Dell™ Management Console

Version 1.1

User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: —A WARNING indicates a potential for property damage, personal injury, or death.

March 2010

Contents

1

Introduction

Dell™ Management Console is a one-to-many systems management application that provides enhanced discovery, inventory, monitoring, patch updates, and reporting features.

Dell Management Console is a Web-based graphical user interface (GUI) with a scalable, modular console for basic hardware management as well as advanced functions, such as asset management, enhanced security, and compliance. You can install Dell Management Console on a management station in a networked environment.

Dell Management Console is a free software that you can download from the Dell Support website at support.dell.com; however, you must register at the Dell website at **dell.com/openmanage/register** for a free permanent license. The registration enables you to continue using Dell Management Console after the 30-day trial period. Dell Management Console also supports a variety of Symantec™ plug-ins like the Symantec Server Management Suite.

NOTE: As Symantec Inc. acquired Altiris Inc. this document may contain references to Altiris™ and Symantec.

New Features in This Release

In this release, the following features are available:

- Power Monitoring — Enables you to monitor a standard set of power consumption counters for devices.
- Lifecycle Controller enabled Patch Updates — Enables you to perform patch updates for servers with Lifecycle Controller version 1.3 and Integrated Dell Remote Access Controller (iDRAC) version 6.
- Health Monitor E-mail Task — Enables you to configure Dell Management Console to send e-mail alerts on the status of preselected devices' health to specific users.
- You can gather inventory information for Dell EqualLogic devices. For more information, see your Dell EqualLogic documentation available at support.dell.com/manuals.

For upgrading from earlier releases of Dell Management Console to this release, see the *Support Information Matrix for Dell Management Console Version 1.1*.

Getting Started With Dell Management Console

To install and set up Dell Management Console, consider the following process:

1 Plan the Dell Management Console installation — Plan the installation based on the following requirements:

- Network size
- Network devices that you want to manage and the protocols required to communicate with the network devices; for example, Simple Network Management Protocol (SNMP), Windows® Management Interface (WMI), Web Services for Management (WS-MAN), or the Intelligent Platform Management Interface (IPMI) protocols, and so on. For more information on the devices and the required protocols, see Table 5-1.
- Attributes that you want to monitor. For example, you can manage only the health, or health and performance of your devices.
- Tiered software deployment to a number of sites. For more information, see the Symantec documentation available from **Help→ Documentation Library** or **Help→ Context**.

For more information, see “Planning Your Dell Management Console Installation.”

2 Install Dell Management Console — You can install Dell Management Console using the *Dell Management Console* DVD or from the Dell website at **dell.com/openmanage**. For more information on installing the Dell Management Console, see “Installing, Uninstalling, and Upgrading Dell Management Console.”

3 Preparing to configure Dell Management Console — It is of utmost importance to *plan* for the configuration of Dell Management Console and your network devices. Plan to configure the following details:

- Discovery tasks, for example, defining Include ranges and Exclude ranges, such as IP addresses, subnets, host names, and custom ranges

- Types of devices on your network, both Dell and non-Dell
- Security of your devices
- Connection profiles and credentials. For more information, see "Connection Profiles and Credentials Management."

4 Configure Dell Management Console, in the following sequence:

   a Discovery tasks — Define a group of network devices that you want to discover.

   b Agent deploy — Deploy the Altiris Agent and then deploy the Dell OpenManage™ agent—Dell OpenManage Server Administrator (OMSA) on the target servers.

   c Inventory — Gather inventory information for memory, processor, power supply, embedded devices, and software and firmware versions. For more information, see "Configuring Inventory Settings."

   d Organize network devices — You can organize network devices based on organization or geographical location.

   e Status polling settings — Perform a power and connectivity health check for all discovered devices. This determines whether a device is operating normally, is in a non-normal state, or is powered down. For more information, see "Monitoring and Alerting."

   f Event management and alerting — Configure protocols.

   g Management Information Base (MIB) — If your network has non-Dell devices, import the appropriate MIBs to recognize the traps received from those devices. For more information, see "Importing MIBs."

   h Performance and health monitoring — Monitor real-time health and performance of network devices.

   i Patch management — Deploy updates to a single system or a group of systems at a time using the Altiris Agent or LC enabled patch updates.

   j Tasks — Configure groups of systems.

   k Reports — Choose methods to report results that are displayed on the Dell Management Console and set the default view for the reports.

Planning Your Dell Management Console Installation

This section answers some questions that you may have while planning for the Dell Management Console installation.

What are the basic hardware requirements for installing Dell Management Console?

Depending on your specific Dell Management Console deployment and your network environment, it is advisable to exceed the recommended configurations for processor speed, amount of memory, and hard-drive space.

Recommended Minimum Hardware Configuration

- Microsoft® Windows Server® 2003 R2 SP2 (32-bit) — Standard or Enterprise Editions
- Physical Processors — Two
- RAM — 4 GB
- DVD Drive
- Microsoft .NET Framework version 3.5 or 3.5 SP1
- Windows Internet Information Services version 6.0
- Microsoft SQL Express 2005 or SQL Express 2008, SQL Server 2005 or SQL Server 2008 (64-bit Remote)
- (Recommended) A remote database and at least 8GB memory available for larger environments

For more information, see **DellTechCenter.com**.

I have already installed the Microsoft SQL Server 2005 for Dell OpenManage IT Assistant. If I want to migrate to Dell Management Console, will this database work or should I install another database?

In general, the number of systems you expect to manage and the number of alerts you expect from your managed systems determine the database to use with Dell Management Console. If you manage less than 500 devices, you can use either SQL Express 2005 or SQL Server 2005 (32-bit).

Which systems management protocol(s) should I plan to install or enable?

In general, your choice of protocols is determined by the systems you want to monitor and the respective agent protocols they support. If the systems you want to monitor have agents that use the Simple Network Management Protocol (SNMP), Windows® Management Interface (WMI), Web Services for Management (WS-MAN), or the Intelligent Platform Management Interface (IPMI) protocols, then configure these protocols in Dell Management Console.

In Dell Management Console, you can configure a **Connection Profile** to include the protocols you require. Dell Management Console connects to the device on the network using the protocols you define in the **Connection Profile**.

How should I organize my managed systems' IP addresses if I am using more than one systems management protocol on a subnet?

Where possible, group systems using the same systems management protocol into contiguous subnets. This strategy increases manageability during the creation of Dell Management Console discovery ranges.

Is the performance of my monitoring network determined by the attributes I want to monitor?

Yes, the devices' attributes that you want to monitor determine the resources required. For example, to monitor only the health of your systems, the recommended minimum hardware configuration is sufficient. However, the configuration depends on the *number of systems* that you want to monitor.

To monitor the health and performance of your systems, it is advised that you exceed the recommended configuration. See "Recommended Minimum Hardware Configuration."

I have a multi-tiered network with management systems in various parts of the world. How would that affect the way I install Dell Management Console?

Having management stations in different parts of the world affects the way you install Dell Management Console. For more information, see the Symantec documentation on tiered infrastructure. Symantec documents are available in the **Help→ Documentation Library**.

Planning to Configure the Dell Management Console

After installing the Dell Management Console, you must plan to configure it.

My network has Dell and non-Dell devices. Should I configure them separately?

Yes, you must import the appropriate MIBs for all non-Dell devices that you want to monitor. Importing the MIBs for non-Dell devices will allow you to receive SNMP alerts for them.

What are the security options to be configured for using Dell Management Console?

See the Symantec documents available in the **Help→ Documentation Library** on role-based security.

I am migrating from Dell OpenManage IT Assistant. How do I migrate the discovery ranges to Dell Management Console?

For information on migrating the discovery settings from IT Assistant, see "Importing IT Assistant Discovery Settings."

Is there any special configuration required for the features I want to use?

You can configure any or all features according to your requirements. See Table 1-1 for the agents you should deploy on the managed devices for each feature to work properly.

Table 1-1. Supported Features by Agents

Feature	No Agent	Dell OpenManage Server Administrator	Altiris Agent
Discovery	Will discover through IPMI, WMI, or SNMP	Required for a detailed Hardware Summary in the Resource Manager	Not required
Inventory	Basic inventory through IPMI, WMI, or SNMP	Required for a detailed Hardware Summary in the Resource Manager	Not required

Table 1-1. Supported Features by Agents *(continued)*

Feature	No Agent	Dell OpenManage Server Administrator	Altiris Agent
Monitoring Health	Out-of-band health monitoring through IPMI*	Required for agent-based health monitoring through SNMP	Not required
Events and Alerting	Basic IPMI platform event traps (PET) only	Required for comprehensive hardware events	Not required
Hardware configuration tasks	NA	Required	Not required
Deploying the Dell agent—Server Administrator	NA	NA	Required
Patch (firmware/drivers/ BIOS) management	NA	NA	Required
Monitor Operating System Performance	Will monitor on Windows agentless through WMI/IPMI*	Required if IPMI* is not enabled/available	Required for systems running on Linux

* IPMI is available on Dell PowerEdge™ *x8xx* servers or later.

How can I enable my managed devices so I can manage them using Dell Management Console?

For Dell PowerEdge™ systems using the SNMP and WMI protocols, the Dell OpenManage™ Server Administrator should be installed on the managed system to get the most manageability.

You can manage other non-server devices if protocols and credentials have been correctly set up in Dell Management Console. For example, if you want to manage a network printer, it should be SNMP-enabled and the community string should be defined in Dell Management Console Connection Profile settings. For more information, see "Connection Profiles and Credentials Management."

Other Documents You May Need

You can access the following documents for your reference.

- Symantec documents are available under **Help→ Documentation Library**.
  - Symantec documentation includes documentation for Notification Server 7.0.
- Online Help is available under **Help→ Context**.
- *Support Information Matrix for Dell Management Console* is available on the Dell Support website at **support.dell.com/manuals**.
- For information on terms used in this document, see the *Glossary* on the Dell support website.
- For more information on Dell EqualLogic, see your Dell EqualLogic documentation available on the Dell Support website at support.dell.com/manuals.
- Additional documents are available on Dell Tech Center, **delltechcenter.com/page/Dell+Management+Console** and also on **en.community.dell.com/groups/.**
- For the latest software and user documentation for Navisphere CLI, see powerlink.emc.com.

2

Installing, Uninstalling, and Upgrading Dell Management Console

Dell™ Management Console uses the Symantec™ modular architecture to provide you with solutions that best fit your needs. The Dell Management Console is built on the Symantec infrastructure and leverages its key technologies for completing tasks, software deployment, and discovery and inventory of devices on the network.

The Symantec Installation Manager (SIM) is the installer for Dell Management Console. The SIM installer installs SIM on the management station and the SIM provides Dell Management Console as an installation option.

Installation Requirements

For information on the recommended hardware configuration, see "Recommended Minimum Hardware Configuration."

The management station on which you want to install the Dell Management Console should contain the following software prerequisites.

Symantec Installation Manager Prerequisites

Before you install Dell Management Console, you must install Microsoft® .NET Framework 3.5 (available on the *Dell Management Console* DVD) on the management station.

NOTE: If the prerequisites are not installed on the management station, the SIM installer (present on the *Dell Management Console* DVD) installs the prerequisites before proceeding to install the Dell Management Console.

Install Readiness Prerequisites

- Microsoft Windows Server® 2003 32-bit (Enterprise or Standard)
- Microsoft ASP .NET framework

- SQL Express 2005 Express for up to 500 managed systems

  Microsoft SQL Express 2008, SQL Server 2005 or SQL Server 2008 (64-bit Remote Only) for 500+ managed systems
- At least 8 GB of free disk space. 10 GB of free disk space is recommended.
- Internet Information Services 6.0
- Microsoft Internet Explorer® version 7.0 or 8.0

  For more information on the installation prerequisites see the *Support Information Matrix for Dell Management Console* Version *1.1*.

Other Considerations

- Do not configure the management station as a Windows Domain Controller.
- If you are installing the Dell Management Console through the Terminal Service, ensure that the installation is through the console session. For example, mstsc/console.
- (Highly recommended) On the management station, install configure and enable the HyperText Transfer Protocol over Secure Socket Layer (HTTPS).
- If you are upgrading to this release of Dell Management Console, then use SIM. SIM must be connected to internet for getting the latest updates. When you launch SIM, all the critical updates are listed and the recommended updates are listed in the **Updates** section. Select Dell Management Console.

Installing Dell Management Console

You can install the Dell Management Console and other utilities from the *Dell Management Console* DVD or download and install it from the Dell website at **dell.com/openmanage**. You can also install the dependencies for Dell Management Console from this installer.

1. Insert the *Dell Management Console* DVD into the DVD drive. If the installation program does not start automatically, navigate to the root folder of the DVD and double-click **setup.exe**.

   The **Dell Management Console** dialog box is displayed.
2. On the Welcome screen, select **Install Dell Management Console**.

A message prompting you to restart the machine to increase the number of ports is displayed. Select **Yes**.

After system restart, run the installer. The installer scans your system for the Microsoft .NET framework. If the .NET is not installed, then you are prompted to install the .NET framework.

If there are no missing dependencies, the **Symantec Installation Manager Setup** dialog box is displayed.

3 Click **Next**.

4 Accept the End User License Agreement and click **Next**.

5 In the **Destination Folder** dialog box, browse to a folder where you want to install Dell Management Console and click **Begin Install**.

6 When the installation is complete, select **Automatically launch Symantec Installation Manager**, and then click **Finish**.

The **Symantec Installation Manager** launches automatically.

NOTE: To download hot fixes, patches, and trial versions for the value added plug-in solutions, you must have Internet access.

7 On the **Symantec Installation Manager** main dialog box, select **Install new products**.

8 On the **Install New Products** dialog box, select **Dell Management Console** and click **Next**.

You can select various filters and select **show all available versions** to view and install other components.

9 On the **Optional Installs** dialog box, select the Available features you want to install and then click **Next**.

10 Accept the End User License Agreement, and click **Next**.

The **Install Readiness Check** dialog box displays dependencies and recommendations.

11 If some dependencies are missing, install the requirements.

NOTE: Check the install readiness for the .Net certificate and the SQL Maximum Memory configuration.

Click **Check install readiness again** and click **Next**.

12 On the **Dell Management Console Configuration** dialog box, enter the local administrator credentials.

If you have configured e-mail information, you can verify the configuration by sending a test e-mail.

13 Click **Next**.

14 On the **Database Configuration** dialog box, enter details of the Microsoft SQL Server that is used by Symantec Management Console, and click **Next**.

NOTE: If you used Dell OpenManage IT Assistant with SQL Server 2005, then depending on the number of managed devices, you can use the same database with Dell Management Console. See "Recommended Minimum Hardware Configuration"for more information.

15 In the **Review Installation Details** dialog box, click **Begin Install**.

Dell Management Console is installed.

The Product Licensing dialog box is displayed.

16 In the **Product Licensing** dialog box, click **Next**.

The Installation Complete dialog box is displayed.

17 In the Installation Complete dialog box, click **Finish**.

You can install other Dell utilities using the *Dell Management Console* DVD.

For information on installing Dell Management Console on the Dell Client Manager, see the *Symantec Management Platform Installation Guide*.

Points to Note After Installation

- After installing the Dell Management Console, if you want to change the operating system and Symantec Management Console passwords, always change the Symantec Management Console password *before* changing the operating system password.

