central Reporting Types (see page 35).

CA ARCserve Central Reporting Types

The reports provided by CA ARCserve Central Reporting are categorized into five types of reports: Alert Report, Data Trend Reports, Resource Utilization Reports, Backup Reports, and Data Distribution Reports. In addition, some of the reports have an enhanced capability to drill down into the report to display more detailed information.

This section contains the following topics:

Alert Report

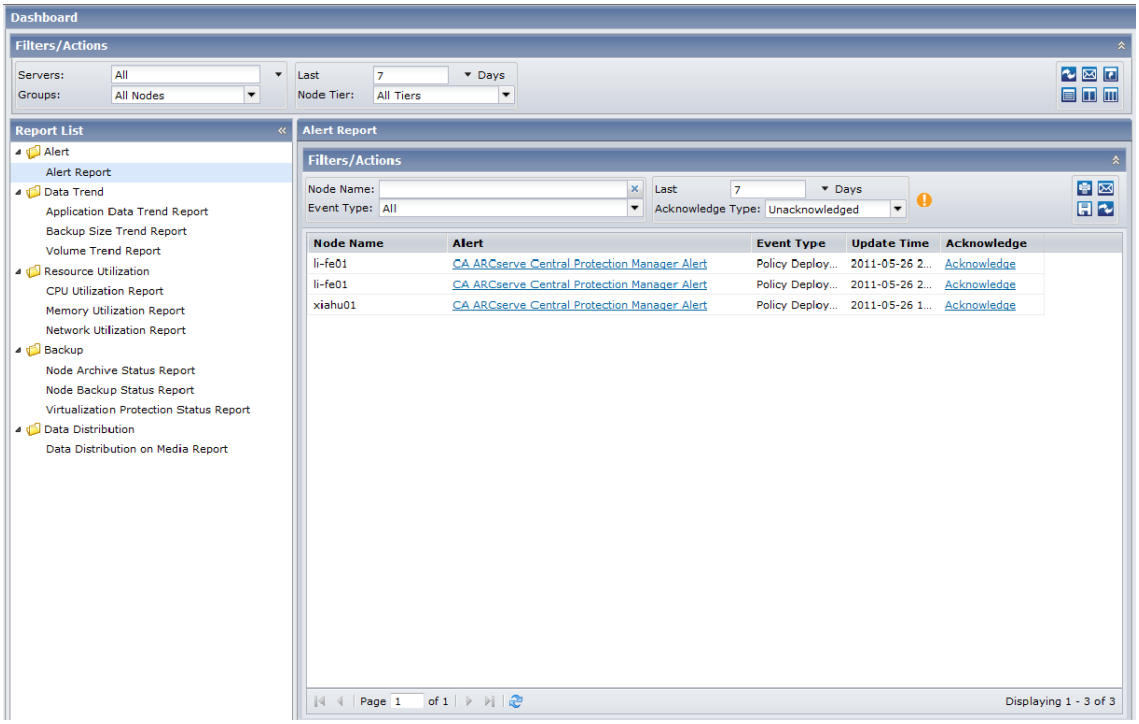
The Alert Report displays all alert messages for each node during the specified time period.

This section contains the following topics:

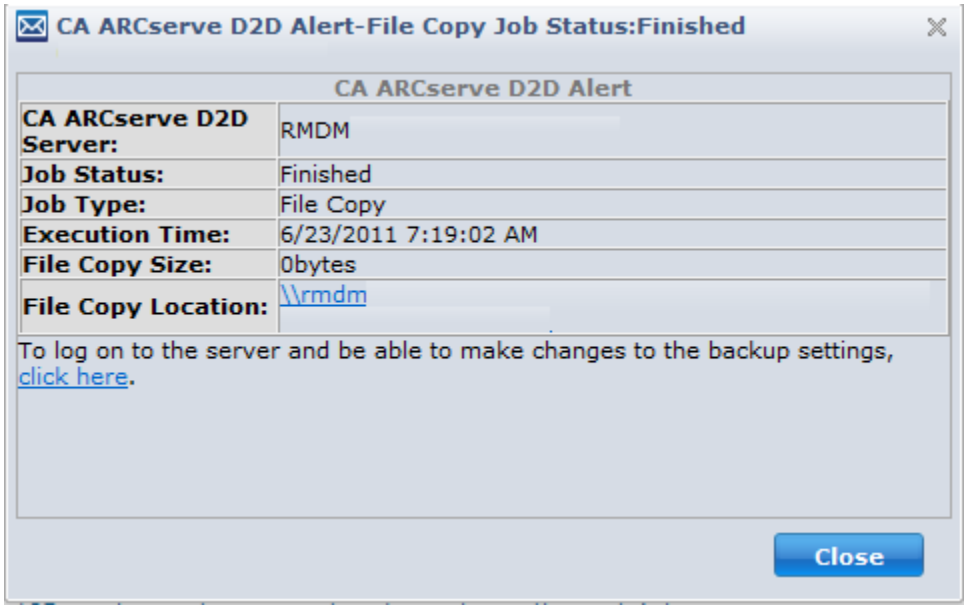
Alert Report View

The Alert Report generates alerts for each node from their corresponding application. The report displays detailed information about the nodes and event types.

You can view the Alert report screen by clicking the Dashboard tab from the Navigation bar.



For more details about the message, click the hypertext link for the alert you want to view.



This report contains the following filters:

- **Node Name**--Specifies the name of the Primary Server, Standalone Server, or Global Dashboard Central Primary Server for the CA ARCserve Backup or the CA ARCserve D2D nodes.
- **Event Type**--Specifies the following event types for the selected node:
  - All
  - New Updates Available
  - Successful Backup, Restore, or Export job
  - Failed Backup, Restore, or Export job
  - Policy Deployment Failed
  - Missed Jobs
  - PKI Alert
  - Destination Free Space Monitor
  - Synchronization Not Done
  - Host-Based VM Backup Errors
  - Virtual Standby Monitor
  - Virtual Standby Failed
  - Virtual Standby Successful
  - Skip/Merge job waiting in the job queue
  - Discovery
- **Last (number of) Days**--Specifies a preset listing of the commonly used data collection time periods (1, 3, 7 (default), and 30 days) to select from. You can also manually enter a value in this field.
- **Acknowledge Type**--Specifies All, Acknowledge, or Unacknowledged messages.

Be aware of the following:

- The Global Filters - Servers, Groups, Last (number of) Days, and Node Tier filters, do not apply to this report.
- To view the CA ARCserve Central Virtual Standby alerts, register the source nodes and the monitor in the CA ARCserve Central Protection Manager application.
- To view the CA ARCserve Central Host-Based VM Backup alerts, register the CA ARCserve D2D virtual machine proxy server in the CA ARCserve Central Protection Manager application

The Alert Report displays results for the following items:

- **Node Name**--Indicates the name of the Primary Server, Standalone Server, or Global Dashboard Central Primary Server for the CA ARCserve Backup or the CA ARCserve D2D nodes.
- **Alert Message**--Indicates the alert message for the corresponding node.

  Note: Clicking the Alert message displays more information about that particular alert.
- **Event Type**--Indicates the type of event for the corresponding node.
- **Update Time**--Indicates the time the alert message was last updated.
- **Acknowledge**--Lets you acknowledge the alert message by clicking the Acknowledge hyperlink and removing it from the table.

  Note: You can review the removed message again by selecting Acknowledged from the Acknowledge Type drop down in the local filters section.

Note: You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.

Data Trend Reports

This section contains the following topics:

Application Data Trend Report

The Application Data Trend Report is an SRM-type report that displays the data size used for each type of application in a historical view. The report 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 on supported Windows operating system. In addition, the report allows you to drill down to display more detailed information for a single node.

Application Data Trend Report Benefits

The Application Data Trend Report is helpful in analyzing the current (and historical) size of data used for CA ARCserve Backup and CA ARCserve D2D protected applications. In addition, this report is also helpful in determining the future application size based upon anticipated growth trends. With this information, you can predict disk space requirements for a future time period and take actions accordingly to help ensure that the environment is properly protected. This report lets you select specific or several applications to analyze the overall data size for these applications.

Application Data Trend Report View

The Application Data Trend Report is displayed in graph format showing the amount of data used (in GB) for each particular application, with the anticipated trends during a future time period. The report lets you specify the view mode (Week, Month, Year, All (default), 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 or click on any sample point along the data line to display more details.

The following filters can be used for the Application Data Trend Report:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This filters all reports based upon the selected node tier.

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

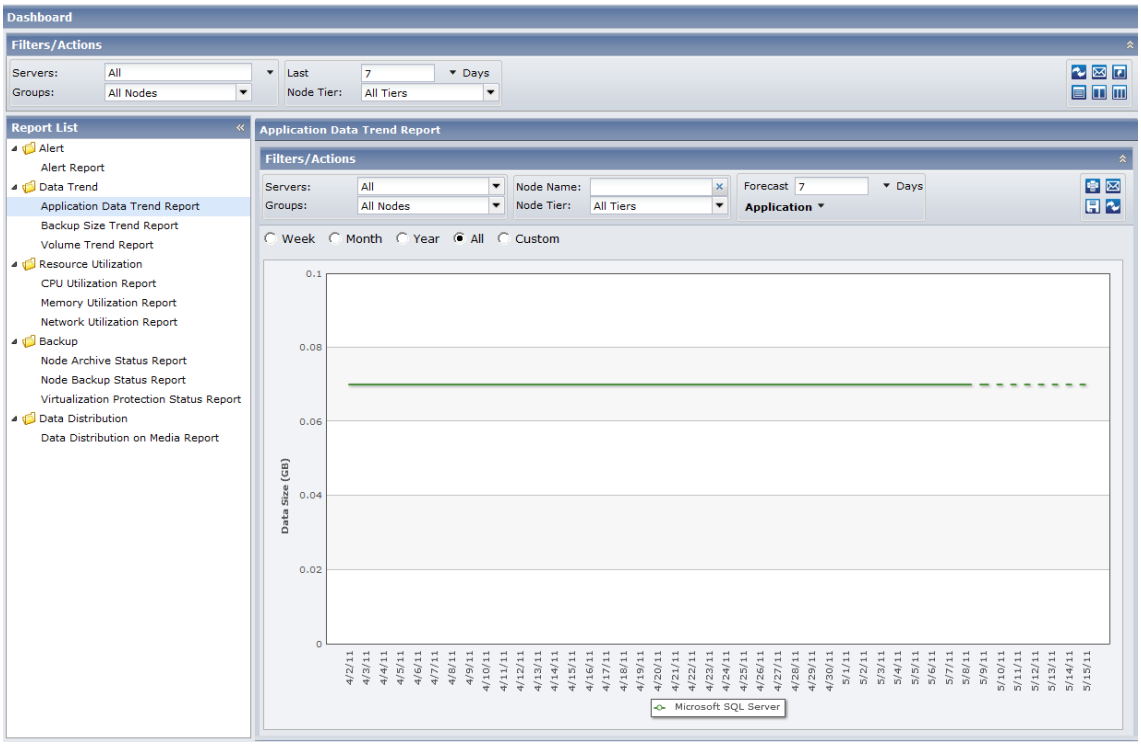
  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Forecast**--Lets you select or manually enter the number of days for a forecasted time range (maximum number of days is 90).
- **Application**--Lists the individual applications associated to the server and group you selected.

  The following applications are supported:

  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Microsoft SharePoint Server
  - Oracle Server
  - Lotus Domino
  - Sybase Server

- Informix Dynamic Server
- SAP
- Hyper-V
- VMware

Note: CA ARCserve Backup supports these applications with the exception of Microsoft SQL Server and Microsoft Exchange Server, which CA ARCserve D2D supports.



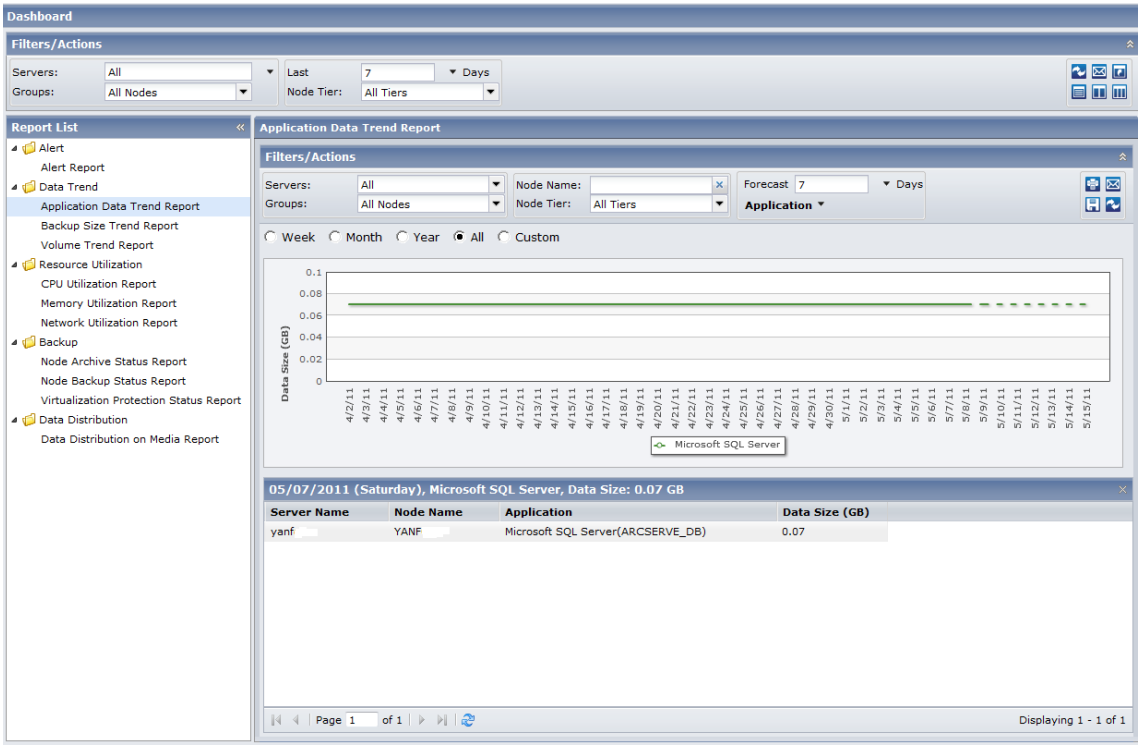
This report lets you easily see the projected trends in storage capacity for the applications to help you plan for your future data storage needs. The data from each application is displayed as a separate line with a separate color and the projected data is displayed with a dotted line. A summary line chart is also available to display the overall data size (and trend) for all selected applications. Only data from installed applications (protected by CA ARCserve Backup and CA ARCserve D2D) are displayed.

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

Application Data Trend Drill Down Report

The Application Data Trend Report can be further expanded to display more detailed information. You can click a sample point on the line chart to show the details of that time period.

The following sample contains detailed information for the Application Data Trend Report:



This drill-down report includes the following data for each application:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Application**--Indicates only the installed applications protected by CA ARCserve Backup or CA ARCserve D2D.
- **Data Size (GB)**--Indicates the overall data size of the application.

Note: You can drill into each column name to sort in ascending or descending order and view any of the columns on the screen. All columns are enabled by default.

Backup Size Trend Report

The Backup Size Trend Report displays the backup data size of both CA ARCserve Backup and CA ARCserve D2D in a historical view. This report projects the growth trend that you can prepare for future storage space requirements. This report also contains information for nodes which run on supported Windows operating systems and allows you to drill down to display more detailed information for an individual node.

Backup Size Trend Report Benefits

The Backup Size Trend Report is helpful in analyzing the current (and historical) backup data size for CA ARCserve Backup and CA ARCserve D2D protected servers. In addition, this report is also helpful in determining the future backup size based upon anticipated growth trends. With this information, you can predict disk space requirements for a future time period and take actions accordingly to help ensure that the environment is properly protected. The Backup Size Trend Report lets you select specific or several servers to analyze the overall backup size for these servers.

Backup Size Trend Report View

The Backup Size Trend Report is displayed in graph format showing the amount of data used (in GB) for each particular application, with the anticipated trends during a future time period. The report lets you specify the view mode (Week, Month, Year, All (default), 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 or click on any sample point along the data line to display more details.