  However, if the operating system password is changed before the Notification Server password, use the following command to change the Notification Server password:

```
aexconfig /svcid user:<username (domain,
machine\user)> password:<password>
```

NOTE: The `aexconfig` command is available under the **Altiris/Notification server/bin** folder.

- After installing the Dell Management Console, if you change the system hostname and try to launch the Dell Management Console, a server exception is displayed.

  For more information on troubleshooting this issue, see the section on **Symantec Management Server Error** in the *Dell Management Console Online Help*.

Uninstalling Dell Management Console

To uninstall Dell Management Console, do the following:

1. Go to **Add or Remove Programs** and run the Symantec Platform and Solutions wizard.
2. Select the **Symantec Platform and Solutions** component and click **Uninstall**.

   The Dell Management Console is uninstalled.

You can also uninstall the Dell Management Console from the *Dell Management Console* DVD.

1. Insert the *Dell Management Console* DVD.
2. On the **Dell Management Console** dialog box, select **Install Dell Management Console**.
3. Navigate through the install wizard until the **Install Products** dialog box is displayed.
4. Select the Dell Management Console option and click **Uninstall**.

   The Dell Management Console is uninstalled.

NOTE: When you uninstall Dell Management Console, the Dell Management Console database is not uninstalled.

Upgrading to the Latest Version of Dell Management Console

You can upgrade the Dell Management Console from the previous version using the *Dell Management Console* DVD.

If you are upgrading to this release of Dell Management Console, then use SIM. SIM must be connected to internet for getting the latest updates. When you launch SIM, all the critical updates are listed and the recommended updates are listed in the Updates section. Select Dell Management Console.

NOTE: While upgrading the Dell Management Console, the **Dell Management Console Configuration** and **Database Configuration** screens are not displayed.

After the SIM launches, you may be prompted to install some critical updates. It is recommended that you install all updates before you continue with the Dell Management Console upgrade.

Dell Management Console 1.1 is based on the Symantec Management Platform (SMP) SP3. Therefore, it is recommended that you upgrade to Dell Management Console 1.1 *before* (*or while*) installing the latest version of Server Management Suite and Dell Client Manager from *Dell Management Console Version 1.1* DVD.

Troubleshooting

For information on troubleshooting, see the *Online Help*.

3

Migrating the Dell OpenManage IT Assistant Discovery Settings

If you have not used Dell™ OpenManage™ IT Assistant or do not want to migrate discovery ranges to the Dell Management Console, skip this section.

If you are an existing user of IT Assistant, read this section to know how to migrate discovery ranges to the Dell Management Console.

The Dell Management Console allows you to migrate discovery setting information from IT Assistant 8.0 and later.

Importing IT Assistant Discovery Settings

You can migrate the following discovery settings from the IT Assistant database to the Dell Management Console:

- Exclude ranges
- Include ranges
- Protocol information associated with include ranges:
  - SNMP: retries, timeout, and read community strings

    NOTE: Write community strings are not migrated as the Dell Management Console does not have write community strings.

  - ICMP: retries and timeout
  - Dell|EMC NaviCLI®: user name and password
  - IPMI: retries, timeout, user name, password, and KGkey
  - CIM: domain name, user name, and password. If you do not provide the domain name, `localhost` is used.
  - Dell™ PowerVault™ MD Storage Array protocol enable/disable information
- Discovery scheduling information

The Database Migration User Interface

You can access the database migration link by clicking **Home**→ **Dell Management Console Portal**. In the **Dell Enterprise Management Quick Start** Web part, on the **Getting Started** tab, click **Migrate Dell OpenManage IT Assistant Discovery Settings**.

Points to Note Before Migrating the IT Assistant Discovery Settings

- You can migrate only the discovery ranges from IT Assistant 8.0 and later to the Dell Management Console database.
- After you start the database migration process, you cannot cancel or stop the migration.
- You can also migrate data from a *remote* IT Assistant database and from a named instance of the database. Ensure that the connection between the local system and the remote database is working.
- Before migrating discovery ranges, to reduce the load on the Dell Management Console system, you can reduce the number of threads used for each discovery task. To change the default value of 40, go to **Settings**→ **All Settings**. On the right hand pane, under **Settings**→ **Discovery and Inventory**→ **Network Discovery Settings**, change the default value.

  If you want to change the network discovery settings after migration, you will have to select each discovery task and edit it. For more information, see “Discovery Performance.”

Remote Database

To specify the remote database, ensure that the connection between the local system and the remote database is working. To enable the remote database connection, see “Enabling Remote Connection to SQL Server 2005 or 2008 Express.” Provide the IT Assistant database location and the authentication mode.

- Microsoft® Windows® Authentication — Ensure that the username and password is the same for both IT Assistant and Dell Management Console.

- Mixed/SQL Authentication — Provide the administrator SQL login credentials for the IT Assistant database. The given SQL login credentials should be e*nabled* and have the appropriate *server roles* and *user mapping* for the remote database.

IT Assistant creates its database in the Windows Authentication mode only. To use SQL Authentication, change the authentication mode. For more information, see "Enabling SQL Server and Windows Authentication."

IT Assistant supports the default instance of the remote database. If you have configured the database for IT Assistant with the named instance, specify the named instance along with the server name, for example, **MyServer/NamedInstance**.

Enabling Remote Connection to SQL Server 2005 or 2008 Express

By default, SQL Server does not automatically connect to a remote database; you have to enable it manually. Use the Microsoft Windows' **ODBC Data Source Administrator** tool to verify your remote database connection. If you connect to a remote SQL Server without first enabling the remote connection, an error is displayed.

To resolve this error, do the following:

- Enable both the SQL Server and Windows authentication mode on the SQL Server.
- Enable remote connection using the TCP/IP protocol.

Enabling SQL Server and Windows Authentication

To enable SQL server and Windows Authentication:

1. Log into the SQL Server using SQL Server Management Studio Express on the local SQL Server using Windows Authentication user credentials. Windows account is used to authenticate to SQL Server.
2. In **Object Explorer**, right-click the instance name and select **Properties**.
3. On the left pane, select **Security** and change the Server authentication to **SQL Server and Windows Authentication mode**.
4. Right-click the instance name again, select **Restart** to restart SQL Server service for the changes to take effect.

Enabling Remote Connection

To enable a remote connection:

1 Open **SQL Server Surface Area Configuration**.

2 Select **Surface Area Configuration for Services and Connections**.

3 On the left pane, expand the SQL Server instance→ **Database Engine**→ **Remote Connections**.

4 On the right side select **Local and remote connections**→ **Using both TCP/IP and named pipes**.

5 On the left side, select **SQL Server Browser**→ **Service**.

6 On the right side, if the startup type is **Disable**, change to **Automatic** and click **Apply**.

7 Click **Start** to start the service and click **OK**.

8 Log into the SQL Server from the remote system using SQL Server authentication mode.

Migrating Discovery Information from IT Assistant 8.*x*

1 Install Dell Management Console.

2 Launch Dell Management Console.

3 Click **Home**→ **Dell Management Console Portal**.

4 On the **Dell Enterprise Management QuickStart** Web part, under the **Getting Started** tab, click **Migrate Dell OpenManage IT Assistant Discovery Settings**.

The **IT Assistant Discovery Settings Migration** page is displayed.

5 In the **Discovery Settings Migration** Web part, click **Launch Migration Wizard**.

6 On the first page of the wizard, provide the required parameters to connect to the IT Assistant database.

You can either specify a local or a remotely configured IT Assistant database.

If IT Assistant is configured on a named instance of a database, specify that information in the **Database Server Name**.

For example, `MyITAssistant\MyNamedInstance`.

Select the required authentication mode.

Click **Next**.

7 The second page displays the discovery ranges retrieved from the IT Assistant database that you provided in the previous pane.

The **Include Range** listbox displays all enabled include ranges retrieved from IT Assistant.

NOTE: If a sub-range is disabled within the Include Range, it will not be migrated to Dell Management Console.

The **Exclude Range** listbox displays all exclude ranges retrieved from IT Assistant.

Select each include range from the **Include Range** listbox to view its details (protocols and associated settings.)

Click **Next**.

8 The third page of the wizard displays the migration schedule information of IT Assistant.

However, if you want to run the migration task right away, select **Now** and click **Next**.

9 The final wizard page is an information-only pane.

Click **Finish** to start migration.

Viewing Migrated Data in Dell Management Console

To view the migrated data in Dell Management Console:

1 Click **Home**→ **Discovery and Inventory**→ **Network Discovery**.

2 On the **Network Discovery Task Management** Web part, in the **Available Tasks** tab, you can view the various migrated scan groups (Discovery Tasks.)

The migrated discovery tasks are displayed as **IT Assistant Migrated Discovery Task - <include range>**.

In the **Task Runs** tab, you can view the discovery task status.

3 To view the protocols of the migrated discovery tasks, go to **Settings**→ **All Settings**→ **Monitoring and Alerting**→ **Credential Settings**→ **Credentials Management**.

To view the connection profiles of the migrated discovery tasks, go to **Settings**→ **All Settings**→ **Monitoring and Alerting**→ **Protocol Management**→ **Connection profiles**→ **Manage Connection Profiles**.

For more information, see “Running the Discovery Task“and “Viewing Results of the Inventory Task.”

4

Dell Management Console User Interface

This chapter describes the user interface (UI) — the look and feel — of Dell™ Management Console.

The underlying framework of the Symantec™ Notification Server® provides a dynamic user interface with rich controls.

Dell Management Console is located under **C:\Program Files\Dell\Sysmgt\dmc**. The launch icon is available under **Start** button→ **Programs**→ **Dell OpenManage Applications**→ **Dell Management Console**→ **Dell Management Console**.

NOTE: If Secure Socket Layer (SSL) is enabled for Dell Management Console, then edit the shortcut on the desktop and the **Start** menu to point to the new SSL location. For example: **https://localhost/Dell/console**.

Dell Management Console is menu-driven and consists of six main menus:

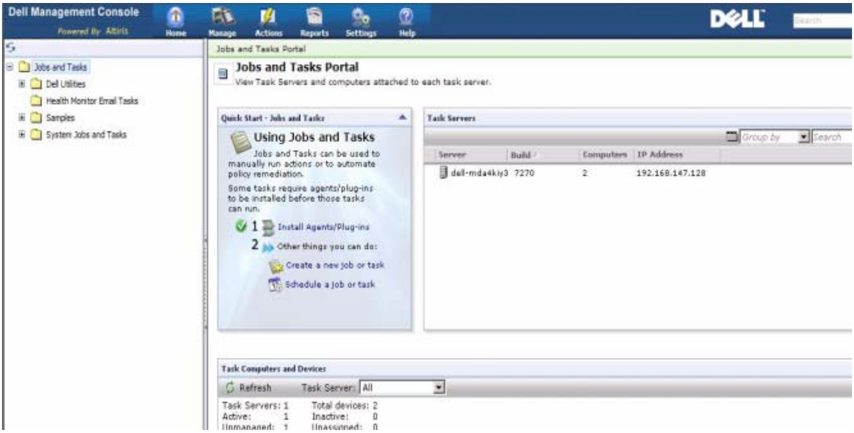
- **Home**
- **Manage**
- **Actions**
- **Reports**
- **Settings**
- **Help**

Based on their functionality, the sub-menus are grouped under each menu. Examples of Dell Management Console sub-menus are as follows:

- The **Home** menu consists of the Dell Management Console portal submenu. As you install plug-ins, the respective portals are available under this menu.
- The **Manage** menu consists of all components that you can manage — from computers, user, resources to tasks and events.
- The **Actions** menu consists of the actions you can perform on the network devices, such as discovery, inventory, monitoring, and deploying agents.

- The **Reports** menu consists of all reports available in Dell Management Console.
- The **Settings** menu consists of sub-menus for configuring security, Symantec Notification Server, and Dell Management Console.
- **Help** menu provides you access to the online help and other documentation links. You can find information about all features from this menu.

Selecting a sub-menu displays a page in which you can navigate through a tree structure on the left side. The right side consists of various Web parts, which are a graphical representation of data. For example, in the **Jobs and Tasks** portal page, the left hand pane displays a tree structure. The right hand pane displays the **Quick Start - Jobs and Tasks**, **Task Servers**, and **Task Computer and Devices** Web parts.



Jobs and Tasks Portal

View Task Servers and computers attached to each task server.

Quick Start - Jobs and Tasks

Using Jobs and Tasks

Jobs and Tasks can be used to manually run actions or to automate policy remediation.

Some tasks require agents/plug-ins to be installed before those tasks can run.

1 Install Agents/Plug-ins

2 Other things you can do:

Create a new job or task

Schedule a job or task

Task Servers

Group by: Search

Server	Build	Computers	IP Address
dell-mda4kiy3	7270	2	192.168.147.128

Task Computers and Devices

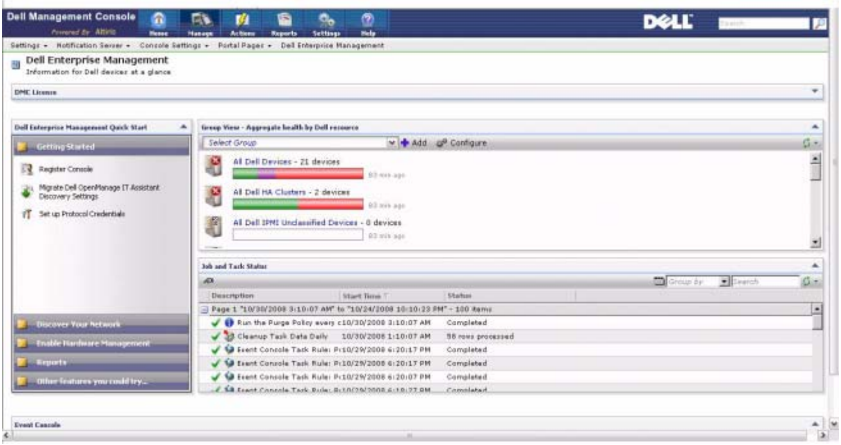
Refresh Task Server: All

Task Servers: 1 Total devices: 2
Active: 1 Inactive: 0
Unmanaged: 1 Unassigned: 0

Home Menu—Dell Management Console Portal Page

The Dell Management Console has a portal page that provides quick access to dashboards and tasks that are specific to managing and monitoring Dell devices on the network. You can access this page from **Home→ Dell Management Console Portal**.

The portal page consists of Web parts for device health, status of tasks, alerts, and so on.


Dell Management Console
Powered by Altiris
Home
Manage
Actions
Reports
Settings
Help
DELL
Search
Settings ▾
Notification Server ▾
Console Settings ▾
Portal Pages ▾
Dell Enterprise Management
Dell Enterprise Management
Information for Dell devices at a glance
DMC License
Dell Enterprise Management Quick Start
Getting Started
Register Console
Migrate Dell OpenManage IT Assistant Discovery Settings
Set up Protocol Credentials
Discover Your Network
Enable Hardware Management
Reports
Other features you could try...
Group View - Aggregate health by Dell resource
Select Group
Add
Configure
All Dell Devices - 21 devices
83 min ago
All Dell HA Clusters - 2 devices
83 min ago
All Dell IPMI Unclassified Devices - 0 devices
83 min ago
Job and Task Status
Group by
Search
Event Console

Page 1 "10/30/2008 3:10:07 AM" to "10/24/2008 10:10:23 PM" - 100 items

Description	Start Time	Status
✓ Run the Purge Policy every c	10/30/2008 3:10:07 AM	Completed
✓ Cleanup Task Data Daily	10/30/2008 1:10:07 AM	58 rows processed
✓ Event Console Task Rule: P:	10/29/2008 6:20:17 PM	Completed
✓ Event Console Task Rule: P:	10/29/2008 6:20:17 PM	Completed
✓ Event Console Task Rule: P:	10/29/2008 6:20:07 PM	Completed
✓ Event Console Task Rule: P:	10/29/2008 6:19:27 PM	Completed

To get started with Dell Management Console, select the **Dell Enterprise Management Quick Start** Web part. The various tabs available on this Web part enable you to configure Dell Management Console.

From the **Dell Enterprise Management Quick Start** Web part, you can do the following:

- Migrating discovery ranges from Dell OpenManage™ IT Assistant.
- Discovering devices on the network and monitoring them.
- Inventorying discovered devices and applying updates.
- Using Dell-specific reports or creating new reports.

Modifying the Dell Management Console Portal Page

You can add or remove Web parts from the portal pages.

1 On the top right hand corner of the **Dell Management Console Portal** page, select **Edit**.

NOTE: The **Edit** button is displayed on this page only when you register the Dell Management Console on the Dell website at **dell.com/openmanage/register**.

2 In **select web part**, choose the Web part you want to display on the portal page and click **Add**.

The Web part is added to the portal page. You can drag and drop the Web part on the portal page to a position of your choice.

3 Click **Apply**.

Launching Applications

You can launch other applications from Dell Management Console. Depending on the type of discovered device, Dell Management Console provides a consolidated launch point for systems management applications for a device.

To launch applications for a device, select from the following options:

- Manage menu
- Resource Manager
- Settings menu
  - Dell OpenManage Network Manager
  - Dell OpenManage RAC Console

Manage menu

1 From Dell Management Console, select **Manage→ All Devices**.

2 On the **All Devices** page, open a device, for example a server, right-click and select **Management Applications**.

The systems management application options are displayed; such as **Dell OpenManage Server Administrator**, **SOL Proxy**, and **Telnet**.

You can launch these application and perform appropriate actions.

Depending on the connection profile, the options available for a device may vary. For example, if you discover a device using the SNMP protocol, the following options are available:

- Dell Open Manage Server Administrator
- RAC Console for systems that have the Dell Remote Access Controller (DRAC) present
- RAC Telnet for systems that have the DRAC present
- Remote Desktop (for Microsoft® Windows® systems only)
- SOL Proxy
- Telnet
- EqualLogic

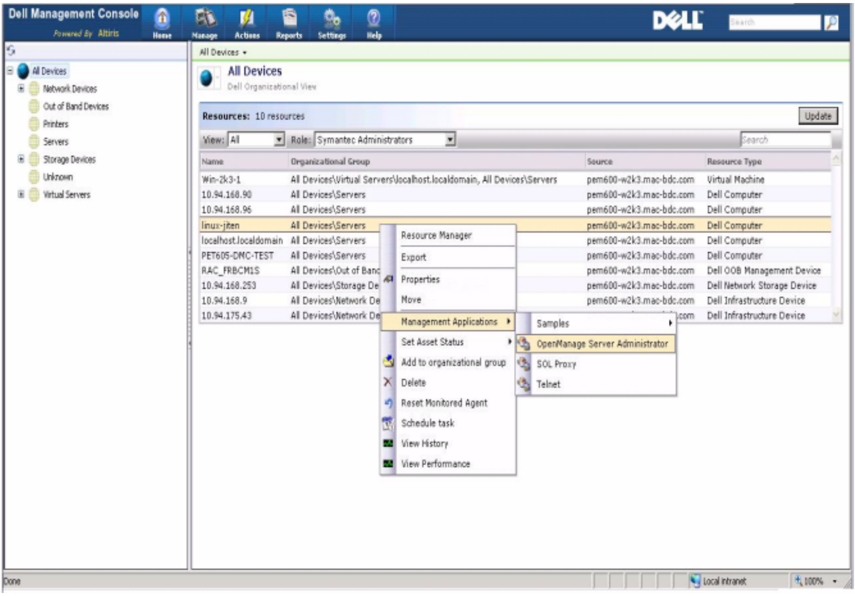
However, if you discover a device with the WMI protocol, the following options are available:

- Dell Open Manage Server Administrator
- Remote Desktop
- SOL Proxy
- Telnet

With IPMI, the following options are available:

- SOL Proxy
- Telnet

For more information on the Connection Profiles, see “Creating a New Connection Profile”and “Editing the Default Connection Profile.”



Resources: 10 resources

View: All Role: Symantec Administrators

Name	Organizational Group	Source	Resource Type
Win-2k3-1	All Devices\Virtual Servers\localhost.localdomain, All Devices\Servers	pem600-w2k3.mac-bdc.com	Virtual Machine
10.94.168.90	All Devices\Servers	pem600-w2k3.mac-bdc.com	Dell Computer
10.94.168.96	All Devices\Servers	pem600-w2k3.mac-bdc.com	Dell Computer
linux-jiten	All Devices\Servers	pem600-w2k3.mac-bdc.com	Dell Computer
localhost.localdomain	All Devices\Servers	pem600-w2k3.mac-bdc.com	Dell Computer
PET605-DMC-TEST	All Devices\Servers	pem600-w2k3.mac-bdc.com	Dell Computer
RAC_FRBCM1S	All Devices\Out of Banc	pem600-w2k3.mac-bdc.com	Dell OOB Management Device
10.94.168.253	All Devices\Storage De	pem600-w2k3.mac-bdc.com	Dell Network Storage Device
10.94.168.9	All Devices\Network De	pem600-w2k3.mac-bdc.com	Dell Infrastructure Device
10.94.175.43	All Devices\Network De	.com	Dell Infrastructure Device

Resource Manager

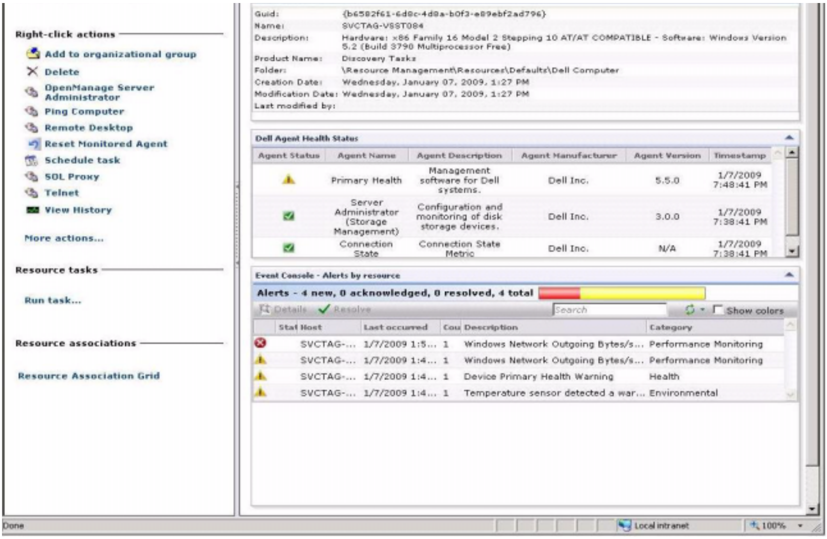
1 Click **Manage**→ **All Devices**.

2 On the **All Devices** page, right-click a device, for example a server, and select **Resource Manager**.

You can also double-click on the device name to access the Resource Manager.

3 The Resource Manager page displays complete information about the device including summaries of hardware, filter, and polices, the calendar of tasks scheduled for this device, and so on.

On the left pane of the **Resource Manager** page, under the **Right-click actions**, the systems management application for the device are displayed.



Guid: {b6582f61-6d8c-4d8a-b0f3-e89ebf2ad796}
Name: SVCTAG-V8ST084
Description: Hardware: x86 Family 16 Model 2 Stepping 10 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
Product Name: Discovery Tasks
Folder: \Resource Management\Resources\Defaults\Dell Computer
Creation Date: Wednesday, January 07, 2009, 1:27 PM
Modification Date: Wednesday, January 07, 2009, 1:27 PM
Last modified by:

Dell Agent Health Status

Agent Status	Agent Name	Agent Description	Agent Manufacturer	Agent Version	Timestamp
⚠	Primary Health	Management software for Dell systems.	Dell Inc.	5.5.0	1/7/2009 7:48:41 PM
✓	Server Administrator (Storage Management)	Configuration and monitoring of disk storage devices.	Dell Inc.	3.0.0	1/7/2009 7:38:41 PM
✓	Connection State	Connection State Metric	Dell Inc.	N/A	1/7/2009 7:38:41 PM

Event Console - Alerts by resource

Alerts - 4 new, 0 acknowledged, 0 resolved, 4 total

	Stat	Host	Last occurred	Cou	Description	Category
⊗		SVCTAG-...	1/7/2009 1:5...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Device Primary Health Warning	Health
⚠		SVCTAG-...	1/7/2009 1:4...	1	Temperature sensor detected a war...	Environmental

Settings Menu — Dell OpenManage Network Manager

1. From Dell Management Console, select **Settings**→ **Console**→ **Right-click Actions**.
2. On the left pane of the **Management Applications** page, click an application, for example **Dell OpenManage Network Manager**.

   The Dell OpenManage Network Manager page is displayed.

   > **NOTE:** This application is a right-click option for an infrastructure device, hence the **Resource Type** is displayed as **Dell Infrastructure Device**.

   The Resource Type for network devices is described in Table 4-1.

Table 4-1. Resource Type for Dell Devices

Dell Device	Resource Type
Dell PowerEdge™ system	Dell Computer
Printer	Dell Printer
Dell|EMC	Dell Network Storage Device
Tape	Dell Network Backup Device

Table 4-1. Resource Type for Dell Devices ***(continued)***

Dell Device	Resource Type
Dell PowerConnect™/KVM/Fibre Channel switch	Dell Infrastructure Device
Dell Remote Access Controller	Dell OOB (out-of-band) Management Device
Dell PowerVault™ MD Arrays Dell|EqualLogic Groups	Dell Network Storage Device

NOTE: It is recommended that you do not change the Resource Type for a device.

3 This application is of command line type, and the default location for this application is displayed on **Command Line**.

NOTE: If you install this application at a location other than the default, ensure that you edit the location displayed on **Command Line**.

Settings Menu — Dell OpenManage RAC Console

1 From Dell Management Console, select **Settings**→ **Console**→ **Right-click Actions**.

2 On the left pane of the **Management Applications** page, click an application, for example RAC Console.

The Dell OpenManage RAC Console page is displayed.

3 This application is a right-click option for a Dell out-of-band (OOB) device, hence the **Resource Type** is displayed as **Dell OOB Management Device**.

NOTE: It is highly recommended that you do not change the Resource Type for a device.

4 This application is of URL type, and the default location for this application is displayed on **Base URL**.

NOTE: If your URL is different from the default or if you have enabled SSL, ensure that you edit the URL for Application Launch to work correctly.

5

Configuring Discovery and Inventory Settings

With Dell™ Management Console you can discover and inventory devices, alert users, update drivers, BIOS, and firmware, and perform a variety of tasks for each system in your enterprise. Managed systems can include servers, printers, tape devices, storage devices, systems with remote access cards, Dell PowerConnect™ switches, and digital keyboard/video/mouse (KVMs) switches used with rack-dense systems.

This section illustrates how a system administrator of a small-to-medium size business (50 servers, plus over 200 client systems, and 10 switches) can use the Discovery and Inventory solutions of Dell Management Console.

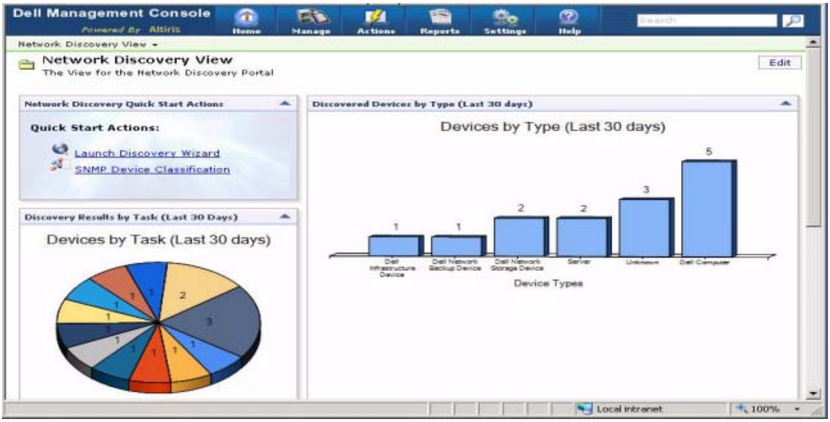
The scenarios illustrates how an administrator in charge of managing network environments can configure Dell Management Console.

NOTE: These scenarios do not illustrate the full capabilities of Dell Management Console.

The Discovery User Interface

To access the Discovery portal: click **Home**→ **Discovery and Inventory**→ **Network Discovery**.

Knowing Your Discovery User Interface


Dell Management Console
Powered By Altiris
Home
Manage
Actions
Reports
Settings
Help
Search
Network Discovery View
Edit
Network Discovery Quick Start Actions
Launch Discovery Wizard
SNMP Device Classification
Discovered Devices by Type (Last 30 days)
Devices by Type (Last 30 days)
1
1
2
2
3
5
Dell Infrastructure Device
Dell Network Backup Device
Dell Network Storage Device
Server
Unknown
Dell Computer
Device Types
Discovery Results by Task (Last 30 Days)
Devices by Task (Last 30 days)
1
1
2
1
1
3
1
1
1
1
1
1
Local intranet
100%

Network Discovery View

The View for the Network Discovery Portal

Quick Start Actions:

The **Network Discovery Quick Start Actions** Web part is a good place to start configuring discovery for network devices.

The **Network Discovery Task Management** Web part at the bottom of the screen displays the available discovery tasks and the tasks that have run.

The **Discovery Results by Tasks** Web part displays the tasks run and the number of devices discovered by the task.

The **Discovered Device Classification** Web part displays the various types of devices discovered. For example, servers, printers, tapes, switches, and so on.

Before Configuring Discovery Settings

Before using Dell Management Console to configure discovery, you must take some basic decisions based on the network. Specifically, you *must* determine the following:

- Host names, IP addresses, or IP subnet ranges of systems that you want to discover.

- Credentials needed to communicate with the devices. For example, if you want to discover Microsoft® Windows® systems by using the WMI protocol, then you must provide Windows credentials to Dell Management Console. See "Managing Credentials."
- Systems management protocols needed to manage the systems and devices on the network. Table 5-1 provides a quick reference.

  To manage the protocols, create the connection profiles according to the systems management protocols supported by the devices. For more information, see "Connection Profiles."

Connection Profiles and Credentials Management

The Credential Manager enables you to encrypt and store sensitive data, namely the credentials, which are used to connect through the various protocols.

A connection profile is a set of protocols and their corresponding credentials that can be configured and saved as a logical set. This set is used by the discovery, inventory, and monitoring solutions as a reference to use the defined protocols.

Dell Management Console uses the connection profile to communicate with a device. Identify devices that require authentication and have a list of their credentials ready. Then create connection profiles for these devices. For example, if ten servers on the network have different authentication credentials, you must create a different connection profile for each of these systems.