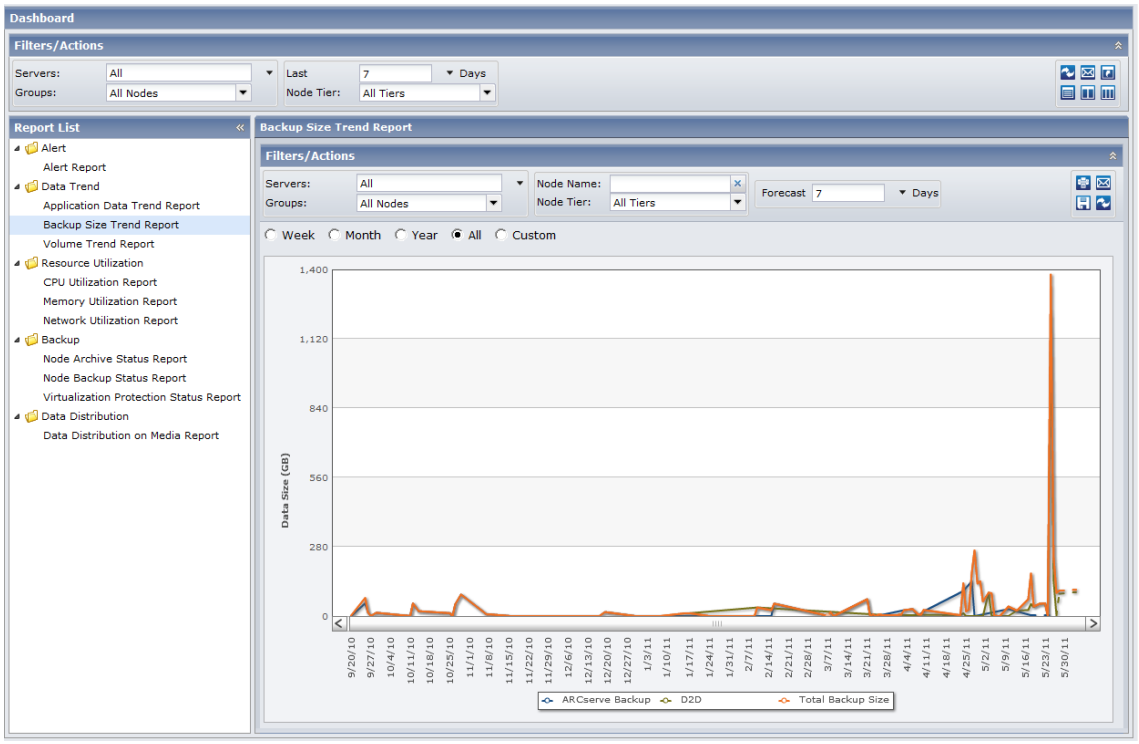
This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This filters all reports based upon the selected node tier.

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

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Forecast**--Lets you select or manually enter the number of days for a forecasted time range (maximum number of days is 90).
- **Application**--Lists the individual applications associated to the server and group you selected.

  Note: The applications supported are: CA ARCserve Backup and CA ARCserve D2D.



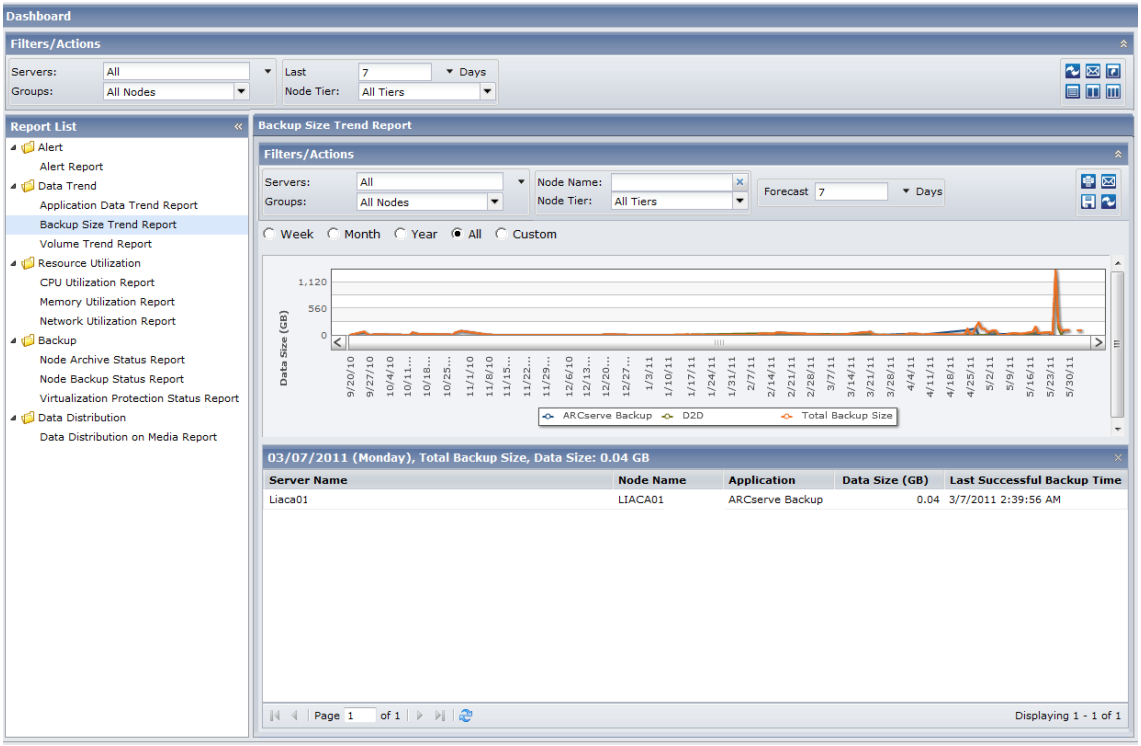
This report lets you see the projected trends in storage capacity for the applications to help you plan for your future backup needs. The data from each application is displayed as a separate line with a separate color and the projected data is displayed with a dotted line. A summary line chart is also available to display the overall data size (and trend) for all selected applications. Only data from installed applications (protected by CA ARCserve Backup and CA ARCserve D2D) are displayed.

Backup Size Trend Drill Down Report

The Backup Size Trend Report can be further expanded to display more detailed information. You can click a sample point on the line chart to show the details of that time period.

Note: For immediate results on specific nodes, you must submit an SRM Probe Job from CA ARCserve Central Protection Manager so that the backup size data is calculated for CA ARCserve Backup and CA ARCserve D2D. If you do not submit an SRM Probe Job manually, then the backup size data is calculated after the scheduled SRM Probe Job is executed. For more details on how to submit SRM Probe Jobs, see the Configure SRM Schedules section in the CA ARCserve Central Protection Manager User Guide.

The following sample contains detailed information for the Backup Size Trend Report:



This drill-down report includes the following data for each application:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Application**--Indicates only the installed applications protected by CA ARCserve Backup or CA ARCserve D2D.
- **Data Size (GB)**--Indicates the overall data size of the application.
- **Last Successful Backup Time**--Indicates the date and time of the last successful backup.

Note: You can drill into each column name to sort in ascending or descending order and view any of the columns on the screen. All columns are enabled by default.

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. The report 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 CA ARCserve D2D and CA ARCserve Backup installed nodes which run a supported Windows operating system and allows you to drill down to display more detailed information for a single node.

Volume Trend 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 that the environment is properly protected.

Volume Trend 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 (default), and Customized Time Range) for the displayed time period.

This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

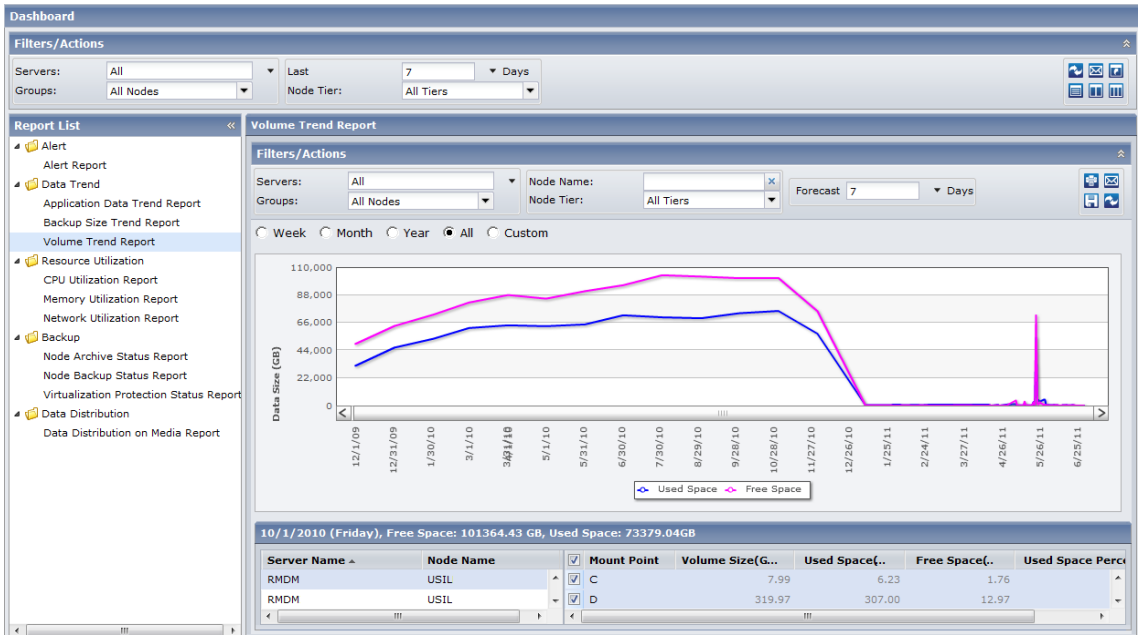
  The Node tier field contains a drop-down menu listing each tier category to select from: High Priority, Medium Priority, and Low Priority.

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Forecast**--Lets you select or manually enter the number of days for a forecasted time range (maximum number of days is 90).

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 is displayed with a dotted line.

By default, the Volume Trend Report displays a drill-down report.

The following sample contains detailed information for the Volume Trend Report:



The drill-down report that includes the following:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Mount Point**--Indicates the root directory where the volumes are mounted.
- **Volume Size (GB)**--Indicates the volume size of the corresponding node.
- **Used Space (GB)**--Indicates the amount of used space on the corresponding node.
- **Free Space (GB)**--Indicates the amount of free space left on the corresponding node.
- **Used Space Percentage**--Indicates the percentage of used space on the corresponding node.

You can also select different volume combinations by checking more than one Node Name to display their accumulated size trends.

Note: You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.

Resource Utilization Reports

This section contains the following topics:

CPU Utilization Report (see page 49)
Memory Utilization Report (see page 53)
Network Utilization Report (see page 57)

CPU Utilization Report

The CPU Utilization Report displays the percentage of CPU usage for CA ARCserve Backup and CA ARCserve D2D protected servers during a specified time period. It is important to monitor CPU usage to make sure that it does not become overloaded too often. If your CPU usage becomes too high, your server response time may become slow or unresponsive. When this situation occurs, you need to determine which process is causing this high CPU usage and remedy the problem.

CPU Utilization Report Benefits

The CPU Utilization Report is helpful in quickly classifying machines based on the amount of CPUs, 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 require an upgrade to 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.

CPU Utilization Report View

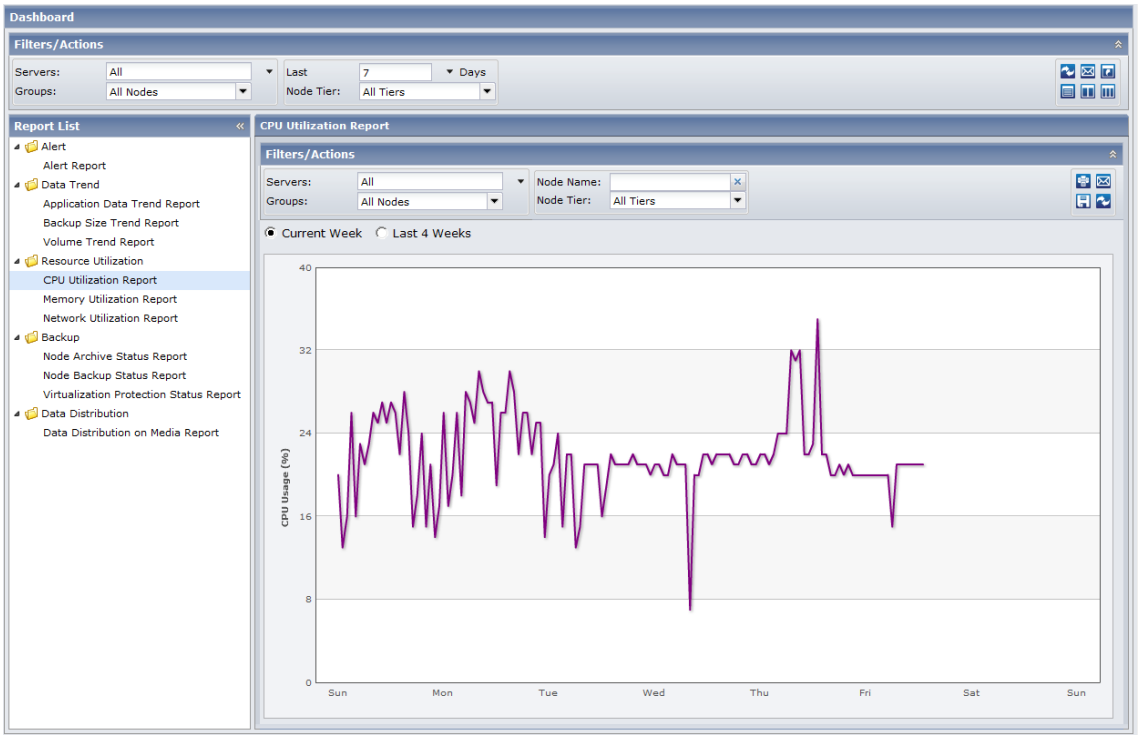
The CPU Utilization Report displays in graph format showing a historical view of the percentage of CPU usage for the monitored servers during a specified time period (only for CA ARCserve D2D and CA ARCserve Backup installed nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data starting from Sunday of the current week, and the Last 4 Weeks mode displays data for the last 4 weeks.

This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This filters all reports based upon the selected node tier.

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

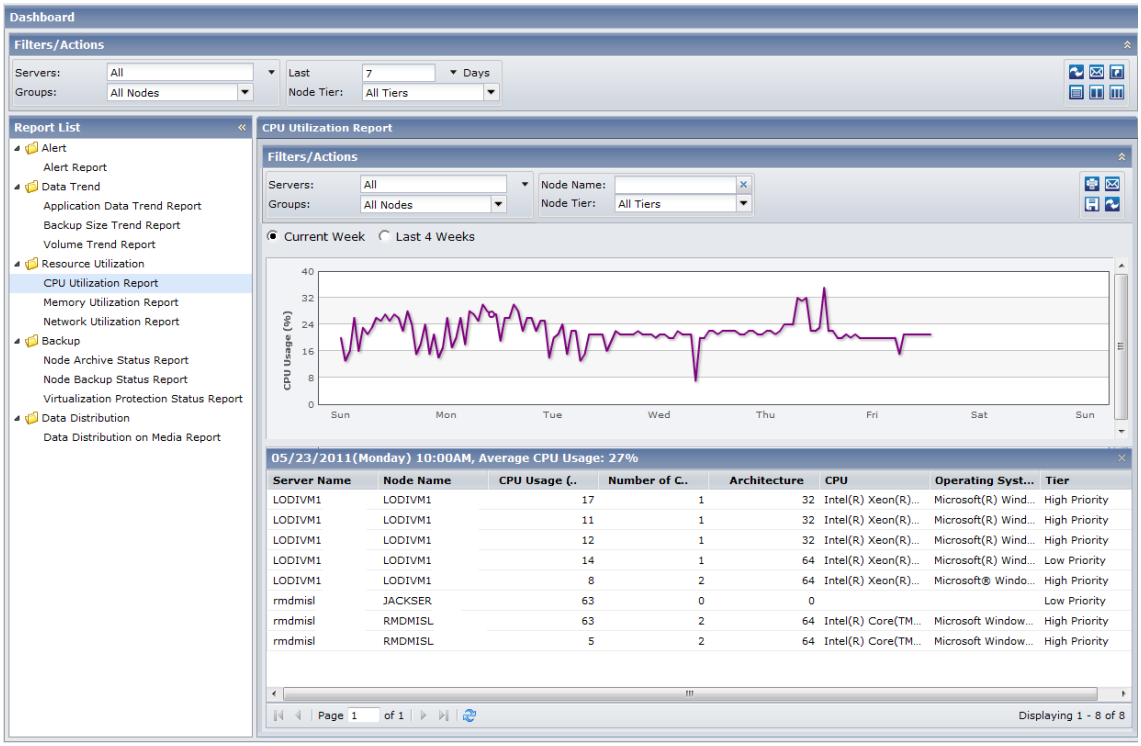
  Note: The tier for CA ARCserve D2D nodes is Medium Priority.