Managing Credentials

To add Dell|EMC storage devices to the network and discover these devices, provide the credentials for the discovery solution to communicate with the Dell|EMC devices.

1. In Dell Management Console, click **Settings→ All Settings**.
2. On the left hand pane, under the **Settings→ Monitoring and Alerting→ Credential Settings** folder, select **Credentials Management**.
3. On the right hand pane, click **Add Credentials**.
4. On the **Add Credentials** dialog box, select **EMC Credentials** as the **Credential Type**.
5. Provide the **Name** of this credential, for example, `emc-cred.`

   Enter the **Username** and **Password** for the Dell|EMC device and click **OK**.

   The new credential is displayed on the **Credential Management** page.

Connection Profiles

Dell Management Console provides a default connection profile. This profile has the following protocols enabled:

- HTTP
- ICMP
- SNMP V1 V2
- SNMP Trap Sender
- WMI

Refer to the default connection profile as a template and create a new connection profile with the protocols that you want to use to discover networked devices.

Viewing the Default Connection Profile

To view the default connection profile:

1. Click **Setting→ All Settings**.
2. On the left pane, select the **Settings** folder→ **Monitoring and Alerting→ Protocol Management→ Connection Profiles→ Manage Connection Profiles**.

Edit the default connection profile to add or remove protocols.

NOTE: Even though the default connection profile already exists, you must still configure the appropriate credentials for each protocol.

Editing the Default Connection Profile

You can edit the **Default Connection Profile** or add a new connection profile by clicking **Add Settings**:

1. On the **Manage Connection Profile** page, select **Default Connection Profile** and click edit (the pencil icon.)

   The **Define Group Settings** page displays the protocols that are pre-configured in the default profile.

2. On the **Define Group Settings** page, select **On** to enable IPMI.
3. Click the up arrow to add the IPMI credentials of the managed device or a group of devices.

   NOTE: You must enter the KGkey of the managed device for IPMI to work correctly. Enter the KGkey in the IPMI Credential Profile of the device. For more information, see "Managing Credentials."

4. Disable other protocols like the HTTP, ICMP, and SNMP Trap Sender if the network devices do not use these protocols.

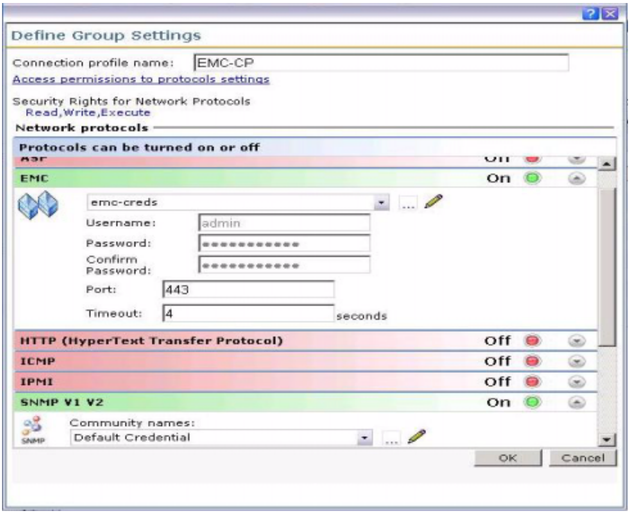
   It is highly recommended to disable the protocols that are not required for network discovery, since higher number of protocols will decrease the speed at which devices are discovered.

5. Click **OK**.

Creating a New Connection Profile

If you add Dell|EMC devices to the network, you cannot use the default connection profile because this connection profile does not have the required systems management protocols enabled. You must create a new connection profile with EMC and SNMP enabled. (see Table 5-1 for connection profiles required for various devices.)

1. See "Viewing the Default Connection Profile."
2. On the **Manage Connection Profiles** page, click **Add Settings**.
3. On the **Define Group Settings** pane, turn on the **EMC** protocol and click the down arrow to configure the EMC credentials.



Define Group Settings

Connection profile name: EMC-CP

Access permissions to protocols settings

Security Rights for Network Protocols
Read,Write,Execute

Network protocols

Protocols can be turned on or off

ASF Off

EMC On

emc-creds

Username: admin

Password: ●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●

Port: 443

Timeout: 4 seconds

HTTP (HyperText Transfer Protocol) Off

ICMP Off

IPMI Off

SNMP V1 V2 On

Community names: Default Credential

4 Enter the Connection Profile name, for example, **EMC_SNMP**.

5 Select **emc-cred** from the drop down list, see “Managing Credentials.”

Dell Management Console retrieves the **emc-cred** information and populates all fields.

6 Select the **SNMP V1 V2** protocol and turn it on and click the down arrow to configure the SNMP credentials and then click **OK**.

The new connection profile is displayed in the **Manage Connection Profiles** page.

Table 5-1. Protocols and Connection Profiles Required For Various Devices

Devices	Systems Management Protocol Supported	Protocols for Connection Profile
Servers running supported Microsoft Windows operating system	SNMP, WMI, and IPMI	SNMP, WMI, or IPMI, or a combination of these
Servers running supported Linux operating system	SNMP and IPMI	SNMP or IPMI, or a combination of these
Dell PowerVault™ storage systems	MD Array	MD Array
Dell PowerConnect Switches	SNMP	SNMP
Tapes	SNMP	SNMP
Printers	SNMP	SNMP
Dell|EMC	SNMP and Navisphere® Secure CLI	SNMP and EMC
Remote Access Controllers	SNMP	SNMP
Digital KVM	SNMP	SNMP
Servers running Lifecycle Controller	Web Services for Management (WS-MAN)	WS-MAN
Dell|EqualLogic	SNMP	SNMP

Creating a Discovery Task

1 Click **Home→ Discovery and Inventory→ Network Discovery**.

2 In the **Network Discovery Home** page, in the **Network Discovery QuickStart Actions** Web part, click **Launch Discovery Wizard**.

The **Discover network devices** page is displayed.

NOTE: On the **Network Discovery Home** page, on the **Available Tasks** tab, click **New** to create a discovery task.

3 In Step 1: **Choose method of device discovery**, select **Targeted network scan** and then click **Next**.

NOTE: If you select ARP, provide the IP address of the router that is configured to accept SNMP requests.

4 In Step 2: **Enter network IP Ranges**, and click **Include→ Custom Range**.

Custom ranges are used to define various subnets at the same time. For example, a custom range of 10.94.*.* with a Subnet mask of 255.255.255.0 will scan all IP addresses from 10.94.1.1 to 10.94.255.254.

Use the custom range with caution as a large custom range can take a very long time to discover the devices.

5 In the **Custom Range** dialog box, enter the following information and then click **Next**:

Custom range: `10.94.168.*`

Mask: `255.255.255.0`

6 In Step 3: **Select device communication protocol**, select **Default Connection Profile**. This profile has protocols such as, HTTP, ICMP, SNMP, and WMI selected.

7 Edit **Default Connection Profile** to include the IPMI protocol, and click **Next**.

See "Editing the Default Connection Profile."

8 In Step 4: **Enter task name**, Enter `Discover_All` as the **Task name** and click **Next**.

9 In Step 5: **Choose when to run the discovery**, and then choose the schedule for the task.

Schedule discovery of devices on the network based on your requirements, for example, once a week.

To run schedule once a week, do the following:

Schedule: Shared Schedule

Select Shared Schedule: Weekly

click **New**.

10 In the **Create New Shared Schedule** page, enter name and description of the schedule.

Select **Add schedule**→ **Scheduled Time** and select 0600 hours as the start time for the discovery task.

Click **No repeat** and select the **Week** and **Monday** in the **Repeat Schedule** screen.

Click **OK**.

11 On the **Discover network devices** page, click **Finish**.

The **Discover_All** task is displayed in the Task Management Portal under **Server Tasks**→ **Network Tasks** folder.

NOTE: All devices/groups of devices that have different authentication credentials will require a new connection profile. For each such device or group of devices, you must create a separate discovery task and map it to the appropriate connection profile.

Running the Discovery Task

After creating the discovery task, you can run the **Discover_All** task:

1 Click **Home**→ **Discovery and Inventory**→**Network Discovery**.

The **Network Discovery Home** page is displayed.

2 On the **Network Discovery Task Management** Web part, select the **Available Tasks** tab.

3 Select the **Discover_All** task and click **Run Now...**.

You can run the discovery tasks migrated from Dell OpenManage™ IT Assistant.

For more information on migrating discovery tasks, see “Migrating Discovery Information from IT Assistant 8.x.”

After discovering the network devices, create and run an inventory task to view details of the devices. For more information, see “Creating an Inventory Task to Inventory All Systems.”

Viewing Discovered Devices

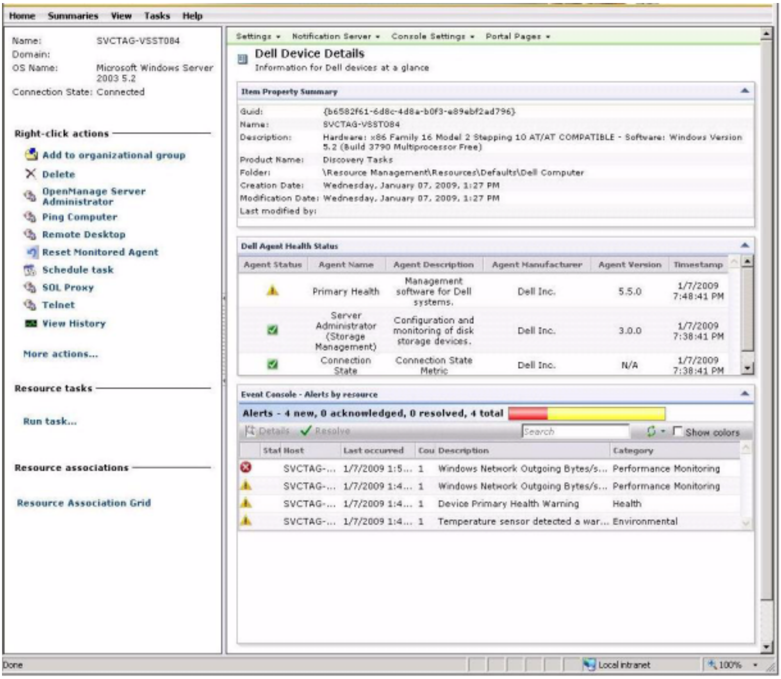
To view the discovered network devices:

1. Click **Manage→ All Devices**.
2. On the left pane, select servers to view the systems that are discovered.

   All servers that have Dell OpenManage Server Administrator installed on them are discovered as **Resource Type=Dell Computer**.

   For information on other resource types, see Table 4-1.
3. Select a system and double-click it to view its details.

   The **Resource Manager** page for this system is displayed.



Name:	SVCTAG-VSST084
Domain:	
OS Name:	Microsoft Windows Server 2003 5.2
Connection State:	Connected

Dell Device Details

Information for Dell devices at a glance

Item Property Summary

Guid:	{b6582f61-6d8c-4d8a-b0f3-e89ebf2ad796}
Name:	SVCTAG-VSST084
Description:	Hardware: x86 Family 16 Model 2 Stepping 10 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
Product Name:	Discovery Tasks
Folder:	\Resource Management\Resources\Defaults\Dell Computer
Creation Date:	Wednesday, January 07, 2009, 1:27 PM
Modification Date:	Wednesday, January 07, 2009, 1:27 PM
Last modified by:	

Dell Agent Health Status

Agent Status	Agent Name	Agent Description	Agent Manufacturer	Agent Version	Timestamp
⚠	Primary Health	Management software for Dell systems.	Dell Inc.	5.5.0	1/7/2009 7:48:41 PM
✓	Server Administrator (Storage Management)	Configuration and monitoring of disk storage devices.	Dell Inc.	3.0.0	1/7/2009 7:38:41 PM
✓	Connection State	Connection State Metric	Dell Inc.	N/A	1/7/2009 7:38:41 PM

Event Console - Alerts by resource

Alerts - 4 new, 0 acknowledged, 0 resolved, 4 total

	Stat	Host	Last occurred	Cou	Description	Category
☒		SVCTAG-...	1/7/2009 1:5...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Device Primary Health Warning	Health
⚠		SVCTAG-...	1/7/2009 1:4...	1	Temperature sensor detected a war...	Environmental

NOTE: If the health of the discovered device is normal, the **Dell Agent Health Status** Web part takes some time to display the primary health metric. For more information on health metric, see Table 9-8.

Point to Note

- If you have to delete a virtual machine, modular system, or a cluster displayed in the **All Devices** tree, first delete the devices under the group and then delete the group. Remove the group from the discovery range too; other wise, the group is displayed after every discovery cycle.

Resource Manager

The **Resource Manager** page contains two Web parts on the right hand pane of the screen.

The **Item Property Summary** Web part contains general information about the discovered device.

The **Dell Agent Health Status** Web part displays all agents associated with a device. This Web part provides status on management agents, such as Server Administrator, Storage Management, and Remote Access Controller. The SNMP or WMI protocol is used to retrieve this information.

The agent health status is driven by events generated by the monitor solution. for more information, see "Monitoring and Alerting." After discovery, the resource manager displays the status of the discovered agents. If the monitor solution initiates an alert originating from one or more monitored agents, the agent status changes to Critical, Warning, or Undetermined.

NOTE: Not all agents are available on all devices. For example, if Storage Management Service Remote Access Controllers are not installed on a system, agent information about the components are not displayed. Absence of agents indicates that the appropriate software is either not installed or the hardware is not properly enabled.

Also, different device types display different agents.

The status of the agent is directly related to health type alerts received for the device being monitored. For example, if the Primary Health for a device is displayed as warning or critical, a corresponding health alert is displayed in the **Event Console** Web part.

Event Console reduces the need to maintain separate tools to monitor systems, software, printers, and other devices. Event Console collects SNMP traps and other status messages and displays them in a single location. All status messages are converted to a common format that links each received message to the affected resource in the Dell Management Console database. These formatted messages are called alerts.

In the Event Console, when traps get generated from FC switches, ethernet switches, or EMC arrays, the IP address of the device is displayed; however, the name of the device is not displayed even though the device is already discovered in Dell Management Console.

Event Console also provides a rule-based triggering system that lets you process alerts in the following ways:

- Launch task server tasks in response to specific alerts.

If launch discovery tasks are available for some devices:

- Prevent specific alerts from being stored in the alert database.
- Forward alerts to another management system.

For more information on Event Console, see the Symantec documentation from **Help→ Context**.

On the left hand side of the **Resource Manager** screen, you can view basic information about the device along with the connection state of the device. The connection state displays whether the device is online or not.

In the **Right-click actions** section, a set of actions that can be performed on the device are displayed. This action list is context-sensitive, and the actions displayed depend on the type of the device being examined (a system, out-of-band device, printer, and so on.)

Discovery Logs

Discovery logs let you review the status of the discovery tasks. The logs provide useful data when you want to troubleshoot issues with discovery. By default, Dell Management Console does not save log entries.

To enable discovery logs:

NOTE: If you are discovering a large number of devices, enabling Discovery Logs may affect the performance of the Dell Management Console.

1. Click **Settings→ All Settings**.
2. On the left pane, select the **Discovery and Inventory** folder → **Discovery Log Settings**.
3. On the right pane, click **Change Settings**.
4. Select **Enable discovery logging**, enter the path where you want to save the discovery logs and click **Save Settings**.

5 Close the browser window and restart the Altiris™ object host service.

Discovery Performance

To manage performance of Dell Management Console for discovery tasks, you can set the number of threads required for each discovery tasks *before* creating the discovery tasks.

1 Click **Settings**→ **All Settings**.

2 On the right hand pane, under **Settings**→ **Discovery and Inventory** → **Network Discovery Settings**.

3 On the right hand pane, change the **Maximum number of threads per discovery task**.

This value is applied to all discovery tasks that you create.

To change the default value after creating a discovery task:

1 Click **Home**→ **Discovery and Inventory**→ **Network Discovery**.

The **Network Discovery Home** page is displayed.

2 On the **Network Discovery Task Management** Web part, under **Available Tasks** tab, select each task for which you want to change the number of threads.

Click the edit button (the pencil icon.)

3 On the **Edit Discovery Task** pane, click **Advanced**.

4 Change the **Maximum number of threads per discovery task** and click **OK**.

Alert-initiated Discovery

The alert-initiated discovery enables discovery of devices *not* managed by Dell Management Console, through alerts or traps.

Configure the trap destination of the *un*-managed devices in the network, with the IP address of the Dell Management Console system. When these devices send traps asynchronously to Dell Management Console system, each trap initiates an individual discovery process, which discovers the node that sent the trap.

This feature is disabled by default.

NOTE: Dell recommends that you use caution when enabling this feature. A high number of alerts from an unmanaged device could cause Dell Management Console to stop responding.

Troubleshooting Discovery

To troubleshoot Discovery issues, use any one or all of these tools:

- Dell Troubleshooting Tool
- Network Discovery Logs
- Altiris™ Log Viewer
- Other Troubleshooting Tools

The Dell Troubleshooting tool is available with the Dell Management Console installables; and with this tool, you can find the cause for connectivity issues. For more information, see the readme; available at the following location: **<DMC DVD>\Tools\Troubleshoot\Readme.txt**.

For troubleshooting the Discovery related issues, see the *Dell Management Console - Trouble shooting Guide* at the following location: **en.community.dell.com/groups**.

Network Discovery Logs

See "Discovery Logs."

Altiris Log Viewer

To view the Altiris Log Viewer:

1. On the system where you installed Dell Management Console, click the **Start** button.
2. Select **Programs→ Altiris→ Diagnostics→ Altiris Log Viewer**.

   The **Altiris Log Viewer** is displayed.

Other Troubleshooting Tools

- IPMI Connectivity Tools

  For example, ipmish.exe, ipmitool.exe
- SNMP MIB Browser

  For example, MG-SOFT MIB Browser
- Network Protocol Analyzer

For example, Wireshark

Creating a New Organizational View and Organizational Group

1. Click **Manage→ Organizational Views and Groups**.
2. On the left pane, right-click the **New Organizational Views→ New→ Organizational View**.
3. Right-click on the New Organizational View and select **New→ Organizational Group**.

   You can add devices to this group and assign an appropriate role to this group.

Configuring Inventory Settings

The Dell Management Console Inventory Solution enables you to gather inventory information from the devices on your network using different protocols.

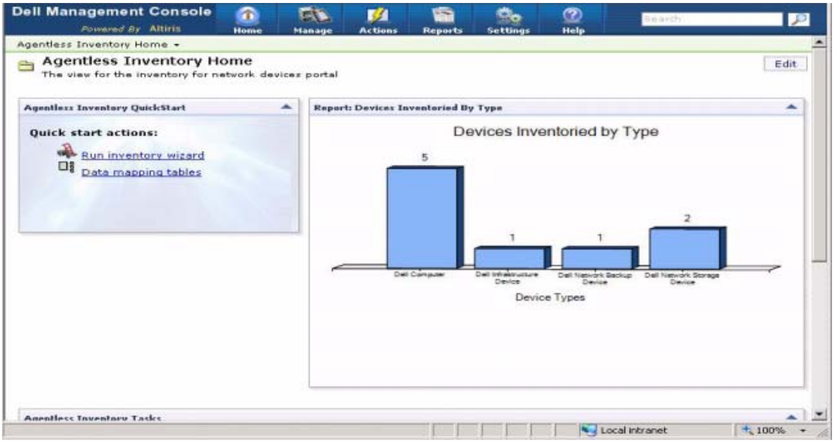
NOTE: Dell systems on which the Server Administrator is installed can enable the inventory task to report back specific details about the system.

Dell Management Console also allows you import MIBs to format incoming SNMP traps. However, you cannot import MIBs and map them to data classes to extend agentless inventory to new devices. This functionality requires a license for the Altiris Inventory Solution from Symantec.

NOTE: In the context of Dell Management Console, *agent-based* means the Altiris™ agent is installed on the target systems; whereas *agentless* means the Dell systems management agent—Dell OpenManage Server Administrator—is installed on the target systems.

To access the inventory portal: click **Home→ Discovery and Inventory→ Agentless Inventory**.

Knowing Your Inventory User Interface


Dell Management Console
Powered By Altiris
Home
Manage
Actions
Reports
Settings
Help
Search
Agentless Inventory Home
Agentless Inventory Home
The view for the inventory for network devices portal
Edit
Agentless Inventory QuickStart
Quick start actions:
Run inventory wizard
Data mapping tables
Report: Devices Inventoried By Type
Devices Inventoried by Type
5
1
1
2
Dell Computer
Dell Infrastructure Device
Dell Network Backup Device
Dell Network Storage Device
Device Types
Agentless Inventory Tasks
Local intranet
100%

The **Agentless Inventory Quick Start** Web part is a good place to start configuring and viewing the inventory information for network devices.

The **Agentless Inventory Tasks** Web part at the bottom of the screen displays the available inventory tasks and the tasks that have run.

Creating an Inventory Task to Inventory All Systems

To inventory the discovered systems and display the information in Resource Manager.

1. Click **Home**→ **Discovery and Inventory**→ **Agentless Inventory**.

   The **Agentless Inventory Home** page is displayed.

2. In the **Agentless Inventory QuickStart** Web part, click **Run inventory wizard**.

   The **Agentless Inventory Task Creation** page is displayed.

3. In step 1: **Choose devices to inventory**, for example, to inventory only the Dell PowerEdge™ systems on the network, select **Choose devices** and select **Servers** from the **Choose a group package** drop-down menu, and then click **Next**.

4 In step 2: **Inventory network task name**, enter a unique name—Dell Server Inventory Task—to help distinguish between various tasks of the same type, and then click **Next**.

5 In step 3: **Schedule**, select **Now**, to run the schedule after creating this task, and then click **Finish**.

You can decide to specify a later date and time to run this task and make this a recurring task.

The Agentless Inventory task is created and displayed on the **Agentless Inventory Home** page under the **Agentless Inventory Tasks** section.

Importing MIBs

You can extend the inventory capability using Management Information Base (MIB).

To perform an MIB import:

1 From Dell Management Console, select **Settings→ All Settings→ Monitoring and Alerting→ SNMP MIB import Browser→ MIB Browser**.

2 From the top right pane, select **Import MIB file→ Browse** and select the required .MIB file and select **Apply**.

3 The MIB file is available at this location, **iso→ org→ dod→ internet→ private→ enterprises.**

Creating an Inventory Task to Inventory Selected Devices in a Custom Organizational Group

After you have created multiple organizational groups, see "Creating a New Organizational View and Organizational Group," you can inventory the Dell|EMC devices only.

1 Click **Home→ Discovery and Inventory→ Agentless Inventory** to display the **Agentless Inventory Home** page.

2 Under the **Agentless Inventory QuickStart** Web part, click **Run inventory wizard**.

The **Agentless Inventory Task Creation** page is displayed.

3 In step 1: **Choose devices to inventory**, for example, to inventory only the Dell|EMC devices on the network, select **Choose devices** and select **All Devices** from the **Choose a group package** drop down menu.

4 Clear all devices except the Dell|EMC devices and then click **Next**.

5 In step 2: **Inventory network task name**, enter a unique name—Dell Server Inventory Task—to help distinguish between various tasks of the same type and then click **Next**.

6 In step 3: **Schedule**, select **Now to run the schedule after** creating this task, and then click **Finish**. You can specify a later date and time to run this task, and make this a recurring task.

Viewing the Progress and Details of the Task

To view the progress of the inventory task:

1 Click **Home→ Discovery and Inventory→ Agentless Inventory** to display the **Agentless Inventory Home** page.

2 Under the **Agentless Inventory Tasks** Web part, select the **Tasks Run** tab.

The status and progress of the tasks are displayed.

3 Under the **Agentless Inventory Tasks** Web part, select the **Available Tasks tab.**

All available inventory tasks are displayed.

4 Double-click the task instance to view additional details of the task.

The details of the task are displayed in a new window.

Viewing Results of the Inventory Task

1 Click on **Manage→ All Devices**.

2 On the left-hand pane, expand the **All Devices** tree and select **Servers**.

The discovered systems are displayed on the right-hand pane with Resource Type as **Dell Computer**.

3 Double-click the system name for which you want to see the inventory details.

4 In the **Resource Manager Home** page, click **Summaries→ Hardware Summary**.

The inventory information of the system is displayed. To view Hardware Summary, install Server Administrator on the target system and categorize the system as a Dell Computer.

6

The Deploying Dell OpenManage Server Administrator Solution

The deployment solution of the Dell™ Management Console provides similar functionality as the Software Update feature in Dell OpenManage™ IT Assistant.

About Deployment Solution

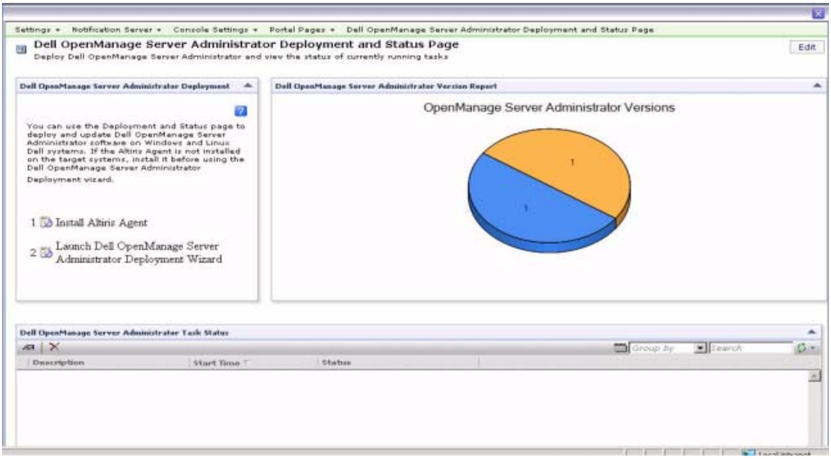
The deployment solution helps you to install the Dell OpenManage agent—Dell OpenManage Server Administrator—on target systems. Dell Management Console communicates with this agent to provide you with the status and health of the target systems. For more information on Server Administrator, see the *Dell OpenManage Server Administrator User's Guide* available on the Dell Support website at **dell.support.com.**

The deploy task includes the following: selecting a software package, specifying a schedule, and specifying the system to apply the software package. There are specific packages for Windows and Linux operating systems.

The Deploy Dell OpenManage Server Administrator User Interface

You can access the **Deploy Dell OpenManage Server Administrator** link in the Dell Management Console portal page on the **Dell Enterprise Management Quick Start** Web part under the **Discover Your Network** tab.

Knowing Your Deploy Dell OpenManage Server Administrator User Interface


Settings ▾
Notification Server ▾
Console Settings ▾
Portal Pages ▾
Dell OpenManage Server Administrator Deployment and Status Page
Edit
Dell OpenManage Server Administrator Deployment
Dell OpenManage Server Administrator Version Report
OpenManage Server Administrator Versions
1
1
Dell OpenManage Server Administrator Task Status
Group By
Search
Description
Start Time
Status
Local intranet

Dell OpenManage Server Administrator Deployment and Status Page

Deploy Dell OpenManage Server Administrator and view the status of currently running tasks

You can use the Deployment and Status page to deploy and update Dell OpenManage Server Administrator software on Windows and Linux Dell systems. If the Altiris Agent is not installed on the target systems, install it before using the Dell OpenManage Server Administrator Deployment wizard.

1 Install Altiris Agent

2 Launch Dell OpenManage Server Administrator Deployment Wizard

Dependency

To be able to deploy Server Administrator from the Dell Management Console, ensure that the Altiris™ agent is present on the target system and registered with the Dell Management Console system.

Others

Obtain the Server Administrator package (**sysmgmt.msi** for Microsoft Windows and .tar.gz and the corresponding .sign file for supported Linux operation systems) from the *Systems Management Tools and Documentation* DVD, the *Dell Server Updates* DVD, or from the Dell Support website at **support.dell.com**.

The Server Administrator package is created in the default, shared library folder. You can access this package from **Manage→ All Resources**.

Deploying Server Administrator Task

Software update involves creating a Software Update task and deploying the Server Administrator agent on the managed system.

Before you deploy OpenManage Server Administrator, you must ensure that the Altiris Agent is installed on the managed system. To install Altiris Agent on the managed system, see Pushing Altiris Agent to Managed Nodes.

Dell Management Console requires Server Administrator to be installed on Dell systems to manage them. Use the Software Update task to install or upgrade to Server Administrator version 5.3 or later.

NOTE: You can use this task to upgrade only if you have Server Administrator version 4.3 or later already installed on the target system.

NOTE: To uninstall Server Administrator from the target systems, see the *Dell OpenManage Server Administrator User's Guide* at the Dell Support website at **support.dell.com**.

Pushing Altiris Agent to Managed Nodes

To push Altiris Agent to managed nodes:

1 Launch Dell Management Console.

2 From Dell Management Console, do any of the following:

- Navigate to **Actions→ Agents/Plug-ins→ Push Altiris Agent**.
- From the **Dell Management Console Portal** page, in the **Dell Enterprise Management Quick Start** Web part, select **Discover Your Network→ Deploy Dell OpenManage Server Administrator**, and then in **Dell OpenManage Server Administrator Deployment and Status Page,** click **Install Altiris Agent**.

3 Click the **Select Computers** Button.

4 Select the computers on which you want to push or install the Altiris Agent and click **OK**.

5 Click **Install Altiris Agent**, and provide the Credentials for installing the Altiris Agent, and then click **Proceed With Install**.

Deleting Server Administrator Package from Management Station

To delete the existing Server Administrator packages from the Dell Management Console system:

1. Click **Manage**→ **All Resources.**
2. Search for *Dell OpenManage* components and delete **Software component**, **release**, **package**, and **product** with the same Dell OpenManage version.

   You can type *Dell* in the search field to view the Dell OpenManage Server Administrator imported packages.

Creating an Agent Deploy Task

If you are using Windows and Linux operating systems, you must create two agent deploy tasks—one for deploying Server Administrator on supported Microsoft Windows systems and the other for deploying Server Administrator on supported Linux operating systems.

1. Click **Home**→ **Dell Management Console Portal**.

   The **Dell Enterprise Management** page is displayed.
2. In the **Dell Enterprise Management Quick Start** Web part, click the **Discover Your Network** tab.

3 Click **Deploy Dell OpenManage Server Administrator**.

The **Dell OpenManage Server Administrator Deployment and Status** page is displayed.