CPU Utilization Drill Down Report

The CPU Utilization Report can be further expanded to display more detailed information. You can click a sample point on the line chart to show the details of that specific time period.

The following sample contains detailed information for the CPU Utilization Report:



The drill-down report includes the following:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.

- **CPU usage (%)**--Indicates the CPU usage of each node.
- **Number of CPUs**--Indicates the number of CPUs used for the corresponding node.
- **Architecture**--Indicates whether the CPU is a 32-bit or 64-bit version.
- **CPU (Central Processing Unit)**--Indicates the type of CPU used.
- **OS (Operating System)**--Indicates the type of operating systems used.
- **Tier**--Indicates the priority level of the node.

Note: You can drill into each column name to sort in ascending or descending order and view any of the columns on the screen. All columns are enabled by default.

Memory Utilization Report

This report displays a historical view of the percentage of memory in use on your client nodes during a specified period of time. This report contains information for nodes which run on supported Windows operating systems and allows you to drill down to display more detailed information for an individual node.

Memory Utilization Report Benefits

The Memory Utilization Report displays the percentage of memory in use on your CA ARCserve Backup and CA ARCserve D2D 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 memory 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 an application or server upgrade may be necessary.

Memory Utilization Report View

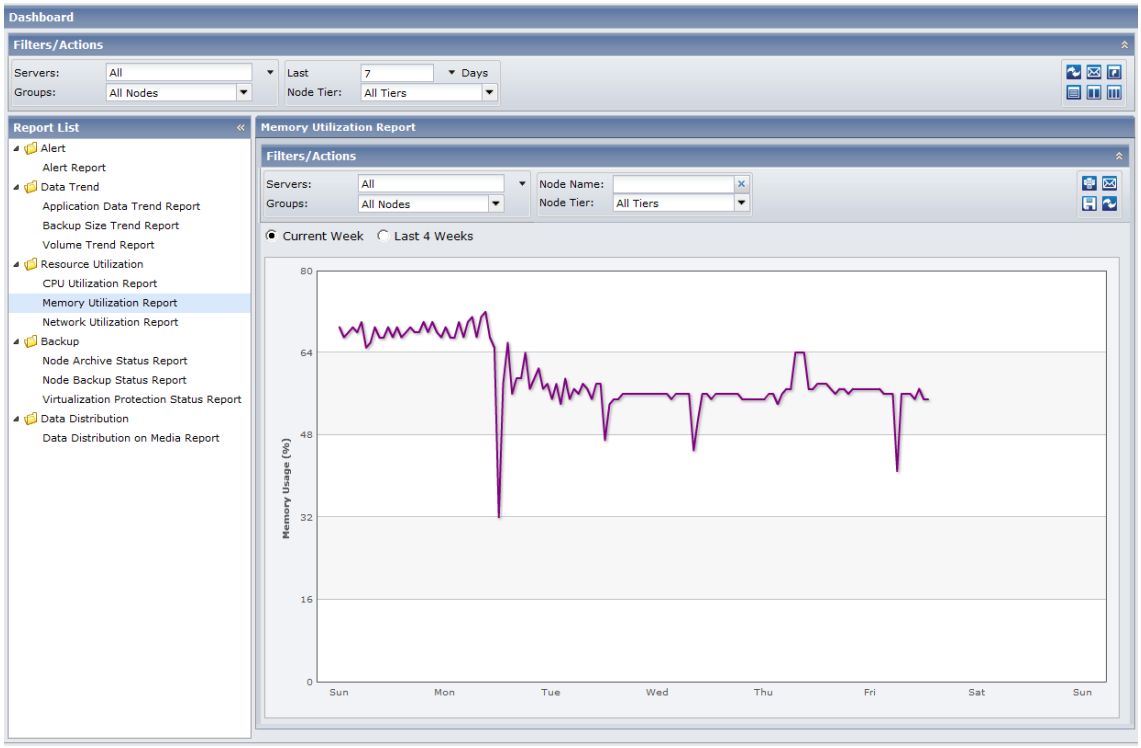
The Memory Utilization Report is displayed in graph format showing a historical view of the percentage of memory usage for the monitored servers during a specified time period (only for CA ARCserve D2D and CA ARCserve Backup installed nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data starting from Sunday of the current week, and the Last 4 Weeks mode displays data for the last 4 weeks. You can click on any sample point along the data line to display more details about that specific sample point.

This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

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

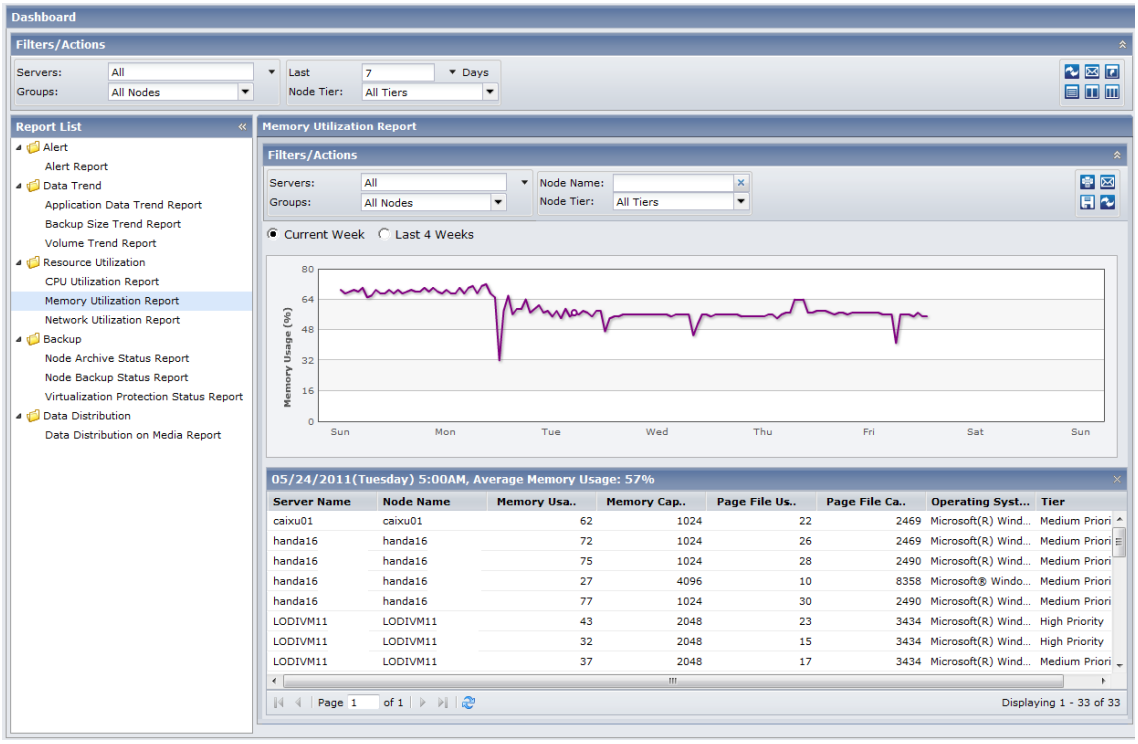
  Note: The tier for CA ARCserve D2D nodes is Medium Priority.


Dashboard
Filters/Actions
Servers: All
Groups: All Nodes
Last 7 Days
Node Tier: All Tiers
Report List
Alert
Alert Report
Data Trend
Application Data Trend Report
Backup Size Trend Report
Volume Trend Report
Resource Utilization
CPU Utilization Report
Memory Utilization Report
Network Utilization Report
Backup
Node Archive Status Report
Node Backup Status Report
Virtualization Protection Status Report
Data Distribution
Data Distribution on Media Report
Memory Utilization Report
Filters/Actions
Servers: All
Groups: All Nodes
Node Name:
Node Tier: All Tiers
Current Week
Last 4 Weeks
Memory Usage (%)
80
64
48
32
16
0
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sun

Memory Utilization Drill Down Report

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.

The following sample contains detailed information for the Memory Utilization Report:



This drill-down report includes the following items for each node:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Memory Usage (%)**--Indicates the percentage of memory usage for the corresponding node.
- **Memory Capacity**--Indicates the amount of memory capacity for the corresponding node.

- **Page File Usage (%)**----Indicates the percentage of page file usage for the corresponding node.
- **Page File Capacity**--Indicates the amount of page file capacity for the corresponding node.
- **OS (Operating System)**--Indicates the type of operating system used.
- **Tier**--Indicates the priority level of the 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.

Be aware of the following:

- You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.
- 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.

Network Utilization Report

This report displays a historical view of the percentage of network capacity in use on your client nodes during a specified period of time. This report contains information for nodes which run on supported Windows operating systems and allows you to drill down to display more detailed information for an individual node.

Network Utilization Report Benefits

The Network Utilization Report displays the percentage of NIC bandwidth you are currently using on your CA ARCserve Backup and CA ARCserve D2D 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, therefore you would want the network utilization to be as low as possible. If your network utilization continually becomes too high, you need to determine which process is causing this high usage and remedy the problem.

Network Utilization Report View

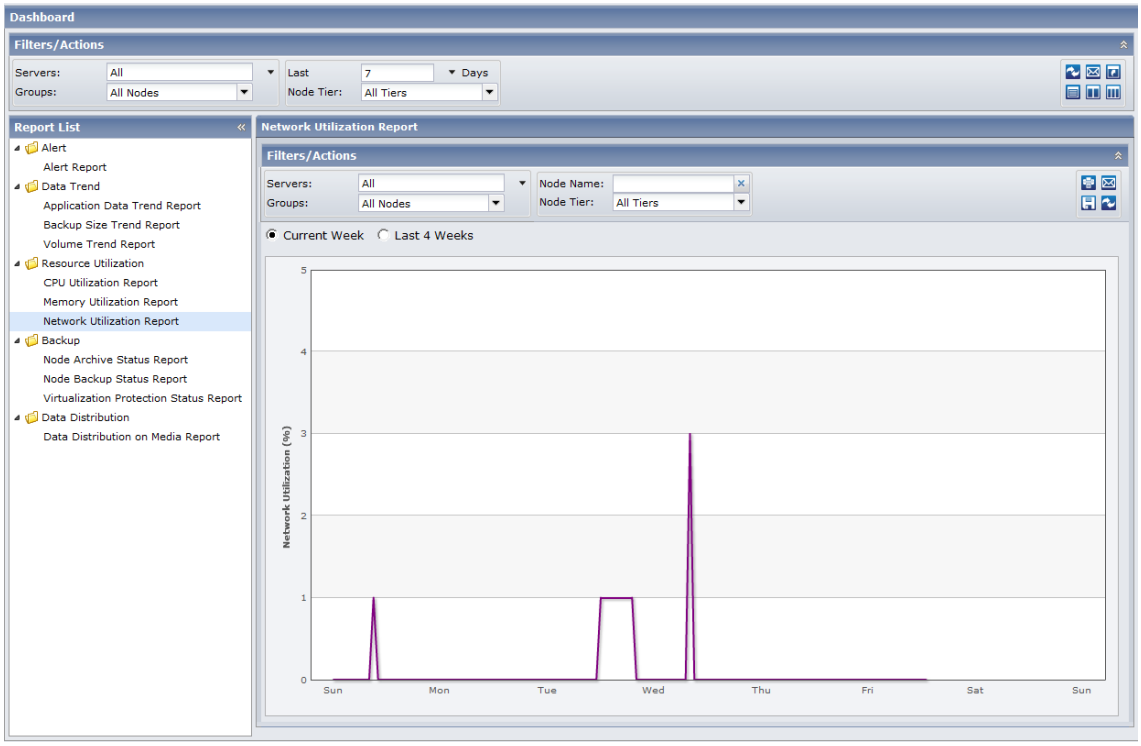
The Network Utilization Report is displayed in graph format showing a historical view of the percentage of network (NIC) usage for the monitored servers during a specified time period (only for CA ARCserve D2D and CA ARCserve Backup installed nodes which run a supported Windows operating system). The report lets you specify the view mode (Current Week or Last 4 Weeks) for the displayed time period. The Current Week mode displays data starting from Sunday of the current week, and the Last 4 Weeks mode displays data for the last 4 weeks. You can click on any sample point along the data line to display more details about that specific sample point.

This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

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

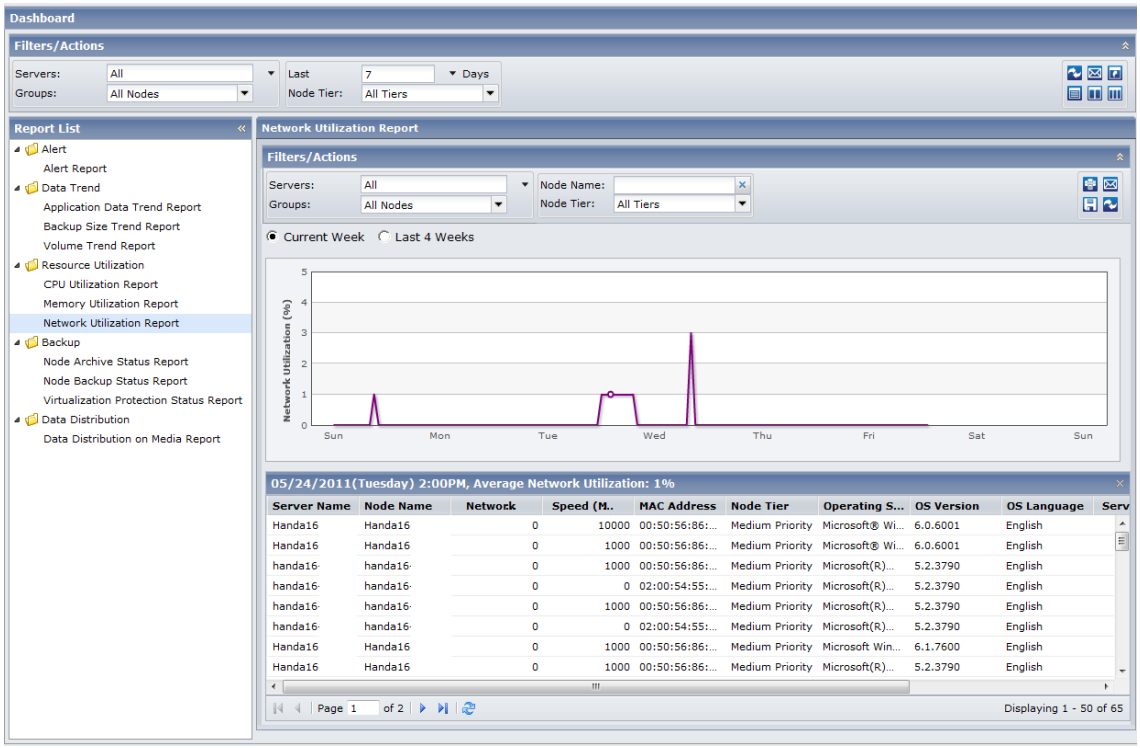
  Note: The tier for CA ARCserve D2D nodes is Medium Priority.


Dashboard
Filters/Actions
Servers: All
Groups: All Nodes
Last 7 Days
Node Tier: All Tiers
Report List
Alert
Alert Report
Data Trend
Application Data Trend Report
Backup Size Trend Report
Volume Trend Report
Resource Utilization
CPU Utilization Report
Memory Utilization Report
Network Utilization Report
Backup
Node Archive Status Report
Node Backup Status Report
Virtualization Protection Status Report
Data Distribution
Data Distribution on Media Report
Network Utilization Report
Filters/Actions
Servers: All
Groups: All Nodes
Node Name:
Node Tier: All Tiers
Current Week
Last 4 Weeks
Network Utilization (%)
0
1
2
3
4
5
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sun

Network Utilization Drill Down Report

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.

The following sample contains detailed information for the Network Utilization Report:



This drill-down report includes the following items for each node:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Network Utilization (%)**--Indicates the percentage of network usage for the corresponding node.
- **Speed Mbps**--Indicates the bandwidth speed of the corresponding node.

- **MAC address**--Indicates the MAC address of the corresponding node.
- **Node Tier-**--Indicates the priority level of the node.

You can also click the name of an individual node to display the line chart information for that particular node overlaid on the overall line chart.

Be aware of the following:

- You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.
- 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.

Backup Reports

This section contains the following topics:

Node Archive Status Report

This report shows the most recent archive status of CA ARCserve Backup nodes and file copy status of CA ARCserve D2D nodes during the specific time period. This report allows you to drill down to display more detailed information about each selected category.

Node Archive Status Report Benefits

The Node Archive Status Report is helpful in analyzing and determining which nodes are more effective than others for archive or file copy 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 or file copy 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 or file copy. 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.

Node Archive Status Report View

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

This report contains the following filters:

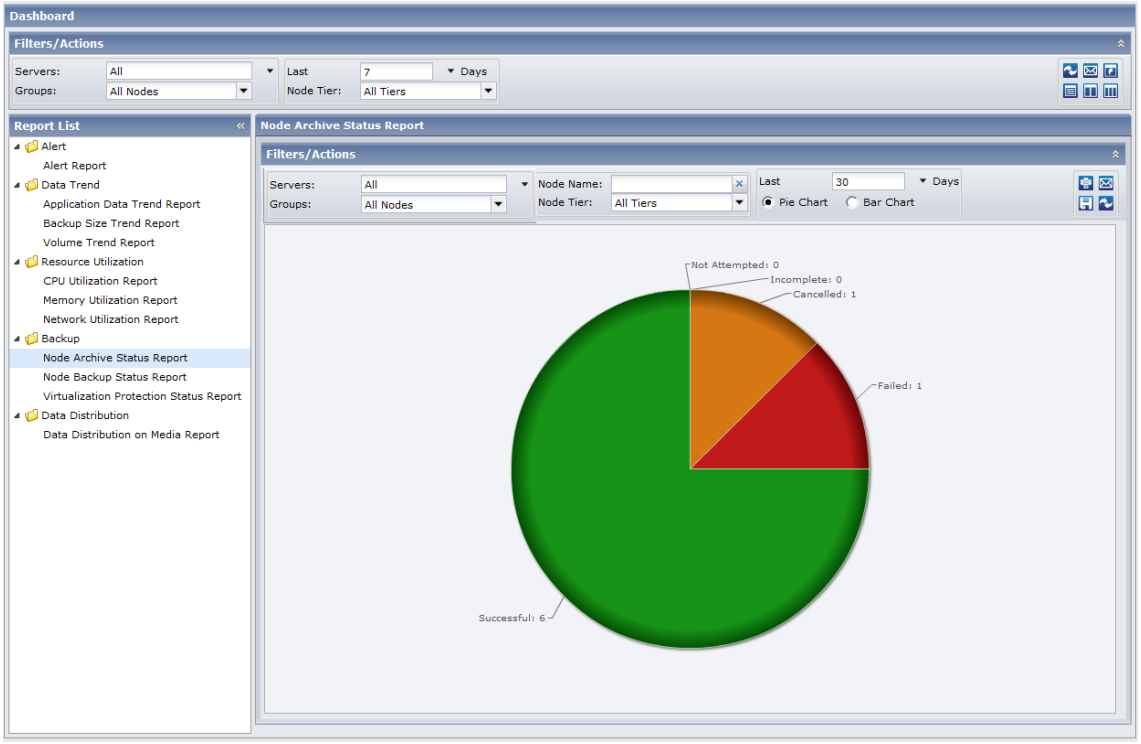
- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

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

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Last (number of) Days**--Specifies a preset listing of the most commonly used data collection time periods (1, 3, 7 (default), and 30 days) to select from. You can also manually enter a value in this field.

Pie Chart

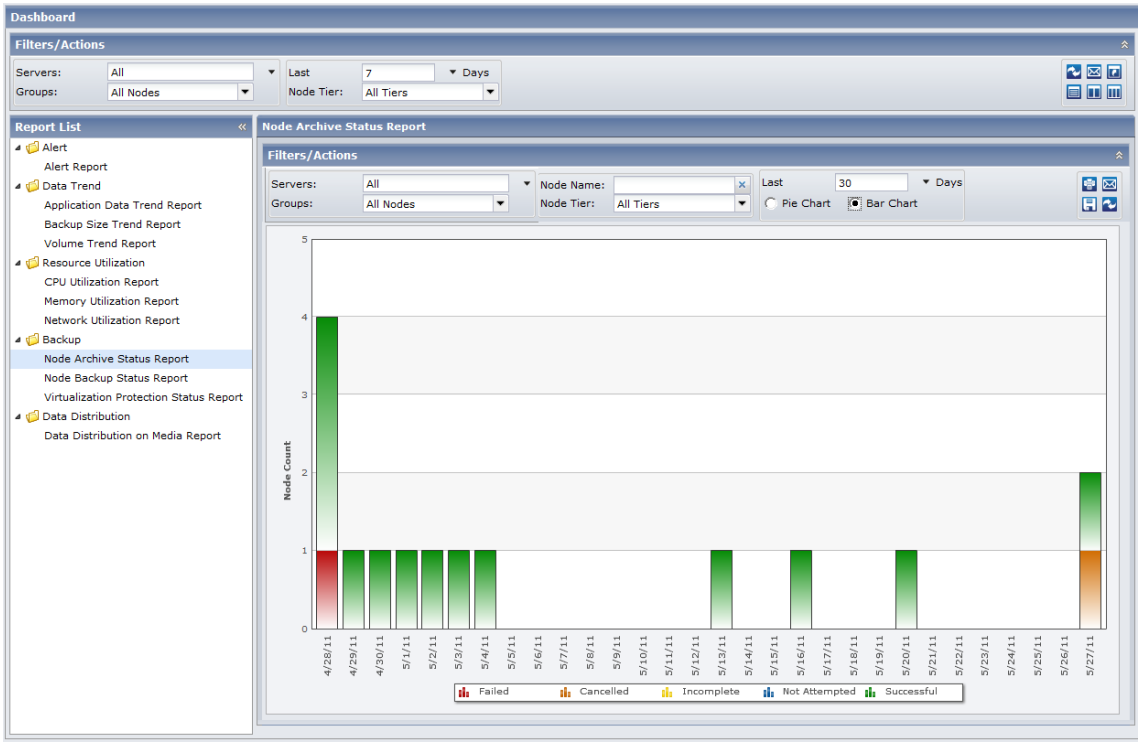
The pie chart provides a high-level overview of nodes that were archived or copied and pasted for **all days** of the specified time period. The status categories shown in the pie chart represent a percentage of the **total number** of nodes that were archived during the last specified number of days, 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 or copied and pasted 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.

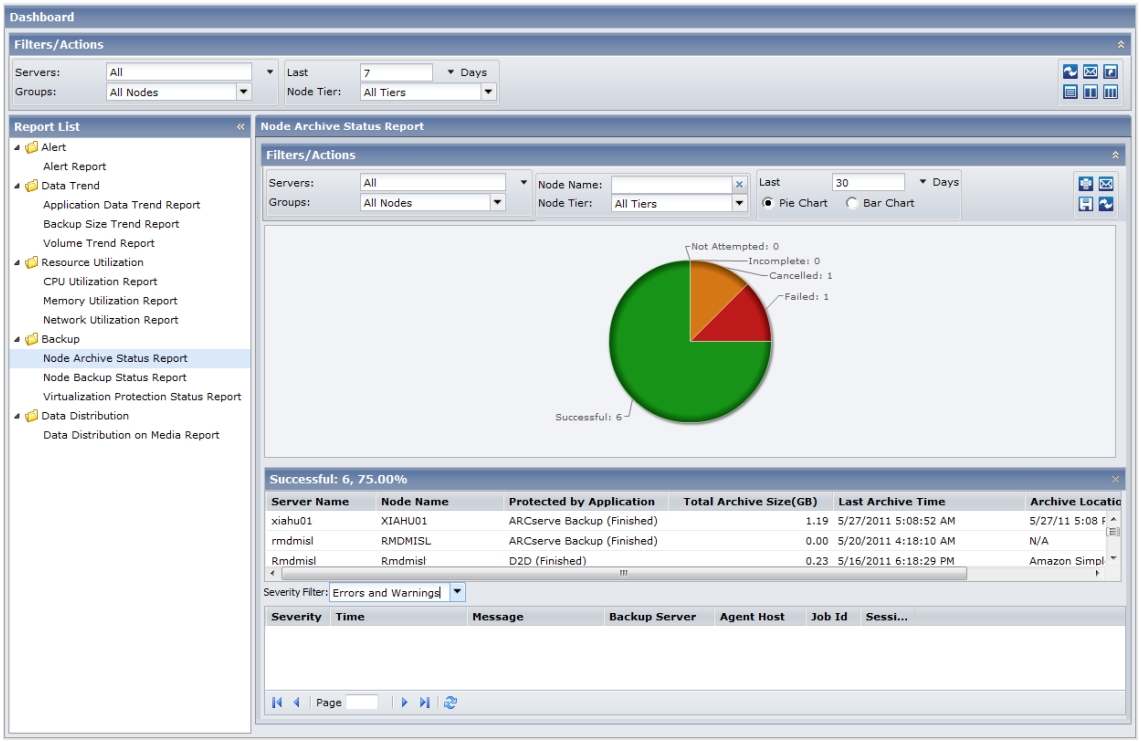
Note: By default, the CA ARCserve Central Reporting only displays bar chart information for a maximum of 90 days. Increasing the number of displayed days to more than 90 days would result in the bar chart information not being legible. If you specify to display report information for more than 90 days, 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.)



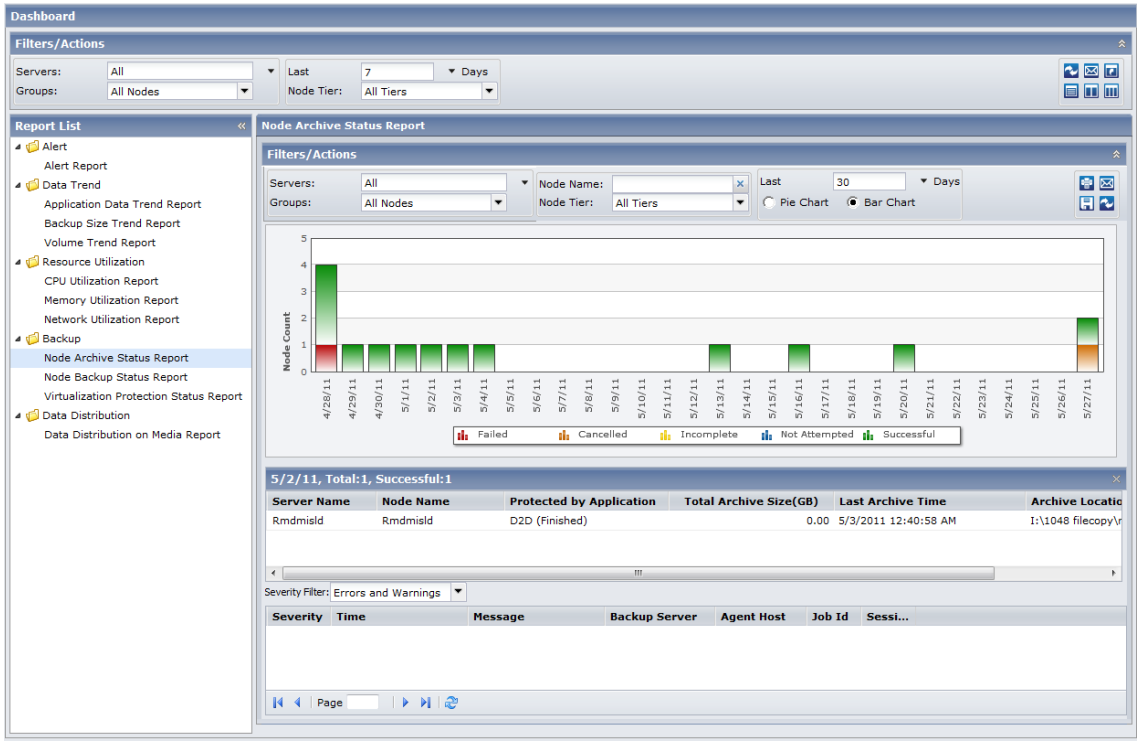
Node Archive Status Drill Down Report

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

The following sample contains detailed information for the Node Archive Status Report in Pie view:



The following sample contains detailed information for the Node Archive Status Report in bar view:



The drill-down reports include the following:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Total Archive Size (GB)**--Indicates the total size of data archived or copied to the corresponding node.
- **Last Archive Time**--Indicates the date and time of the last archive or file copy.
- **Archive Location**--Indicates the destination where the archive or file copy resides.

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

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:

- You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.
- CA ARCserve Central Reporting 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.

Node Backup Status 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.

Note: The Node Backup Status Report includes CA ARCserve Backup, CA ARCserve D2D, and virtual machine backups performed by CA ARCserve Central Host-Based VM Backup.

Node Backup Status Report View

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

This report contains the following filters:

- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
  - For power-on virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays the host name of the virtual machine in the report results.
  - For power-off virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays 'Unknown (*virtual machine name*)' in the report results.
  - **Note**: You cannot filter this report by searching for the word 'Unknown', however, to search for 'Unknown' Node Names, leave the Node Name filter blank to return all Node Name results or power-on the virtual machine to be detected.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

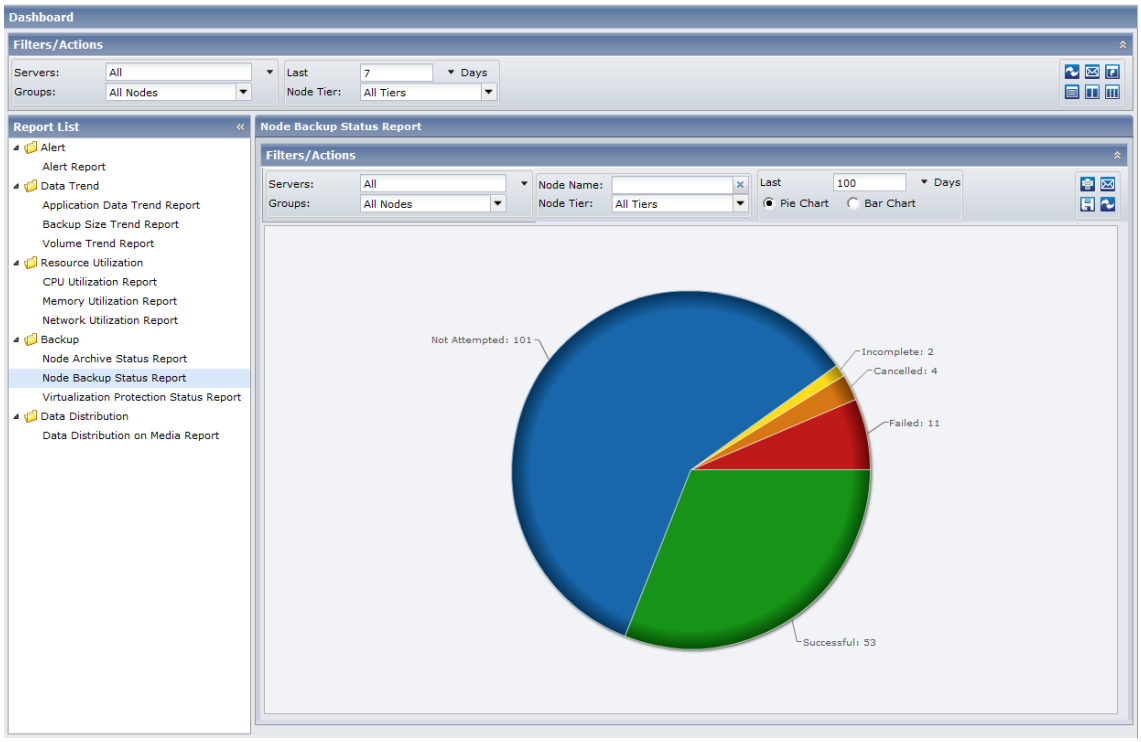
  The Node tier field contains a drop-down menu listing each tier category to select from: High Priority, Medium Priority, and Low Priority.