NOTE: Install the Altiris agent before deploying Server Administrator. Register the agent with the Symantec Notification Server® that is used to deploy Server Administrator. If you push the agent from one system and Server Administrator from another, the task fails. For information on installing the Altiris Agent, see the Symantec documentation.

4 Click **Launch Dell OpenManage Server Administrator Deployment Wizard**.

5 On step 1: Select a software package of the **Dell OpenManage Server Administrator Deployment** page, then you can select from the following options and then click **Next**:

- **Create a new Software Delivery Package from a CD.**

  Select to upload the Server Administrator installer from the local system, CD/DVD, or a network location.

NOTE: If you choose this option, a package is created in the Symantec Software Library for future use.

- **Select an existing Software Delivery Package.**

  If you have already imported the package then you can reuse it.

NOTE: Use this task to upgrade only if Server Administrator version 4.3 or later is already installed on the target system.

You can specify additional parameters to deploy Server Administrator. For more information on the parameters, see the *Dell OpenManage Server Administrator User's Guide* located on the Dell Support website at **support.dell.com**.

6. On the second page of the wizard select the Windows or Linux package based on the requirement, and then click **Next**:

   a. Select the target systems using any of the following options:

      - **Quick Add:** Enter the system names in this field. This option is useful when the number of target systems is small.
      - **Add**: Add computers from a list of discovered systems. This option is useful when the number of target systems is medium.

        The **Select Computer** page is displayed.
      - **Add Groups**. This option is useful when the number of target systems is large.

   b. Select the systems on which you want to deploy Server Administrator and click **OK**.

7. On the third page of the wizard, select the deployment schedule and runtime options.

   Click **Now** and then click **Deploy Dell OpenManage Server Administrator**.

   NOTE: Select the **Override Maintenance window on target** option for the task to run even if it is scheduled outside the maintenance window. For more information on maintenance windows see the *Online Help*.

   The software update task will run as soon as you finish creating the task.

   If the target system has an Adaptec controller, the agent deploy task requires a reboot of the system.

   To restart the system: Select the **Reboot the target system if required** option.

If you want to deploy Server Administrator on systems with supported Linux operating systems, then, create a new task. For deploying Server Administrator on Linux systems, you must specify the corresponding signature file. This file is located in the *Dell Server Updates* DVD.

When you upload the Server Administrator MSI (for Windows) or **tar.gz** (for Linux) for the first time, a Server Administrator software update package is created and for the subsequent agent deploy tasks, you can reuse this package to deploy Server Administrator on different Dell systems.

Viewing the Task Details

After the task is run, the status is displayed on the **Dell OpenManage Server Administrator Deployment and Status** page under the **Dell OpenManage Server Administrator Task Status** Web part.

Double-click the task instance to view details of the task.

For tasks that are scheduled for later time, double-click the task from the **Dell OpenManage Server Administrator Task Status** Web part and change the schedule.

Changing Default Location of the Software Library

If you want to change the location of the library folder:

1. Choose a folder where you want to save the software packages.
2. Share the folder over the network and provide write permission to the administrator only.
3. Click **Settings→ All Settings.**
4. On the left pane, select **Settings→ Software→ Software Catalog and Software Library Settings→ Software Library Configuration**.
5. On the right pane, provide the new shared library location to Dell Management Console.

7

Managing Jobs and Tasks

A task is an action that you want to perform on a system.

The Dell™ Management Console enables you to perform tasks, such as, configuring the hardware or power reset a target device. Based on where you want to execute a task, these tasks are categorized as:

- Client Tasks — The client tasks are executed on remote computers through a Task Server. Client tasks always involve a communication between the server and a set of clients. For example, Altiris™ power control tasks.
- Task Server Tasks — A Task Server task can be run on the Symantec™ Management Console or on a system that has a Task Server installed. All the remote Task Servers should be registered with the Symantec Management Console. For example, command line builder tasks.
  The Task Server tasks are similar to client tasks, but can be run on an unmanaged system (that is, a system that does not have the Altiris Agent installed on it). For more information on Task Server, see the *Online Help* or Symantec documentation.

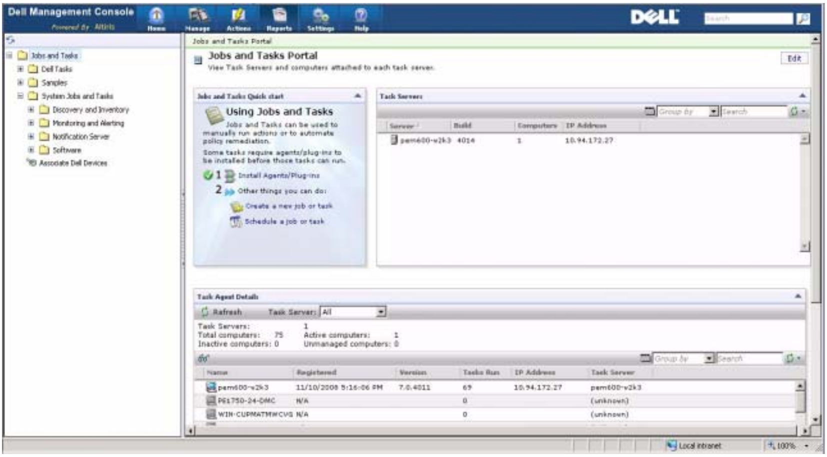
  A Task Server allows you to reuse tasks in multiple jobs or to clone and modify tasks as required.
- Server Tasks — The server tasks are executed on the Symantec Management Console. A server task may also involve communicating with a set of clients if the purpose of the task so requires. For example, network discovery tasks.

A job is a task that runs two or more tasks in a specific sequence. A complex scenario can have precondition checks to run under different situations by having nested jobs within each other. See the Online Help for more information on creating jobs.

The Jobs and Tasks User Interface

You can access the Jobs and Tasks portal page by clicking **Manage→ Jobs and Tasks**.

Knowing Your Jobs and Tasks User Interface



Jobs and Tasks Portal

View Task Servers and computers attached to each task server.

Using Jobs and Tasks

Jobs and Tasks can be used to manually run actions or to automate policy remediation.

Some tasks require agents/plug-ins to be installed before those tasks can run.

Server	Build	Computers	IP Address
pem600-v2k3	4014	1	10.94.172.27

Task Agent Details

Task Server: All

Task Servers: 1
Total computers: 75
Inactive computers: 0
Active computers: 1
Unmanaged computers: 0

Name	Registered	Version	Tasks Run	IP Address	Task Server
pem600-v2k3	11/10/2008 5:16:06 PM	7.0.4011	69	10.94.172.27	pem600-v2k3
PE1750-24-DMC	N/A		0		(unknown)
WIN-CUPMATMWCVG	N/A		0		(unknown)

The **Quick Start - Jobs and Tasks** Web part on the right pane is a good place to get started on the Tasks solution. You can use this Web part to create and schedule new tasks and jobs.

The **Task Computer and Devices** Web part displays a list of devices assigned to each Task Server. You can sort the devices on the Task Server or right-click a device to view the tasks run on the device.

The **Task Servers** Web part displays all the Task Servers registered with the Symantec Management Console.

On the left pane, you can view sample jobs and tasks.

NOTE: The sample tasks are read-only tasks and you can only run these tasks.

When you create your first Dell task, Dell Management Console creates the **Dell Task** folder under the **Jobs and Tasks** root folder.

Using the Jobs and Tasks Module

To display the **Jobs and Tasks Portal,** select click **Manage→ Jobs and Tasks**. The Task Management solution (**Create New Task** page) displays the tasks in a tree structure and is grouped in folders. The Dell tasks are grouped under the **Dell Tasks** folder.

You can schedule tasks to run half-hourly, hourly, during business hours, daily, weekly, monthly, or as custom-defined. The shared schedule allows you to specify the time, start date, end date, and repetitive execution, for example, daily, once, weekly, monthly, at logon, or at system startup.

You can run tasks on one or more devices or one or more collections. For tasks that are scheduled, the credentials entered are saved so that the task can run without user intervention.

Dell Management Console has pre-defined sample tasks for shutdown (Power Control Device), wake up (Power Control), command line (Run Script), and remote command line (Command Line Builder). You can use these sample tasks and modify them by configuring the task parameters appropriately.

NOTE: Install the Altiris Agent on the managed systems before you run the **Run Script** task.

All tasks listed under the **Dell Tasks** folder in the **Create New Task** page, except the **Associate Dell Devices** task, can be added as part of the Server and Client jobs.

The **Associate Dell Devices** task can only be added to a Server job.

For information on all Dell tasks, see the *Online Help*.

Scheduling a Task

To schedule a shutdown task on a group of systems, for example, every third Saturday of the month at 6 p.m. for the entire year, except in June, do the following:

1 Click **Manage→ Jobs and Tasks** to display the **Jobs and Tasks Portal**.

2 In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.

3 In the **Create New Task** page, select the **Power Control Device** task.

4 Select **Shut down** and click **OK**.

The **Power Control Device - Shut down** task is created and is displayed under the **Task Server Tasks**→ **Dell Tasks** folder.

5 Select the **Power Control Device - Power Off** task from the **Jobs and Tasks** tree on the left pane.

The details are displayed in the right pane.

6 In the **Task Status** pane, select **New Schedule** and configures the following settings in the **Schedule Task** page:

Schedule: Shared Schedule

Select Shared Schedule: Monthly

Click **New**.

7 In the **Create New Shared Schedule** page, enter name and description of the schedule.

Select **Add schedule**→ **Scheduled Time** and select 1800 hours as the start time for the shut down task.

Click **No repeat** and select the **Month (week view)** and select **Week 3** and **Saturday** in the **Repeat Schedule** screen.

Select the **Year (week view)** and select all months in the year except June.

8 In the **Create New Shared Schedule** page, click **Advanced** and select the start and end dates (for the entire year) for this task and click **OK**.

9 In the **New Schedule** page, click **Add** to select the computers or groups of computers for this task.

10 On the **Power Control Device - Shut down** task page, click **Save changes**.

The Shut down task scheduled for every third Saturday of the month at 6p.m. for the entire year, except in June, is created.

NOTE: To run the **Power Control Device - Shut down** task immediately on some systems, in the **Task Status** pane, click **Quick Run** and select the systems.

Creating a Configure SNMP Task

NOTE: You can configure this task for managed systems running Windows operating systems only.

You can configure the SNMP service properties, such as Security, Traps, and Agents using the **Configure SNMP** task.

1. Click **Manage→ Jobs and Tasks** to display the **Task Management Portal**.
2. In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.
3. In the **Create New Task** page, under **Dell Tasks→ Other** folder, select the **Configure SNMP** task.
4. In the right pane, in the **SNMP Task Settings**, select the **Add or Modify SNMP Service Properties**.
5. Click **Security** to set the security properties for a community.
6. In the **SNMP Service Security Properties** page, add the accepted community names for your organization and specify whether or not Dell Management Console should accept SNMP packets from a host.

   To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.

   To limit the acceptance of SNMP packets from the Dell Management Console server, click **Accept SNMP packets from these hosts**, click **Add**, and then types the Dell Management Console server host name or IP address in the **Host name, IP, or IPX** address box.
7. In the **SNMP Task Settings** section, click **Traps** to specify the community name and set the trap destinations.
8. In the **SNMP Task Settings** section, click **Agents** to specify the physical location of the agent and the person responsible for this agent.
9. Click **OK** to create the configure SNMP task.

   This task is displayed on the **Jobs and Tasks** portal page under **Dell Tasks**.

   NOTE: Enable the SNMP service on the managed systems before running this task.
10. To run the task on a group of systems, click **New Schedule**.

11 In the **Create New Schedule** page, select **Now**.

12 In the **Selected Devices** section, click **Add** to add the devices on which you want to run this task.

NOTE: Restart SNMP service on the managed systems for the changes to take effect.

Creating a Command Line Builder Task for Executing Server Administrator Commands on Managed Systems

Command line builder tasks are pre-defined tasks, such as remote Server Administrator task, IPMI task, or a Remote Access Controller task, that enable you to run an executable with a set of defined parameters or commands and targeted towards a single or a set of managed systems.

To create a command line builder task to display a summary of the system information including system chassis, operating system, software profile, and hardware profile information of a group of managed systems.

NOTE: Server administrator must be installed on the managed systems for Dell Management Console to fetch this data.

1 Click **Manage→ Jobs and Tasks** to display the **Task Management Portal**.

2 In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.

3 In the **Create New Task** page, under **Dell Tasks→ Other** folder, select the **Command Line Builder** task.

4 From the **Command Line Type**, select **Remote Server Administrator** and then `omreport`.

Click **Add**.

Select `system` and click **Add**.

Select `summary` and click **Add**.

Or, in **Command Syntax**, type `omreport system summary`.

NOTE: You can select up to four parameters from the drop-down list; after which the parameters are not dynamically populated.

5 Click **Advanced and** enter the user credentials and specify the path for the log file to capture the output and then click **OK**.

> **NOTE:** If you do not specify any credentials, the task uses the system-login credentials to communicate with the managed device.

> **NOTE:** The task uses the system-login credentials of the management station to communicate with the managed device, therefore, if you do not specify credentials for managed systems running supported Linux operating systems, the task fails and displays multiple "Access Denied" messages.

> **NOTE:** If you are creating this task for managed systems running on Linux, then, select the **Task Options** tab and specify the **SSH port number** and select the **Generate Trusted key for Linux**.

The Command Line Builder task is displayed under the **Dell Tasks** folder.

6 To run the task on a group of systems, click **New Schedule**.

7 In the **Create New Schedule** page, select **Now**.

8 On the **New Schedule** page, click **Add** to add the devices on which you want to run this task.

Creating a Command Line Builder Task on Managed Systems to Run Remote Access Controller Commands

To create a command line builder task to run remote access controller commands managed systems.

> **NOTE:** Dell Remote Access Controller must be present on the managed systems for Dell Management Console to run these commands.

1 Click **Manage→ Jobs and Tasks** to display the **Task Management Portal**.

2 In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.

3 In the **Create New Task** page, under **Dell Tasks→ Other** folder, select the **Command Line Builder** task.

4 From the **Command Line Type**, select **Dell OpenManage Remote Access Controller** and then `setniccfg`.

Click **Add**.

Select `-s` and enter the value `192.168.0.120 255.255.255.0 192.168.0.1` and then click **Add**.

Or, in **Command Syntax**, type `setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1`.

NOTE: You can select a maximum of four parameters from the drop-down list, after which the parameter drop-down is not dynamically populated.

5 Click **Advanced** and enter the user credentials and specify the path for the log file and then click **OK**.

NOTE: If you do not specify any credentials, the task uses the factory default credentials to communicate with the managed device.

The command Line Builder task is displayed under the **Dell Tasks** folder.

6 To run the task on a group of systems, click **New Schedule.**

7 In the **Create New Schedule** page, select **Now**.

8 On the **New Schedule** page, click **Add** to add the devices on which you want to run this task.

Creating an Associate Dell Devices Task

If you discover devices using **Import Microsoft Active Directory** or **Import Domain Membership/WINS** task or by pushing the Altiris Agent on the target devices, the Dell devices are not classified.

For more information on discovering devices with Active Directory import or domain resource, see the *Dell Management Console Online Help*.

To associate a connection profile with each of the discovered devices and classify these devices as Dell devices.