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Last (number of) Days**--Specifies a preset listing of the most commonly used data collection time periods (1, 3, 7 (default), and 30 days) to select from. You can also manually enter a value in this field.

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

Pie Chart

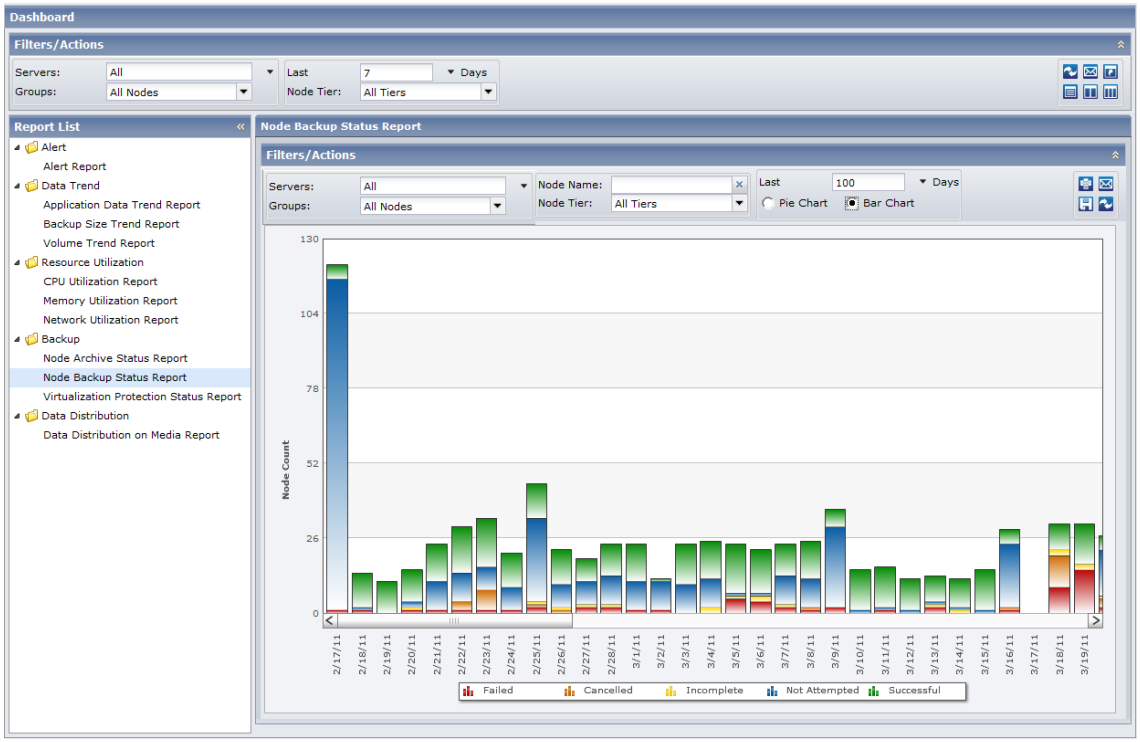
The pie chart provides a high-level overview of nodes that were backed up for all days of the specified time period. The status categories shown in the pie chart represent a percentage of the total number of nodes that were backed up during the last specified number of days, with the most recent backup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



Bar Chart

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

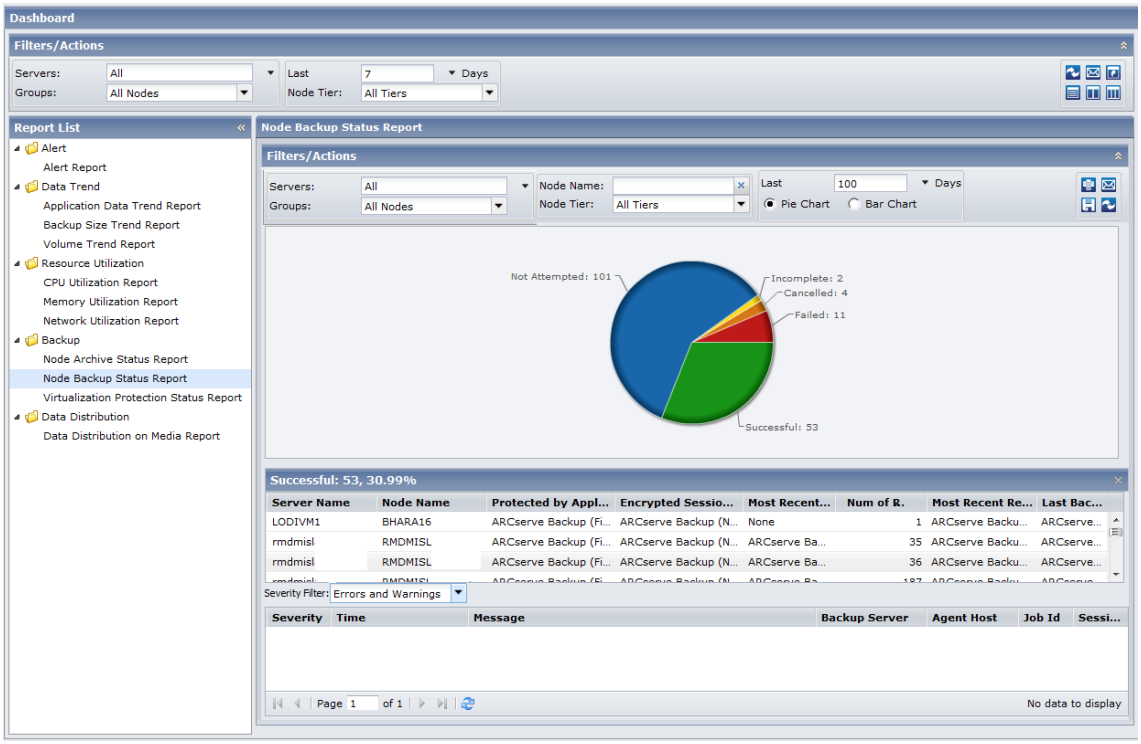
Note: By default, CA ARCserve Central Reporting only displays bar chart information for a maximum of 90 days. Increasing the number of displayed days to more than 90 days would result in the bar chart information not being legible. If you specify to display report information for more than 90 days, the 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).



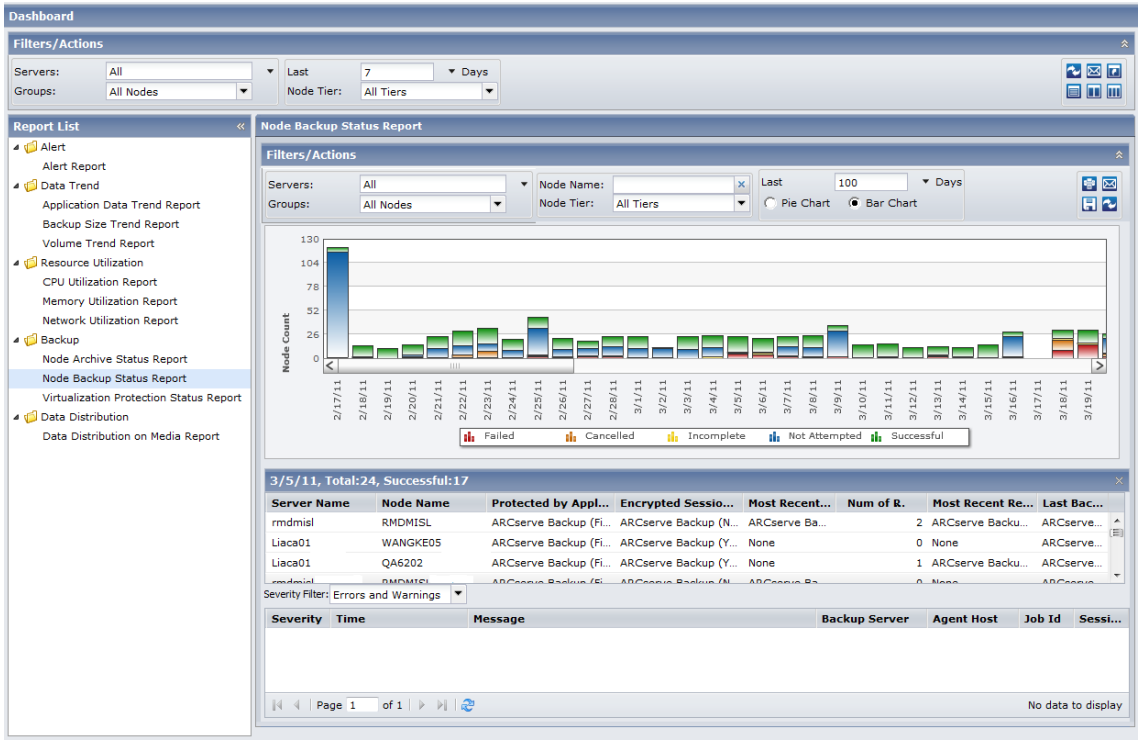
Node Backup Status Drill Down Report

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

The following sample contains detailed information for the Node Backup Status Report in Pie view:



The following sample contains detailed information for the Node Backup Status Report in bar view:



The drill-down reports include the following:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
  - For virtual machines protected by CA ARCserve Central Host-Based VM Backup, the Server Name field displays the host name of the proxy.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
  - For power-on virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays the host name of the virtual machine.
  - For power-off virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays 'Unknown (*virtual machine name*)'.

- **Protected by Application**--Indicates the type of application protecting the node.
- **Encrypted Sessions Available**--Indicates if the CA ARCserve D2D or CA ARCserve Backup sessions are encrypted.
- **Most Recent Successful Disaster Recovery Backup**--Indicates the most recent successful disaster recovery backup status for the corresponding node.
- **Number of Recovery Points**
- **Most Recent Recovery Points**
- **Last Backup Type**--Indicates the last backup job performed.

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:

- You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.
- CA ARCserve Central Reporting 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.

Virtualization Protection Status Report

The Virtualization Protection Status Report shows the most recent protection status for each virtual machine (VM) that was backed up using VMware Consolidated Backup (VCB) technology, Microsoft Hyper-V, CA ARCserve Central Virtual Standby, or CA ARCserve Central Host-Based VM Backup.

Virtualization Protection Status Report Benefits

The Virtualization Protection Status Report is helpful in analyzing and determining which virtual machines (VMs) 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 VMs. 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.

Virtualization Protection Status Report View

The Virtualization Protection Status Report is displayed in a pie chart where you can drill into to view more details on virtual machine statuses.

This report contains the following filters:

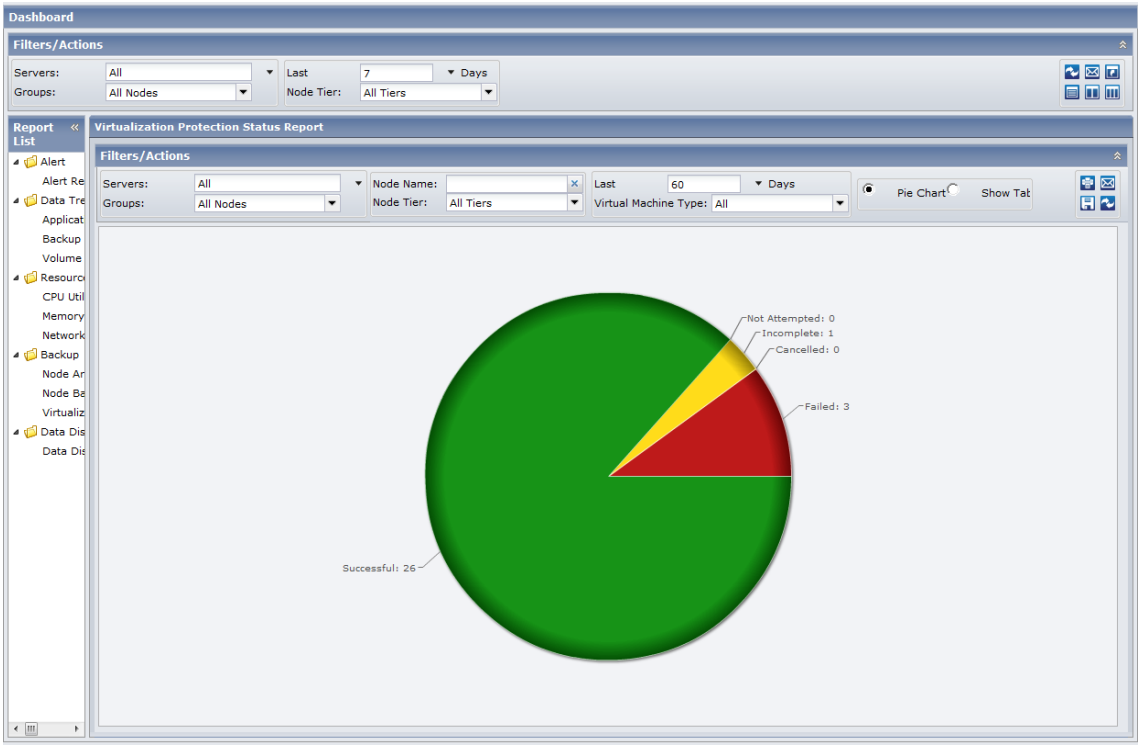
- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of the CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
  - For power-on virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays the host name of the virtual machine in the report results.
  - For power-off virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays 'Unknown (*virtual machine name*)' in the report results.

    Note: You cannot filter this report by searching for the word 'Unknown', however, to search for 'Unknown' Node Names, leave the Node Name filter blank to return all Node Name results or power-on the virtual machine to be detected.
- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This will filter all reports based upon the selected node tier.

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

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.
- **Last (number of) Days**--Specifies a preset listing of the most commonly used data collection time periods (1, 3, 7 (default), and 30 days) to select from. You can also manually enter a value in this field.
- Virtual Machine Type--Specifies the type of virtual machine for the node you want to see the most recent backup status for.