A connection profile contains protocol settings and credentials required by the discovery and inventory modules to communicate with remote agents on the device. Discovery and inventory of devices may not work correctly without this association. Associate Dell Devices task should be set to run periodically to reflect changes in the network topology or protocol settings, and to create associations for new devices.

To create this task:

1. Click **Manage→ Jobs and Tasks** to display the **Task Management Portal**.
2. In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.
3. In the **Create New Task** page, under **Dell Tasks→ Other** folder, select the **Associate Dell Devices** task.
4. On the right pane, select the default connection profile and under **Select the target devices you want to associate with the selected connection profile**, select the devices discovered through the **Import Microsoft Active Directory** or **Import Domain Membership/WINS** task.
5. Select **Apply to→ Resources**.
6. On the **Select Resources** page, click **Add Rule** in the **THEN** drop down, select **exclude resources not in resource list** and click the ellipses (**...**).
7. From the group of **Available Resources**, under **Group**, select the devices you want to run the task on and then click **OK**.

   The devices that you selected is displayed on the **Create New Task** page.
8. Schedules the task to run right away.

NOTE: The **Associate Dell Devices** is a Server task and can be created and run only on the Symantec Management Console. Therefore, the **Quick Run** and **Target Selection** options under **New Schedule** are not displayed.

To view the result of this task:

1. Click **Manage→ All Resources**.
2. The associated Dell devices are now displayed under **Organizational Views→ All Devices**.

Dell Tasks Rollout Policy

If you are managing a large multi-tiered (hierarchical) enterprise to monitor devices on your network, you can install the Task Server on multiple systems to reduce the load on the Symantec Management Console. This arrangement also reduces the network traffic by having the Altiris Agent access the closest Task Server for jobs and tasks downloads.

For more information on Creating and managing hierarchical relationships, see the *Online Help*.

To support the multi-tiered Task Server architecture, the Dell tasks require the Dell tasks rollout policy to be run on all the registered Task Servers.

To run the Dell tasks rollout policy on all registered Task Servers, do the following:

- Manually enable the rollout policy that targets all Task Servers using the built-in collection.
- After you enable the rollout policy, wait until next polling interval for the task components to be deployed.

Registering a Site Server (Task Server) With the Notification Server Computer

1. Click **Settings→ Notification Server→ Site Server Settings**.
2. On the left hand pane, expand the **Site Management** listing.
3. If the Task Server is not displayed, click **New→ Site Server**.
4. Select the **Site Server** from the list of **Available computers** and click **OK**.
5. Select the services you want for this server.

   The server should now be configured properly as a site server for Task Services.

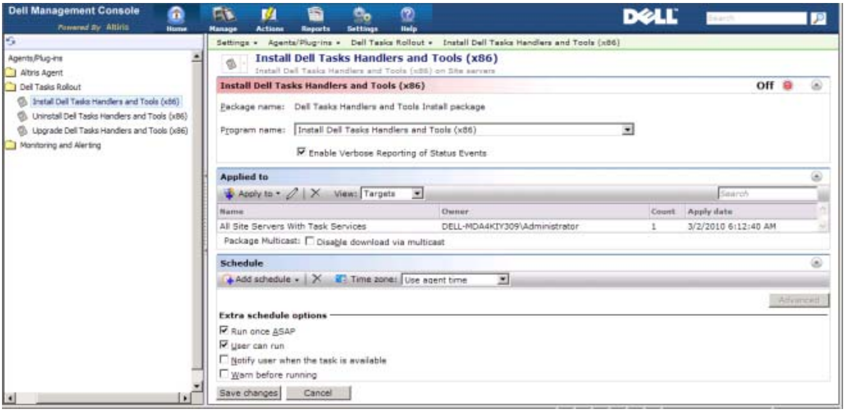
The **Task Server** Web part in the **Jobs and Tasks** portal (**Manage→ Jobs and Tasks**) displays all Task Servers registered with the Notification Server computer. If the Notification Server and Task Server are on the same system, the Computer count is displayed as 1.

Creating a Dell Tasks Rollout Policy Task

1 Click **Actions**→ **Agents/Plug-ins**→ **Rollout Agents/Plug-ins**.

2 Under the **Dell Tasks Rollout** folder, select **Install Dell Tasks Handlers and Tools**.

3 On the right pane, for the **Program Name**, select **Install Dell Tasks Handlers and Tools**.



Dell Management Console
Powered By Altiris
Home
Manage
Actions
Reports
Settings
Help
DELL
Search
Settings ▾ Agents/Plug-ins ▾ Dell Tasks Rollout ▾ Install Dell Tasks Handlers and Tools (x86)
Agents/Plug-ins
Altiris Agent
Dell Tasks Rollout
Install Dell Tasks Handlers and Tools (x86)
Uninstall Dell Tasks Handlers and Tools (x86)
Upgrade Dell Tasks Handlers and Tools (x86)
Monitoring and Alerting
Apply to ▾
View:
Add schedule ▾
Advanced
Save changes
Cancel

Install Dell Tasks Handlers and Tools (x86)

Install Dell Tasks Handlers and Tools (x86) on Site servers

Install Dell Tasks Handlers and Tools (x86) Off

Package name: Dell Tasks Handlers and Tools Install package

Program name: Install Dell Tasks Handlers and Tools (x86)

☑ Enable Verbose Reporting of Status Events

Applied to

View: Targets

Name	Owner	Count	Apply date
All Site Servers With Task Services	DELL-MDA4KIY309\Administrator	1	3/2/2010 6:12:40 AM

Package Multicast: ☐ Disable download via multicast

Schedule

Time zone: Use agent time

Extra schedule options

☑ Run once ASAP

☑ User can run

☐ Notify user when the task is available

☐ Warn before running

4 Click **Apply to**→ **Computers**.

> **NOTE:** You can apply the policy only to Tasks that meet the Task Server requirements. For more information, see the *Online Help*.

5 On the **Select Computers** screen, click **Add rule**.

6 In the **THEN** drop down menu, select **exclude computers in** and then select **Computer list** and click **(...)**.

7 Select the computers you do not want to include as Task Servers and click **OK**.

8 On the **Dell Advanced Tasks Handlers Install** page, enter the schedule for the task and click **Save changes**.

> **NOTE:** You can create a **Dell Configuration Tasks handlers install** task using the same procedure.

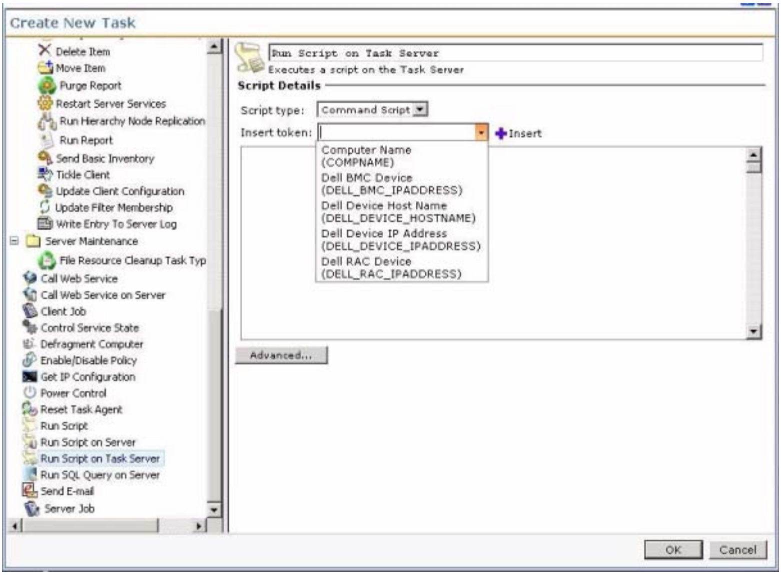
The policy creates a task internally to deploy the task components.

Tasks Token

A token is an item that has no value except in a particular instance. Dell Management Console allows you to create command line tasks using pre-defined tokens. These tokens are replaced with actual values corresponding to the target device when the task is run.

Dell Management Console has the following pre-defined tokens:

- %DELL_BMC_IPADDRESS%,
- %DELL_DEVICE_HOSTNAME%,
- %DELL_RAC_IPADDRESS%, and
- %DELL_DEVICE_IPADDRESS%



Create New Task

Run Script on Task Server

Executes a script on the Task Server

Script Details

Script type: Command Script

Insert token:

To use the preceding tokens to create a task:

1. Click **Manage→ Jobs and Tasks** to display the **Task Management Portal**.
2. In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.
3. In the **Create New Task** page, select the **Run Script on Task Server** task.
4. On the right pane, select the **Script Type**.

5 Enter the command script text and select a pre-defined Dell token.

6 Click **Insert** to insert a token in the script text and click **OK**.

7 The task is created and displayed under the **Jobs and Tasks** folder on the left pane.

Creating a Run Script Task Using Task Tokens for Executing a Script or Command on Managed Storage-Systems

You can create a **Run Script on Task Server** task to run a Naviseccli command to get the current values of the performance logging properties on a group of managed storage-systems.

NOTE: Ensure that the managed storage-systems support Naviseccli commands. Configure the management station to run Naviseccli commands on the remote storage-systems.

1 Click **Manage**→ **Jobs and Tasks**.

2 In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.

3 In the **Create New Task** page, select the **Run script on Task Server** task.

4 From the **Script Type**, select **Command Script**.

5 In the script text, enter the following command syntax:

```
"C:\NaviCLITool\naviseccli.exe" -h -
AddUserSecurity -password mypass -scope 0 -user
Tom analyzer -get -narinterval
```

6 From **Insert token** drop down menu, select the **DELL_DEVICE_IPADDRESS** token and click **Insert** to insert the token in the script text after `-h` option and, click **OK**.

The command displayed as follows:

```
"C:\NaviCLITool\naviseccli.exe" -
h%DELL_DEVICE_IPADDRESS% -AddUserSecurity -
password mypass -scope 0 -user Tom analyzer -get -
narinterval
```

7 The task is created and displayed under the **Jobs and Tasks** folder on the left pane.

8. To run the task on a group of managed storage-systems, click **New Schedule**.
9. In the **Create New Schedule** page, select **Now**.
10. On the **New Schedule** page, click **Add** to add the managed storage-systems on which you want to run this task.
11. When the task runs, the %**DELL_DEVICE_IPADDRESS**% token is substituted by the actual IP address for each target storage-system.

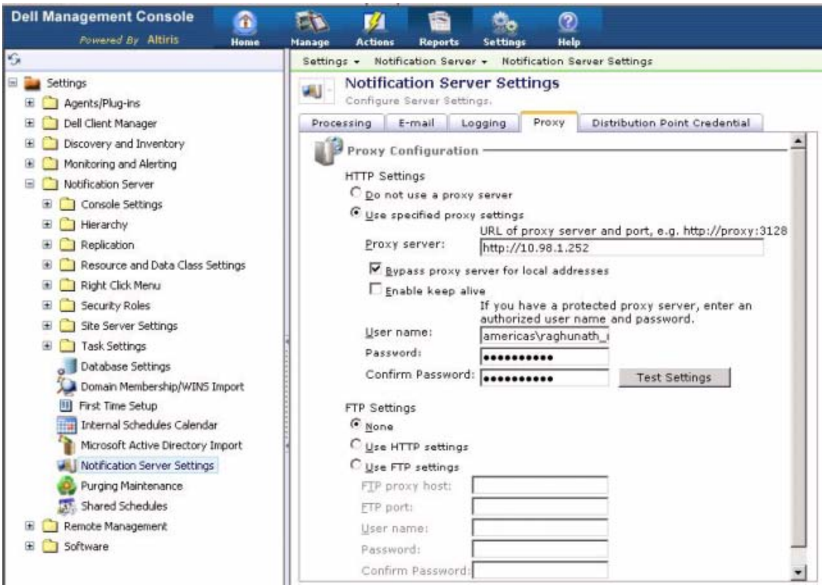
Creating a Warranty Extractor Task

The Warranty Extractor Task is a Server Task that can be used to extract warranty information for managed devices with service tags (specifically, Dell PowerEdge™ systems, Dell PowerConnect™ switches, and DRAC/CMC). The task retrieves warranty information from the Dell Support website.

To run the warranty information extraction task successfully, ensure that the Dell Management Console can connect to the Dell Support website.

To configure and test proxy settings.

1. Click **Settings**→ **All Settings.**
2. In the left pane, click **Notification Server**→ **Notification Server Settings**.
3. On the right pane, click the **Proxy** tab to configure the proxy settings.



HTTP Settings

○ Do not use a proxy server

● Use specified proxy settings

URL of proxy server and port, e.g. http://proxy:3128

Proxy server: http://10.98.1.252

☑ Bypass proxy server for local addresses

☐ Enable keep alive

If you have a protected proxy server, enter an authorized user name and password.

User name: americas\raghunath_

Password: ●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●

FTP Settings

● None

○ Use HTTP settings

○ Use FTP settings

FTP proxy host:

FTP port:

User name:

Password:

Confirm Password:

To create the Warranty Extractor task:

1 Click **Manage**→ **Jobs and Tasks** to display the **Task Management Portal**.

2 In the **Jobs and Tasks Quick Start** Web part, click **Create a new job or task**.

3 In the **Create New Task** page, under the **Dell Utilities** folder, select the **Warranty Extractor** task.

4 On the right pane, enter the number of days for which you want to retrieve the warranty information for the newly discovered devices.

> **NOTE:** When you run the Warranty Extractor Task for the first time, warranty information is retrieved for all the managed devices. On subsequent runs, the retrieve information for newly-discovered devices are retrieved (that is, devices that were discovered by the Dell Management Console after the first run of the task). Dated warranty information is refreshed (that is, warranty information that was retrieved over 60 days ago.)

You can choose to refresh either all the warranty information by selecting **Delete all existing warranty information** or choosing a selective refresh by entering a value for **refresh information retrieved n days ago**.

NOTE: If the warranty report does not display any retrieved information, then, check if the proxy settings are enabled correctly, and for all subsequent reports, you must select the **Delete all existing warranty information** option.

5 If the Dell Management Console is managing a large number of devices, the Warranty Extractor task may take some time to complete. If the task is running for a long time, you can specify that the task retrieve and process information in subsets of size 'n' (specified in the **Update information for 'n' devices at a time** field).

   You can click **Warranty report** to view the information retrieved for the *n* devices that you specified.

6 Click **OK**.

   This task is displayed on the **Jobs and Tasks** portal page under **System Jobs and Tasks→ Notification Server**.

7 To run the task on a group of systems, click **New Schedule**.

8 In the **Create New Schedule** page, select **Now**.

You can view historical information about the devices that are no longer managed by the Dell Management Console, that is, devices that are deleted from the Dell Management Console device list. This information is updated in the warranty report each time you run the Warranty Extractor Task and is displayed in the **Device Status** column.

Hardware Configuration Tasks

Dell™ Management Console provides a set of hardware configuration tasks that you can use to quickly configure server hardware settings. These tasks enable you to configure common BIOS and common Baseboard Management controller (BMC) settings on Dell PowerEdge™ systems.

About Hardware Configuration Tasks

The hardware configuration tasks offer the same functionality as the System BIOS task. If you change any settings on the **Advanced** pane of **Hardware Configuration Tasks**, you must re-enter the **Admin** password to run the task successfully.