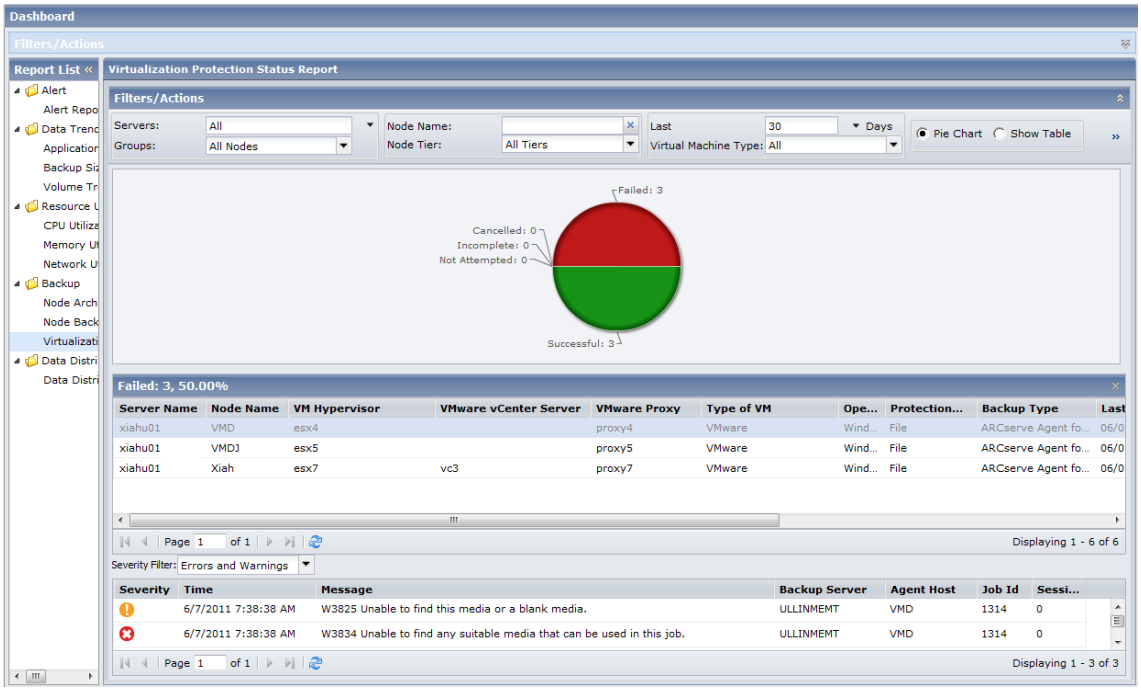
The pie chart is divided into a series of sectors: Successful, Incomplete, Failed, Cancelled, and Not Attempted. Each sector represents a percentage of the particular virtual machine being monitored. For more details on each sector, see Virtualization Protection Status Drill Down Report (see page 77).


Dashboard
Filters/Actions
Servers:
All
Groups:
All Nodes
Last
7
Days
Node Tier:
All Tiers
Report List
Alert
Alert Re
Data Tre
Applicat
Backup
Volume
Resourc
CPU Util
Memory
Network
Backup
Node Ar
Node Ba
Virtualiz
Data Dis
Data Dis
Virtualization Protection Status Report
Filters/Actions
Servers:
All
Groups:
All Nodes
Node Name:
Node Tier:
All Tiers
Last
60
Days
Virtual Machine Type:
All
Pie Chart
Show Tab
Not Attempted: 0
Incomplete: 1
Cancelled: 0
Failed: 3
Successful: 26

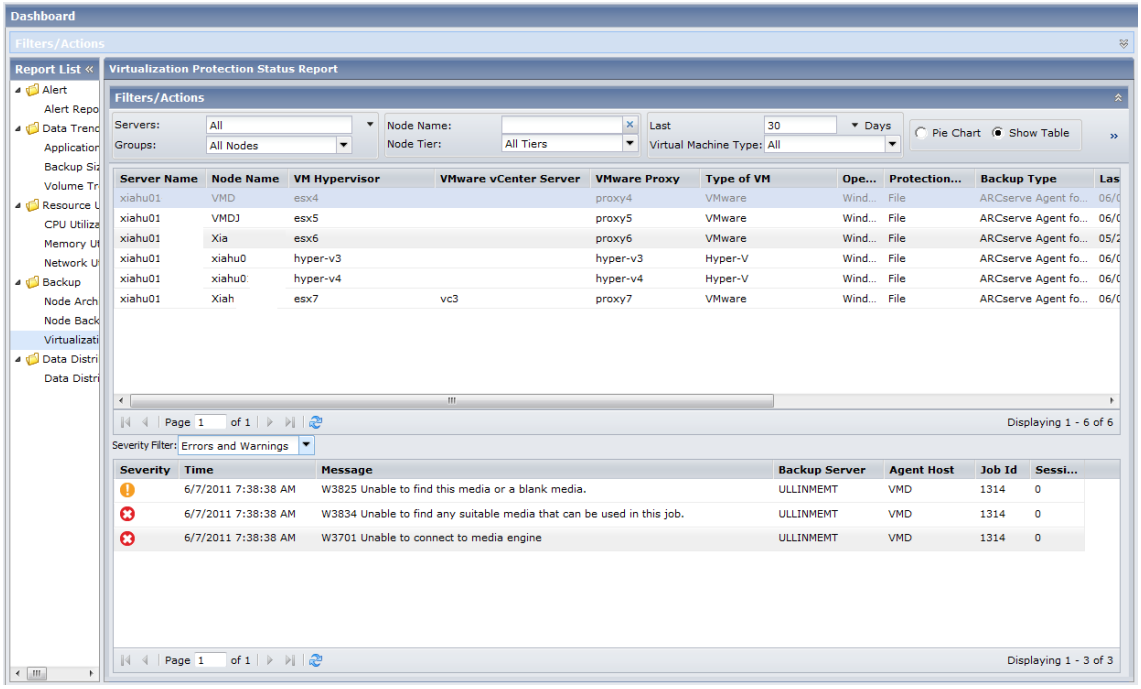
Virtualization Protection Status Drill Down Report

The Virtualization Protection Status Report can be further expanded from the Pie chart or Show Table view to display a drill-down report filtered by the selected category.

The following sample contains detailed information for the Virtualization Protection Status Report in Pie view:



The following sample contains detailed information for the Virtualization Protection Status Report in Table view:



The drill-down report includes the following information for each column name based on the type of backup job performed:

Note: To retrieve data for the type of backup job performed, do the following:

- **CA ARCserve Backup Agent for Virtual Machines**--Add the CA ARCserve Backup primary server to CA ARCserve Central Protection Manager and perform the CA ARCserve Backup synchronization.
- **CA ARCserve Central Host-Based VM Backup**--Add the proxy server to CA ARCserve Central Protection Manager and perform the CA ARCserve D2D synchronization.
- **CA ARCserve Central Virtual Standby**--Add CA ARCserve D2D nodes to the CA ARCserve Central Protection Manager and perform the CA ARCserve D2D synchronization.

Column Name	CA ARCserve Backup Agent for Virtual Machines	CA ARCserve Central Host-Based VM Backup	CA ARCserve Central Virtual Standby
Server Name	<CA ARCserve Backup Primary Server Host Name>	<Proxy Host Name>	<Source Host Name>
Nodes Name	<Virtual Machine Host Name>	<Virtual Machine Host Name> (Power-on virtual machine)	<Source Host Name>

Column Name	CA ARCserve Backup Agent for Virtual Machines	CA ARCserve Central Host-Based VM Backup	CA ARCserve Central Virtual Standby
Virtual Machine Hypervisor	<Virtual Machine name of the Hyper-V server> (via Hyper-V) <Virtual Machine name of the ESX server> (via ESX/ESXi) <Virtual Machine name of the ESX server> (via vCenter)	<Virtual Machine name of the ESX server> (via vCenter) <Virtual Machine name of the ESX server> (via ESX/ESXi)	<Virtual Machine name of the ESX server> (via vCenter) <Virtual Machine name of the ESX server> (via ESX) <Virtual Machine name of the Hyper-V server> (via Hyper-V)
VMware vCenter Server	<Virtual Machine name of the vCenter server provided by the user>	<Virtual Machine name of the vCenter server provided by the user>	<Virtual Machine name of the vCenter server provided by the user>
VMware Proxy	<Proxy Host Name>	<Proxy Host Name>	<Monitor Host Name> **Note**: The <Monitor Host Name> is displayed only if it is used as a proxy for data transfer.
Type of Virtual Machine	'VMware' or 'Hyper-V'	'VMware'	'VMware' or 'Hyper-V'
Operating System	'Windows' or 'Linux'	'Windows'	'Windows'
Protection Mode	'RAW' or 'File' (based on backup type)	'CA ARCserve Central Host-Based VM Backup'	'CA ARCserve Central Virtual Standby'
Backup Type	'CA ARCserve Backup Agent for Virtual Machines'	'CA ARCserve Central Host-Based VM Backup'	'CA ARCserve Central Virtual Standby on VMware' or 'CA ARCserve Central Virtual Standby on Hyper-V'
Last Backup Time	<Time of last backup>	<Time of last backup>	<Time of last conversion>
Type of Recovery	'RAW' or 'File' (based on backup type)	'VM/File/App' (Power-on virtual machine) or 'VM' (Power-off virtual machine)	'Power-on VM' (Power-on virtual machine) or 'V2P' (Virtual to Physical)
Most Recent Recovery Point	<Time of the most recent recovery point>	<Time of the most recent recovery point>	<Time of the most recent conversion>
Last Backup Status	'Successful', 'Failed', or 'Cancelled'	'Successful', 'Failed', or 'Cancelled'	'Successful', 'Failed', or 'Canceled'

You can find descriptions for each field below:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
  - For virtual machines protected by CA ARCserve Central Host-Based VM Backup, the Server Name field displays the host name of the proxy.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
  - For power-on virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays the host name of the virtual machine.
  - For power-off virtual machines protected by CA ARCserve Central Host-Based VM Backup, this field displays 'Unknown (*virtual machine name*)'.
- **Virtual Machine Hypervisor**--Indicates the type of server, whether it is an ESX or Hyper-V, the virtual machine is hosted on.
- **VMware vCenter Server**--Indicates the name of the VMware vCenter used for the particular node.

  Note: VMware vCenter Server allows for the management of multiple ESX servers and virtual machines (VMs) from different ESX servers through a single console application.
- **VMware Proxy**--Indicates the name of the VMware Proxy for the particular virtual machine.
- **Type of Virtual Machine**--Indicates the type of virtual machine being monitored. The virtual machine types can be Hyper-V or VMware.
- **Operating System**--Indicates the type of operating system.
- **Protection Mode**--Indicates the type of Protection mode of the virtual machine. The Protection Mode can be Raw, File, Host Based VM backup, or Virtual Standby Machine.
- **Backup Type**--Indicates the type of protection for the node.
- **Last Backup Time**--Indicates the date and time of the last backup.
- **Type of Recovery-**-Indicates the type of recovery. The recovery types can be: Raw, File, VM/File/APP, Power-on VM, or V2P (Virtual to Physical).
- **Most Recent Recovery Point**--Indicates the date and time of the most recent recovery point of the virtual machine.
- **Last Backup Status**--Indicates the status of the last virtual machine backup.

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:

- You can drill into each column name to sort in ascending or descending order and have the option to view any of the columns on the screen. All columns are enabled by default.
- CA ARCserve Central Reporting 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.

Data Distribution on Media Report

The Data Distribution on Media Report displays the amount and distribution of data that was backed up to a File System Device media during the last specified number of days. This report also shows a comparison of the raw data size to the compressed data size (in GB).

Data Distribution on Media Report Benefits

The Data Distribution on Media Report is helpful in analyzing all servers within your CA ARCserve Backup Domain and CA ARCserve D2D server 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 the savings in backup size can also result in a savings of the needed backup resources.

Data Distribution on Media Report View

The Data Distribution on Media Report is displayed in a bar chart format, showing the amount of backup data (in GB) within your CA ARCserve Backup Domain and CA ARCserve D2D server that has been distributed on one of the following devices during the last specified number of days:

- File System Device
- Deduplication
- Tape
- Cloud
- D2D Disk

Each device is divided into two separate categories for comparing the savings of compressed data size and raw data size.

The report contains the following filters:

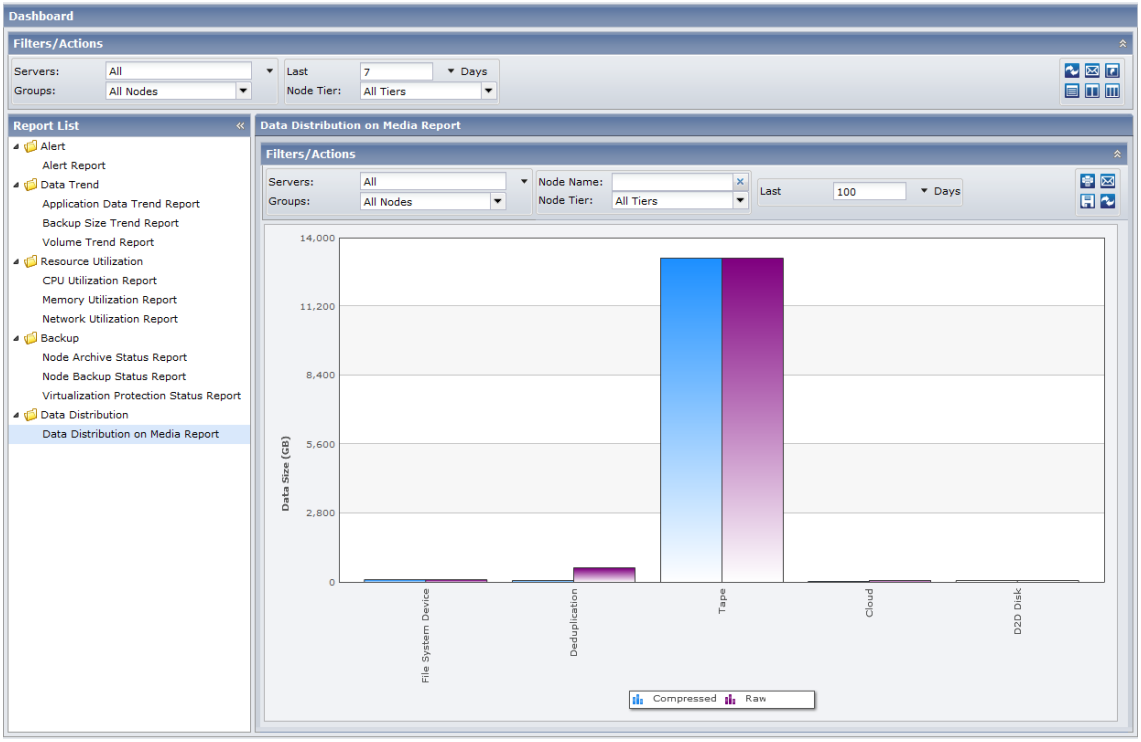
- **Servers**--Specifies All or specific nodes added from CA ARCserve Central Protection Manager.
- **Groups**--Specifies All or specific application types and names of CA ARCserve Backup and CA ARCserve Central Protection Manager default and custom groups.
- **Node Name**--Specifies the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.

- **Node Tier**--Specifies the tier category for the nodes you want to monitor. This filters all reports based upon the selected node tier.

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

  Note: The tier for CA ARCserve D2D nodes is Medium Priority.

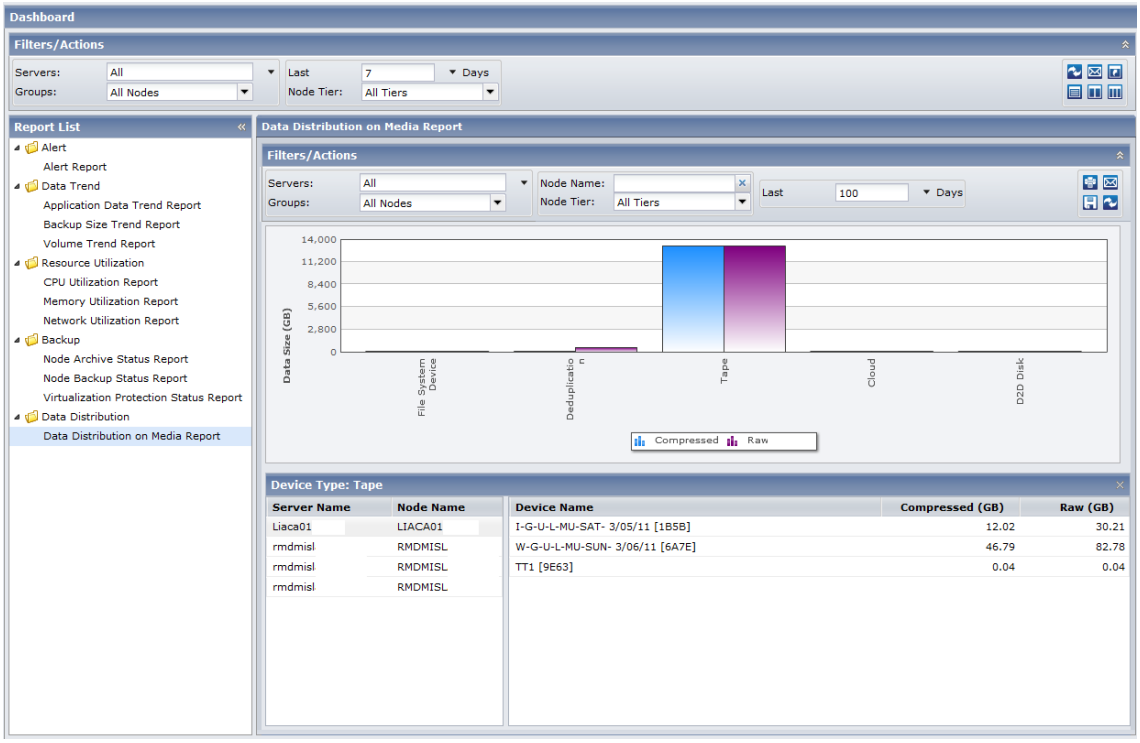
- **Last (number of) Days**--Specifies a preset listing of the most commonly used data collection time periods (1, 3, 7 (default), and 30 days) to select from. You can also manually enter a value in this field.



Data Distribution on Media Drill Down Report

The Data Distribution on Media Report can be further expanded to display more detailed information. You can click any device for compressed data size or raw data size to view the comparison in savings between the two.

The following sample contains detailed information for the Data Distribution on Media Report:



The drill-down report includes the following:

- **Server Name**--Displays one of the following server names, based on the backup performed:
  - For CA ARCserve Backup nodes, the Server Name field displays the name of the CA ARCserve Backup primary server, standalone server, or central primary server (of a Global Dashboard) where the node is protected.
  - For CA ARCserve D2D nodes, the Server Name field displays the host name of the CA ARCserve D2D node where CA ARCserve D2D backup and file copy is performed.
- **Node Name**--Indicates the name of the agent node or the member server for CA ARCserve Backup or the name of the CA ARCserve D2D node.
- **Device Name**--Indicates the name of the selected device from the bar chart.

- **Compressed (GB)**--Indicates the compressed data size of the device.
- **Raw (GB)**--Indicates the raw data size of the device.

Note: You can drill into each column name to sort in ascending or descending order and view any of the columns on the screen. All columns are enabled by default.

View CA ARCserve Central Reporting Logs

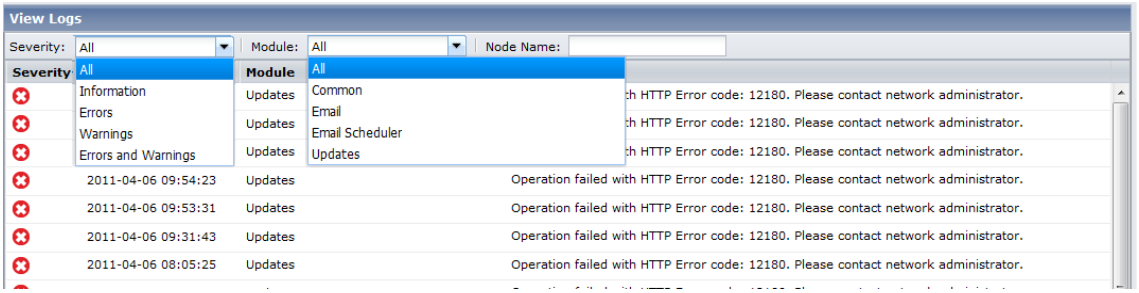
The View Log contains comprehensive information about all the operations performed by your application. The log provides an audit trail of every job that is run (with the most recent activities listed first) and can be helpful in troubleshooting any problems that may occur.

To view CA ARCserve Central Reporting logs

1. From the home page, click View Logs in the navigation bar.

   The View Logs screen appears.

Equation 1: View Logs



2. From the drop-down lists, specify log information that you want to view.

   - **Severity--**Lets you specify the severity of the log that you want to view. You can specify the following severity options:
     - **All--**Lets you view all logs, regardless of the severity.
     - **Information--**Lets you view only logs that describe general information.
     - **Errors--**Lets you view only logs that describe severe errors that occurred.
     - **Warnings--**Lets you view only logs that describe warming errors that occurred.
     - **Errors and Warnings--**Lets you view only severe errors and warning errors that occurred.
   - **Module--**Lets you specify the module for which you want to view logs. You can specify the following module options:
     - **All--**Lets you view logs about all application components.
     - **Common--**Lets you view logs about common processes.
     - **Email**--Lets you view only logs on sent and received emails.
     - **Email Scheduler**--Lets you view only logs about scheduled emails.
     - **Updates--**Lets you view only logs about updating the application.
   - **Node Name--**Lets you view only logs for a specific node.

     Note: This field supports the wildcard '*' and '?'. For example, enter 'lod*' to return all activity logs for the machine name that begins with 'lod'.

   Note: The Severity, Module, and Node Name options can be applied collectively. For example, you can view Errors (severity) that relate to Updates (Module) for Node X (Node Name).

   Click Refresh. 

   The logs display based on the view options specified.

   Note: The displayed Time in the log is based on the current time zone where the CA ARCserve Central Protection Manager application resides.

Add Links to the Navigation Bar

Each of the CA ARCserve Central Applications has an Add New Tab link in the Navigation bar. Use this feature to add entries in the Navigation bar for additional web-based applications you would like to manage. However, for every application that is installed, a new link is automatically added to the Navigation bar. For example, if you installed CA ARCserve Central Reporting and CA ARCserve Central Virtual Standby on "Computer A" and then launch CA ARCserve Central Reporting, CA ARCserve Central Virtual Standby is automatically added to the Navigation bar.

Note: Every application that is installed is detected only if other CA ARCserve Central Applications are on the same computer.

Follow these steps:

1. From the Navigation bar of the application, click the Add New Tab link.
2. Specify the Name and URL of the application or website you want to add. For example, www.google.com.

   Optionally, specify the location of an icon.
3. Click OK.

   The new tab is added to the bottom of the Navigation bar.

Be aware of the following considerations:

- The CA Support link is added by default for your convenience.

You can remove the new tab by highlighting the tab and click the Remove link.

Reporting Tasks

CA ARCserve Central Reporting provides reporting tasks that are beneficial to you. Just to name a few, you can email multiple reports on a scheduled basis, view multiple reports at a time, or export data on the reports you select as a CSV file for use in a spreadsheet.

This section contains the following topics:

Schedule Reports by Email

CA ARCserve Central Reporting lets you create a schedule to send reports by email to specified recipients. These report emails are automatically updated, generated, and sent as scheduled. You can customize the schedule of the report email messages. The application lets you define the email contents, the reports to attach, to whom to send the reports, and the date and time to send the report. The selected reports display detailed information in table format within the email.

Note: Before an email can be sent, configure the Email settings. For more information, see Configure Email Settings (see page 25).

Follow these steps:

1. Log in to the CA ARCserve Central Reporting server.

   Click Dashboard on the Navigation bar to open the Dashboard screen.

2. Click the email icon located in the upper right corner of the global Filters/Actions section to open the Schedule Emails dialog.

3. Click New on the Schedule Emails dialog to open the New Schedule dialog.

   The following tabs are displayed:

   - **General**--Specify a name and description (optional) for the new schedule.
   - **Email**--Specify the mail settings and content for the email schedule.
   - **Reports**--Select the specific reports that you want to include in the email.
   - **Schedule**--Specify a schedule for the email.

4. Complete the required fields in each tab.

5. Click OK to save the schedule.

Send Individual Reports by Email

CA ARCserve Central Reporting lets you send individual reports to specific recipients. When 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 individual reports by email

1. Login to the CA ARCserve Central Reporting server and click Dashboard on the Navigation bar.

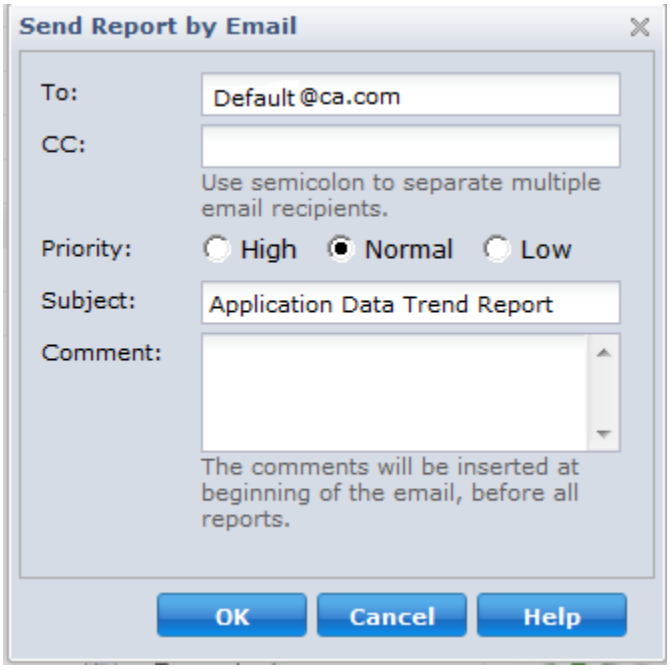
   The Dashboard screen displays.

2. Select a report you want to email from the Report List.

   The selected report is displayed in the Report View.

3. Click on the email icon located in the upper right corner of the local Filters/Actions section.

   The Send Report by Email dialog opens.



4. Complete the following fields:

   - **To**--Specify the recipient the email is sent to.

     Note: This field defaults to the email address specified in the Email Configuration module.

   - **CC**--Specify other recipients, separated by semicolons, you would like to email the report to.

   - **Priority**--Specify the priority of the email. This field defaults to Normal.

- **Subject**--Specify the subject of the email. This field defaults to the report you selected.
- **Comment** (optional)

5. Click OK.

The email is sent successfully.

View Multiple Reports at a Time

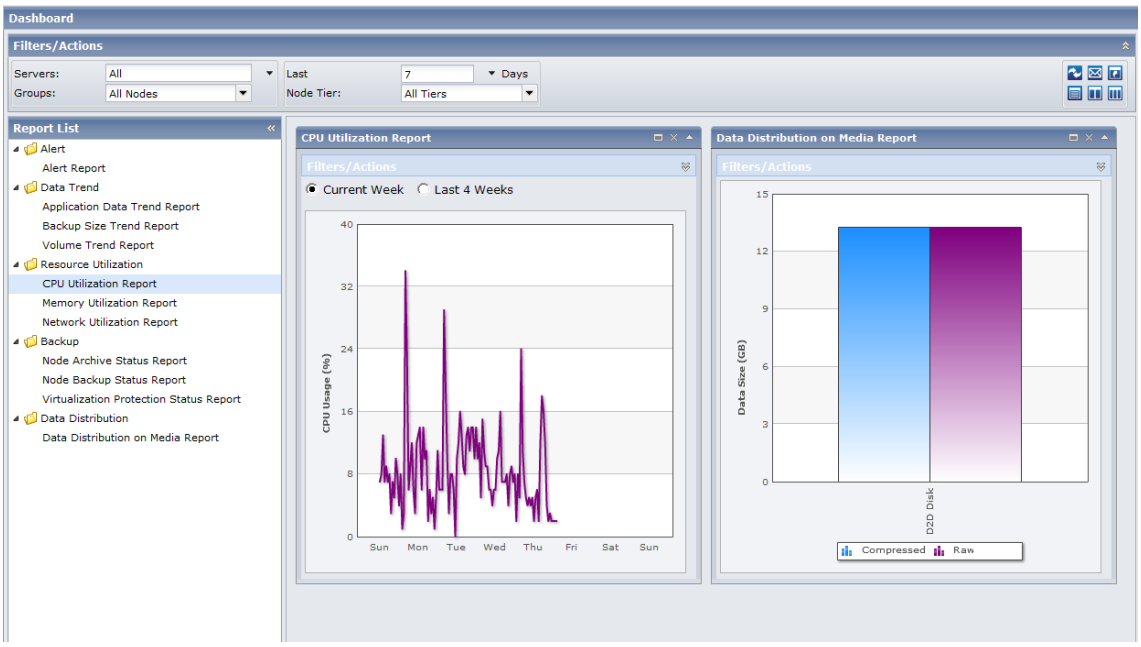
CA ARCserve Central Reporting lets you view multiple reports that can fit in the Report View screen as wide as three columns. There are three icons you can choose from in the upper right corner of the global Filters/Actions section of the Dashboard screen.

-  Report view show only one report

  Displays only one report in the Report View screen.

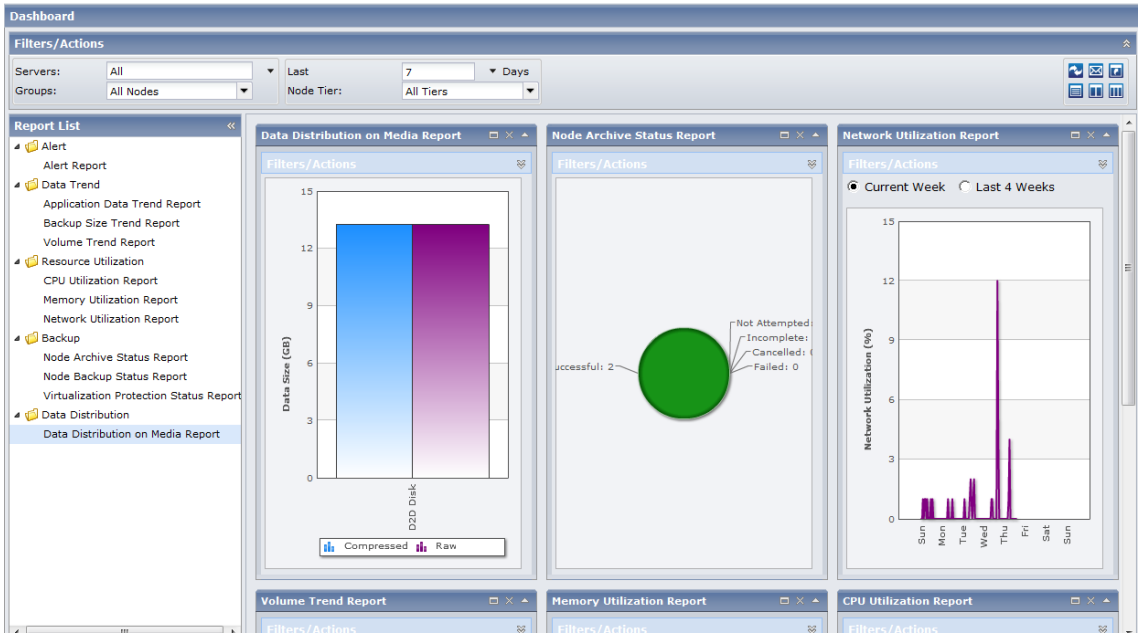
-  Report view show multiple reports in two columns

  Select as many reports from the Report List to view as wide as two columns in the Report View. You can scroll down to view the reports selected.



- Report view show multiple reports in three columns

  Select as many reports from the Report List to view as wide as three columns in the Report View. You can scroll down to view the reports selected.



Save Reports as a CSV File

CA ARCserve Central Reporting 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.

To save reports as a CSV file

1. Login to the CA ARCserve Central Reporting server and click Dashboard on the Navigation bar.

   The Dashboard screen displays.

2. Select the report you want to save from the Report List.

   The selected report is displayed in the Report View.

3. Click on the save icon  located in the upper right corner of the local Filters/Actions section.

   The File Download dialog opens.

4. Click Open to open the file.

   The file opens in Excel.

5. Review the file and save.

The data is saved as a CSV file and is ready for print or email.

Change Server Communication Protocol

By default, CA ARCserve Central Applications use the Hypertext Transfer Protocol (HTTP) for communication among all of its components. If you are concerned about the security of passwords that are communicated between these components, you can change the protocol being used to Hypertext Transfer Protocol Secure (HTTPS). When you do not need this extra level of security, you can change the protocol being used to HTTP.

Follow these steps:

1. Log in to the computer where the application is installed using an administrative account or an account with administrative privileges.

   Note: If you do not log in using an administrative account or an account with administrative privileges, configure the Command Line to run using the Run as Administrator privilege.

2. Open Windows Command Line.

3. Do one of the following:

   - **To change the protocol from HTTP to HTTPS:**

     Launch the "changeToHttps.bat" utility tool from the following default location (the location of the BIN folder can vary depending upon where you installed the application):

     C:\Program Files\CA\ARCserve Central Applications\BIN

     When the protocol has been successfully changed, the following message displays:

     The communication protocol was changed to HTTPS.

   - **To change the protocol from HTTPS to HTTP:**

     Launch the "changeToHttp.bat" utility tool from the following default location (the location of the BIN folder can vary depending upon where you installed the application):

     C:\Program Files\CA\ARCserve Central Applications\BIN

     When the protocol has been successfully changed, the following message displays:

     The communication protocol was changed to HTTP.

4. Restart the browser and reconnect to CA ARCserve Central Applications.

   Note: When you change the protocol to HTTPS, a warning displays in the web browser. This behavior occurs because of a self-signed security certificate that prompts you to ignore the warning and proceed or add that certificate to the browser to prevent the warning from coming back in future.

Chapter 5: Troubleshooting CA ARCserve Central Reporting

This section provides troubleshooting information to help you identify and resolve problems that you can encounter when using CA ARCserve Central Reporting.

This section contains the following topics:

Reports Do Not Display In Internet Explorer

Valid on Windows Server 2008 and Windows Server 2003 operating systems.

Symptom:

When you open CA ARCserve Central Applications websites or view CA ARCserve Central Reporting reports using Internet Explorer, blank web pages appear or Javascript errors occur. The problem occurs when opening Internet Explorer on Windows Server 2008 and Windows Server 2003 operating systems.

This problem occurs under the following conditions:

- You are using Internet Explorer 8 or Internet Explorer 9 to view reports, and the browser does not recognize the URL as a trusted site.
- You are using Internet Explorer 9 to view the reports, and the communication protocol in use is HTTPS.

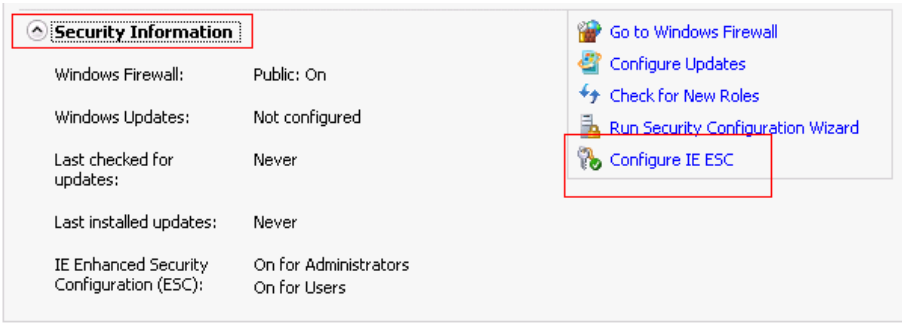
Solution:

To correct this problem, disable Internet Explorer Enhanced Security on the computers that you use to view the reports.

To disable Internet Explorer Enhanced Security on Windows Server 2008 systems, do the following:

1. Log on to the Windows Server 2008 computer that you use to view reports using the Administrator account or an account that has administrative privileges.
2. Right-click Computer on the desktop and click Manage to open the Server Manager window.
3. From the Server Manager window, click Server Manager (Server Name).

   From the Server Summary section, open Security Information and click Configure IE ESC as illustrated by the following:



   The Internet Explorer Enhanced Security Configuration dialog opens.

4. On the Internet Explorer Enhanced Security Configuration dialog, do the following:
   - Administrators--Click Off
   - Users--Click Off.

   Click OK.

The Internet Explorer Enhanced Security Configuration dialog closes and Internet Explorer Enhanced Security is disabled.

To disable Internet Explorer Enhanced Security on Windows Server 2003 systems, do the following:

1. Log on to the Windows Server 2003 computer that you use to view reports using the Administrator account or an account that has administrative privileges.
2. Open Windows Control Panel and then open Add or Remove Programs.
3. From the Add or Remove Programs dialog, click the Add/Remove Windows Components option to access the Windows Components Wizard screen.

   Clear the checkmark next to Internet Explorer Enhanced Security Configuration.

   Click Next.

   Follow the on-screen instructions to complete the configuration and then click Finish.

Internet Explorer Enhanced Security is disabled.

How to Troubleshoot Page Loading Problems

Valid on Windows platforms.

Symptom:

The following error messages appear in browser windows when you log in to CA ARCserve Central Applications, CA ARCserve D2D nodes, and monitoring servers.

Message 1:

Errors on this webpage might cause it to work incorrectly.

Message 2:

!

Solution:

Web pages do not load properly for many reasons. The following table describes common reasons and the corresponding corrective actions:

Reason	Corrective Action
There are problems with the underlying HTML source code.	Refresh the webpage and try again.
Your network blocks Active scripting, ActiveX, or Java programs.	Allow your browser to use Active scripting, ActiveX, or Java programs.

Reason	Corrective Action
Your antivirus application is configured to scan temporary Internet files and downloaded programs.	Filter your antivirus application to allow Internet-related files associated with CA ARCserve Central Applications webpages.
The scripting engine installed on your computer is corrupt or outdated.	Update the scripting engine.
The video card drivers installed on your computer are corrupt or outdated.	Update the video card drivers.
The DirectX component installed on your computer is corrupt or outdated.	Update the DirectX component.

Garbage Characters Appear in Browser Windows When Accessing CA ARCserve Central Applications

Valid on all Windows operating systems. All browsers affected.

Symptom:

When you log in to CA ARCserve Central Applications, garbage characters appear in the content area of your browser window.

Solution:

This problem occurs when you install CA ARCserve Central Applications using HTTPS communication and then try to access CA ARCserve Central Applications using HTTP communication. The underlying CA ARCserve Central Applications web services component does not support the capability to convert HTTP URLs to HTTPS URLs. As a result, garbage characters appear in your browser window. For example:

To correct this problem, access CA ARCserve Central Applications using HTTPS when you install or configure the applications to communicate using HTTPS.

Certificate Error Appears When You Log In to the Application

Valid on Windows platforms.

Symptom:

The following message appears in your browser window when you log in to the application:

- Internet Explorer:

  There is a problem with this website's security certificate.

- Firefox:

  This connection is untrusted.

- Chrome:

  This site's security certificate is not trusted!

If you specify an option that lets you continue to the website, you can log in to the application successfully. However, you encounter this behavior every time you log in to the application.

Solution:

This behavior occurs when you specify to use HTTPS as the communication protocol. To correct this problem temporarily, click the link in your browser window that lets you continue to the website. However, the next time that you log in to the application, you will encounter the message again.

HTTPS communication protocol provides a higher level of security than HTTP communication protocol. If you want to continue to communicate using HTTPS communication protocol, you can purchase a security certificate from VeriSign and then install the certificate on the application server. Optionally, you can change the communication protocol used by the application to HTTP. To change the communication protocol to HTTP, do the following:

1. Log in to the server where you installed the application.
2. Browse to the following directory:

   C:\Program Files\CA\ARCserve Central Applications\BIN
3. Execute the following batch file:

   ChangeToHttp.bat
4. After the batch file executes, open Windows Server Manager.

   Restart the following service:

   CA ARCserve Central Applications Service

Nodes Do Not Appear in Reports After Changing the Name of the Node

Valid on Windows platforms.

Symptom:

The host name of the node was changed after it was added to the Node screen. The node no longer appears on the Node screen.

Solution:

This behavior is expected. CA ARCserve Central Reporting retains the name of the node as it was added from the node screen in CA ARCserve Central Protection Manager. When you rename the node, CA ARCserve Central Reporting cannot detect the node to generate reports about the node.

To correct this problem, do the following:

1. Rename the node.
2. Open the Node screen on the CA ARCserve Central Protection Manager server and delete the node that was renamed.
3. Add the node using its new name.

Note: For information about adding and deleting nodes on the Node screen, see the *CA ARCserve Central Protection Manager User Guide*.

Exporting Data to Microsoft Excel in CSV Format Displays Illegible Content

Valid on Windows platforms.

Symptom:

When I open my report saved in CSV format in Microsoft Excel, it displays illegible content.

Solution:

This behavior is expected in certain types of languages for Microsoft Excel where the file includes multi-byte characters. To resolve this, use the Text Import Wizard feature provided by Microsoft Excel.

Configuration Error Message Appears After Successfully Connecting to CA ARCserve Central Protection Manager

Valid on Windows platforms.

Symptom:

The following error message appears after specifying valid CA ARCserve Central Protection Manager information on the CA ARCserve Central Reporting Configuration screen:

CA ARCserve Central Protection Manager successfully connected but failed to connect to the CA ARCserve Central Protection Manager database. Refer to the CA ARCserve Central Reporting User Guide for help.

Solution:

To correct this problem, do the following:

1. Map the Windows user that is set up CA ARCserve Central Reporting, to the SQL Server where CA ARCserve Central Protection Manager is connected to.
2. Configure the CA ARCserve Central Protection Manager application to connect to the database and verify that SQL Server and Windows Authentication Mode is selected.

Add New Tab Link Not Launching Properly for Internet Explorer 8, 9, and Chrome

Valid on Windows

Symptom:

When I add a new tab link to the Navigation bar specifying an HTTPS URL, the following error messages appear when I click the new tab:

- Internet Explorer 8 and 9:

  Content was blocked because it was not signed by a valid security certificate.

- Chrome:

  The webpage is not available.

Solution:

To correct this problem for Internet Explorer, do the following:

- Internet Explorer 8:

  Click on the message bar and select "Display Blocked Content".

- Internet Explorer 9:

  Click the "Show content" button from the message bar at the bottom of the page. The page refreshes and the added tab link opens successfully.

To correct this problem for Chrome, perform the following steps:

Step 1 - Export Certificate:

1. Open a new tab in Chrome and enter the HTTPS URL.

   A warning message appears, "The site's security certificate is not trusted!"

2. From the address bar, click the lock with the 'X'.

   A pop-up window opens with a Certification Information link.

3. Click the Certificate Information link.

   The Certificate dialog opens.

4. Click the Details tab and then click Copy to File, to save the certificate to your local computer.

   The Certificate Export Wizard dialog opens.

5. Click Next to select the format you want to use to export the file.

   Note: DER encoded binary X.509 (.CER) is selected by default.

6. Click Next to browse to a location where you want to save the certificate.

7. Click Next to complete the Certificate Export Wizard and then click Finish.

The certificate exports successfully.

Step 2 - Import Certificate:

1. Open the Tools Options from Chrome.

   The Options screen opens.

2. Select the Under the Hood option and click Manage Certificates from HTTPS/SSL.

   The Certificates dialog opens.

3. Click Import.

   The Certificate Import Wizard dialog opens.

4. Click Next to browse for the certificate you saved on your local computer.

5. Click Next to open the Certificate Store.

   The Certificate Store dialog opens.

6. Click Browse to open the Select Certificate Store dialog.

   The Select Certificate Store dialog opens.

7. Select Trusted Root Certification Authorities from the file list and click OK.

   The Certificate Store dialog appears.

8. Click Next to complete the Certificate Import Wizard and then click Finish.

   A Security Warning dialog opens stating that you are about to install a certificate.

   Click Yes to agree on the terms.

The certificate imports successfully.

Add New Tab Link, RSS Feeds, and Social Networking Feedback Not Launching Properly on Internet Explorer 8 and 9

Valid on Windows

Symptom:

For an HTTPS CA ARCserve Central Applications URL:

When I add a new tab link to the Navigation bar specifying an HTTP URL, the following error message appears when I click the new tab and the Feedback link:

> Navigation to the webpage was canceled.

In addition, the RSS Feeds are not displayed.

Note: The Feedback link also displays the error message even if you do not select the new added tab link.

Solution:

To correct this problem, do the following:

- Internet Explorer 8:

  After you log in, click No on the pop-up security warning message, "Do you want to view only the webpage content that was delivered securely?" By clicking No allows the delivery of unsecured content to your webpage.

- Internet Explorer 9:

  Click the "Show all content" button on the message bar displayed at the bottom of the page. The page refreshes and the added tab link opens successfully.

Chapter 6: Applying Best Practices

This section contains the following topics:

How the Installation Process Affects Operating Systems

The CA ARCserve Central Applications installation process updates various Windows operating system components using an installation engine named the Microsoft Installer Package (MSI). The components included in MSI let CA ARCserve Central Applications perform custom actions that let you install, upgrade, or uninstall CA ARCserve Central Applications.

The following table describes the custom actions and the affected components.

Note: All CA ARCserve Central Applications MSI packages call the components listed in this table when you install and uninstall CA ARCserve Central Applications.

Component	Description
CallAllowInstall	Lets the installation process check for conditions relating to the current CA ARCserve Central Applications installation.
CallPreInstall	Lets the installation process read and write MSI properties. For example, read the CA ARCserve Central Applications installation path from the MSI.
CallPostInstall	Lets the installation process perform various tasks relating to installation. For example, registering CA ARCserve Central Applications into the Windows Registry.
CallAllowUninstall	Lets the uninstallation process check for conditions relating the current CA ARCserve Central Applications installation.
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering CA ARCserve Central Applications from the Windows Registry.
CallPostUninstall	Lets the uninstallation process perform various tasks after the installed files are uninstalled. For example, removing the remaining files.

Component	Description
ShowMsiLog	Displays the Windows Installer log file in Notepad if the end user selects the Show the Windows Installer log check box in the SetupCompleteSuccess, SetupCompleteError, or SetupInterrupted dialogs and then clicks Finish. (This works only with Windows Installer 4.0.)
ISPrint	Prints the contents of a ScrollableText control on a dialog. This is a Windows Installer .dll custom action. The name of the .dll file is SetAllUsers.dll, and its entry point is PrintScrollableText.
CheckForProductUpdates	Uses FLEXnet Connect to check for product updates. This custom action launches an executable file named Agent.exe, and it passes the following: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Uses FLEXnet Connect to check for product updates on reboot. This custom action launches an executable file named Agent.exe, and it passes the following: /au[ProductCode] /EndOfInstall /Reboot

- **Directories Updated**--The installation process installs and updates CA ARCserve Central Applications files in the following directories by default:

  C:\Program Files\CA\ARCserve Central Applications

  You can install CA ARCserve Central Applications into the default installation directory or into an alternative directory. The installation process copies various system files to the following directory:

  C:\WINDOWS\SYSTEM32

- **Windows Registry Keys Updated**--The installation process updates the following Windows registry keys:

  Default registry keys:

  HKLM\SOFTWARE\CA\CA ARCserve Central Applications

  The installation process creates new registry keys and modifies various other registry keys, based on the current configuration of your system.

- **Applications Installed**--The installation process installs the following applications into your computer:
  - CA Licensing
  - Microsoft Visual C++ 2005 SP1 Redistributable
  - Microsoft Windows Installer 3.1 Redistributable (v2) Package
  - Java Runtime Environment (JRE) 1.6.0_16
  - Tomcat 6.0.32

Binary Files Containing Incorrect File Version Information

CA ARCserve Central Applications installs binary files that are developed by third parties, other CA products, and CA ARCserve Central Applications that contain incorrect file version information. The following table describes these binary files.

Binary Name	Source
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

Binary Files that Do Not Contain an Embedded Manifest

CA ARCserve Central Applications installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve Central Applications that do not contain an embedded manifest and do not contain a text manifest. The following table describes these binary files.

Binary Name	Source
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Binary Files that have a Privilege Level of Require Administrator in Manifest

CA ARCserve Central Applications installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve Central Applications that have a privilege level of Administrator or Highest Available. You must log in using an administrative account or an account with the highest available permissions to run various CA ARCserve Central Applications services, components, and applications. The binaries corresponding to these services, components, and applications contain CA ARCserve Central Applications specific functionality that is not available to a basic user account. As a result, Windows will prompt you to confirm an operation by specifying your password or by using an account with administrative privileges to complete the operation.

- **Administrative Privileges--**The administrative profile or an account with administrative privileges has read, write, and execute permissions to all Windows and system resources. If you do not have Administrative privileges, you will be prompted to enter user name / password of an administrator user to continue.
- **Highest Available Privileges--**An account with the highest-available privileges is a basic user account and a power user account with run-as administrative privileges.

The following table describes these binary files.

Binary Name	Source
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Binary Name	Source
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Index

N

P

R

S

T

U

V