For more information on Advanced settings and hardware configuration parameters, see the *Dell Management Console Online Help*.

You can configure the following settings using the hardware configuration tasks:

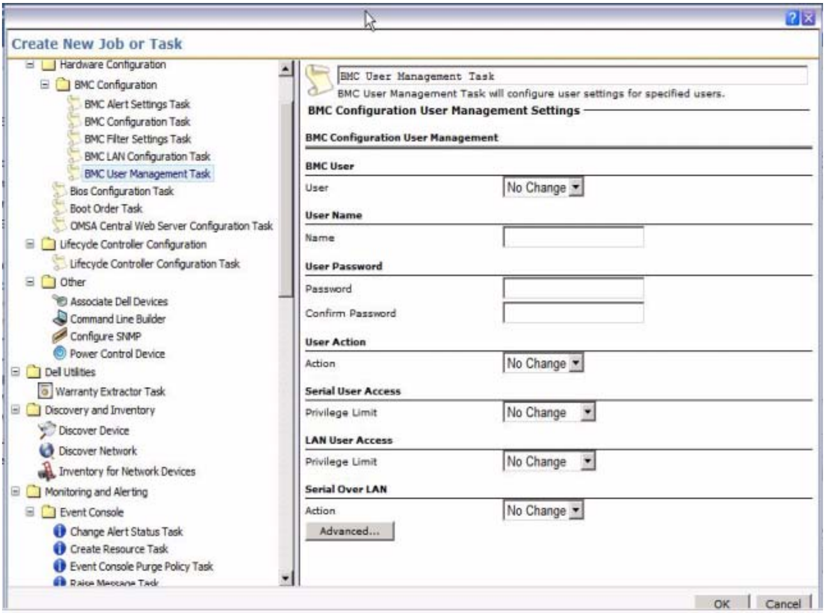
- BIOS Configuration Task — Execute this task to configure the Front Panel LCD settings, memory redundancy settings, keyboard numlock settings, Network Interface Controller (NIC) settings and system security settings.
- BMC Configuration — This task has five sub-tasks:
  - BMC Alert Settings Task — Perform this task to configure platform event alert policies and alert destinations.
  - BMC Configuration Task — Perform this task to configure common BMC parameters, such as LAN channel access, serial configuration parameters, and terminal node settings.
  - BMC Filter Settings Task — Perform this task to configure Platform Event Filter (PEF) settings. For a given PEF event, such as temperature probe failure, you can configure appropriate actions, such as server power off or reboot.
  - BMC LAN Configuration Task — Perform this task to configure LAN and Serial Over LAN (SOL) parameters on Dell PowerEdge systems.

  - BMC User Management Task — Perform this task to configure user settings for specified users.
- Boot Order Task — Perform this task to change the primary device boot sequence of managed systems.
- Central Web Server Configuration Task — Perform this task to configure the Central Web Service URL launch point on managed systems that have Dell OpenManage™ Server Administrator installed.
- Lifecycle Controller Configuration Task — Perform this task to configure the Lifecycle Controller settings.
- Server Task — Health Monitor Email Task — Perform this task to send e-mail alerts on the status of the preselected devices' health.
- Create New Task

Knowing Your Hardware Configuration Task User Interface

To access the Jobs and Tasks portal page: click **Manage→ Jobs and Tasks**.

The **Hardware Configuration** folder is displayed under the **Dell Tasks** folder.



BMC User Management Task

BMC User Management Task will configure user settings for specified users.

BMC Configuration User Management Settings

BMC Configuration User Management

BMC User

User No Change

User Name

Name:

User Password

Password:

Confirm Password:

User Action

Action: No Change

Serial User Access

Privilege Limit: No Change

LAN User Access

Privilege Limit: No Change

Serial Over LAN

Action: No Change

Creating a Hardware Configuration Task

To create a hardware configuration task, see “Using the Jobs and Tasks Module.”

You can view the tasks from the Dell Management Console portal page, in the **Job and Tasks Status** Web part. Double-click a task to view its **Output Properties**.

For more information, see the *Online Help*.

9

Monitoring and Alerting

Dell™ Management Console communicates with managed devices on the network to collect *health* and *performance* data. The Monitoring and Alerting module is the primary interface for monitoring real-time health, performance, and power consumption of systems. This feature uses various protocols such as, Simple Network Management Protocol (SNMP), Common Information Model (CIM), and Intelligent Platform Management Interface (IPMI) to communicate with managed devices.

NOTE: When you configure monitoring and alerting in Dell Management Console. Tracking will not start until the new configuration is active.

Dell™ OpenManage™ Storage Management Related Notes

- When firmware of a storage attached to a server is out of date, in Dell Management Console, the Storage Controller Component status displays a Warning status. For more information on the status of the Storage Controller Component, see OpenManage Server Administrator.
- Whenever a virtual disk is deleted or a physical disk is removed in OpenManage Storage Management; the change is reflected in Dell Management Console only when the monitor agent is restarted or the device session is refreshed (By default, the device session is refreshed, once an hour.)
- Management Information Base (MIB) supports component and rollup status'. The Component status is the status of an element that is treated independent of any rollup status of any child element. The Rollup status is the worst case status of an element and its children. OpenManage Storage Management and Dell Management Console have different interface and requirements to display these status':
  - The OpenManage Storage Management user interface displays only the rollup status. This is specifically required so that you can determine a non-normal state without having to drill-down the complete hierarchy to determine a possible issue.
  - Dell Management Console displays the component status. Dell Management Console monitors devices in a flat view wherein you can see all components that have a non-normal status at once. It is

extremely important not to elevate the component status of any element as this may lead to an assumption that the component is bad, but, the change in status may be due to some rollup status. Therefore, Dell Management Console will not always match the OpenManage Server Administrator user interface for storage drill-down status.

- Use the latest OpenManage version supported for a hardware to prevent errors due to differences in the counters supported in different OpenManage versions.
- All instances for a single counter share a single alert and new alert is not generated when another instance goes to a non-normal state. For example, if there are four temperature probes and an alert is received due to one probe being in a warning state, then even if the another one of the temperature probes goes into a warning state a new alert is not generated.
- A probe instance naming may not match in the OpenManage Server Administrator user interface and the Dell Management Console user interface.

About Monitoring

The Monitor solution allows real-time monitoring of discovered devices through either an agent or agentless interface as defined in the monitor policy.

NOTE: In the context of Dell Management Console, *agent-based* means the Altiris™ agent is installed on the target systems; whereas *agentless* means the Dell systems management agent—Dell OpenManage™ Server Administrator—is installed on the target systems.

NOTE: Symantec Inc. has acquired Altiris® Inc. and this document may have mixed references to both Altiris and Symantec.

A policy defines a set of rules and a target group on which to execute these rules. The rules define the data to monitor and the conditions on which to raise alerts or take some action. Metrics define the data to be monitored and the poll interval for retrieving that data. Dell policies define metrics, rules, and policies to enable health and performance monitoring for Dell hardware.

NOTE: See the Symantec™ User's Guide on the Monitor Solution™ for more information.

Table 9-1. Description of Dell Policies

Dell Policy	Description	Agent -based/ Agentless	Support Coverage	Default Behavior	Default Poll Intervals
Device Primary Health	Monitors the primary device health (Dell OpenManage™ Server Administrator provides this information for Dell servers. For all other devices the embedded agent provides this information.)	Agentless	All Dell devices	Enabled	1 hour
Device Agent Health–Dell Remote Access Controller In-Band	Monitors the health of Dell Remote Access Controller (DRAC) In-Band	Agentless	Dell servers with DRAC	Enabled	1 hour
Device Agent Health–Dell OpenManage Storage Management	Monitors the health of the Dell OpenManage Storage Management	Agentless	Dell servers with Storage Manageme nt	Enabled	1 hour

Table 9-1. Description of Dell Policies *(continued)*

Dell Policy	Description	Agent -based/ Agentless	Support Coverage	Default Behavior	Default Poll Intervals
Device Connection State	Monitor the device connection state	Agentless	All Dell devices	Enabled	1 hour
Performance Monitoring for Microsoft® Windows®	Monitors Windows performance counters	Agentless	Dell servers with supported Windows operating system	Disabled	2 minutes
Performance Monitoring for Linux	Monitors Linux performance counters	Agent-based	Dell servers with supported Linux operating system	Disabled	2 minutes
Power Monitoring	Monitors Dell servers	Agentless	Dell Servers with OpenManage Server Administrators	Disabled	1 hour

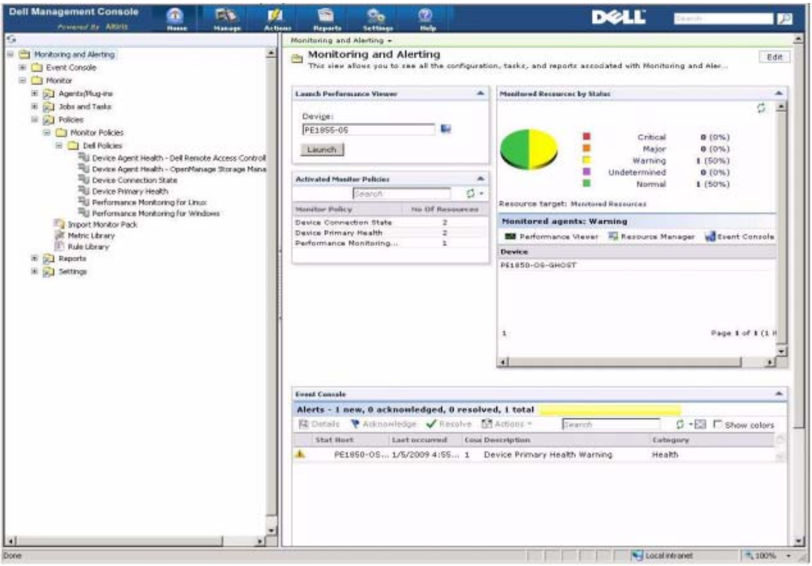
NOTE: All health policies are enabled by default, but you have to enable the performance and power policies. Historical and real-time views only display the enabled policies.

NOTE: The poll times for monitoring are defined on a per metric basis; however, default poll times for all metrics in a policy are the same.

The Monitoring and Alerting User Interface

You can access the Monitoring and Alerting module by clicking **Home→ Monitoring and Alerting**.

Knowing Your Monitoring and Alerting User Interface



Monitoring and Alerting

This view allows you to see all the configuration, tasks, and reports associated with Monitoring and Aler...

Device: PE1855-05

Monitor Policy	No Of Resources
Device Connection State	2
Device Primary Health	2
Performance Monitoring...	1

🟥	Critical	0 (0%)
🟧	Major	0 (0%)
🟨	Warning	1 (50%)
🟪	Undetermined	0 (0%)
🟩	Normal	1 (50%)

Resource target: Monitored Resources

Monitored agents: Warning

Device
PE1850-OS-GHOST

1 Page 1 of 1 (1 i

Event Console

Alerts - 1 new, 0 acknowledged, 0 resolved, 1 total

Stat	Host	Last occurred	Cou	Description	Category
⚠	PE1850-OS...	1/5/2009 4:55...	1	Device Primary Health Warning	Health

The left pane displays the **Monitoring and Alerting** tree. From this tree, you can access policies, the **Metrics Library**, **Rule Library**, **Reports**, and **Settings**.

The right pane displays the Web parts of the user interface. From this pane, you can do the following tasks:

- Launch the performance viewer.
- View activated policies.
- Monitor resources by status.
- View the Event Console, which displays current received alerts.

Dependencies

The Monitoring and Alerting solution is dependent on various factors. Table 9-2 describes these factors in detail.

Table 9-2. Dependencies of the Monitoring Solution

Dependency	Description
Device Agents	Health monitoring requires an agent on the monitored device to provide the data over a protocol. For example, on Dell servers Server Administrator must be installed to monitor the server and retrieve its primary health status. Similarly, a printer must have an embedded agent that supports SNMP in order to monitor its health.
Protocol Support	Dell Monitor metrics are S*mart Metrics* and have protocol dependencies. The metrics require support from one or more of the following protocols or interfaces—SNMP, WMI, WS-MAN, IPMI, NaviCli, Symbol, and Linux commands. See “Connection Profiles and Credentials Management.”
Discovery Solution	Devices that you want to monitor must be discovered and categorized as Dell devices. The discovery solution gathers data for the agent version and the manufacturer, which is used when viewing the agent health in the **Resource Manager** view. **NOTE:** A device can be monitored only by the protocols through which it was discovered. **NOTE:** For a device to be monitored, it should be classified as a *Dell* device. For example, **Dell Computer**, **Dell Printer**, and so on.
Event Solution	The Event Console displays all SNMP traps and monitor alerts received by Dell Management Console. Various Web parts including **Managed Resources by Status, Group View,** and **Resource Manager Health View** use the monitor alerts for computing the device health. Additionally, SNMP traps also drive the “OnDemand Monitoring” feature.
Reporting Solution	The report solution installs Dell monitor-based reports.
Dell Management Console Home page	The Home page contains the **Group Health View**, which is the primary interface for viewing device health status.

Table 9-2. Dependencies of the Monitoring Solution *(continued)*

Dependency	Description
Dell License	Dell License is the default license and is required to monitor the Dell devices. The Dell License also allows limited customization of the existing policies. However, it does not allow you to create new policies.
Unrestricted License	Unrestricted license is the full license, which allows complete modification of the existing monitor policies and creation of user-defined policies. You can purchase this plug-in from Symantec.
Altiris Agent for Linux	Required for Linux performance monitoring.
Linux Monitor Agent	Required for Linux performance monitoring.

Licensing Restrictions for the Monitoring and Alerting Solution

Dell Management Console carries a limited license that impacts the features that you can use in the Monitoring and Alerting solution. This license allows you to run the policies on Dell devices only and allows a limited amount of modification to the policies.

However, if you purchase the unrestricted license or additional monitor packs, you can access the full feature set on the Dell policies as well.

Limited Dell License

With this license, you cannot do the following tasks:

- Create metrics.
- Create rules.
- Clone metrics.
- Modify metrics or rules beyond following exceptions.

You can perform these actions on the Metrics:

- Modify metric polling interval.
- Modify metric timeout.
- Enable or disable metrics.

You can perform these tasks on the Rules:

- Modify rule condition.
- Modify rule value type.
- Modify rule value.
- Modify rule repeat count.
- Modify rule overtime value.
- Modify rule state attributes.
- Modify rule actions attributes.
- Enable or disable rules, packs, and categories.
- Clone rules.

You can perform these tasks on the Policies:

- Modify policy targets.
- Add or delete rules from policies.
- Clone policies.

Performance Monitoring

Performance monitoring enables you to monitor a standard set of performance counters across supported Microsoft Windows and Linux operating systems.

Dependencies for Performance Monitoring

Table 9-3. Dependencies for Performance Monitoring

Dell Policy	Agent/ Agentless	Support Coverage	Default Behavior	Dependencies
Performance Monitoring for Windows	Agentless	Dell servers with supported Windows operating system	Disabled	WMI protocol; Windows 2003 or later
Performance Monitoring for Linux	Altiris Agent	Dell servers with supported Linux operating system	Disabled	glibc 2.2 or later, systat, Linux agent and monitoring agent **NOTE:** For more information on the Monitor solution, see the Symantec User's Guide.

Installing Systat for Linux Performance Monitoring

Confirm if the rpm for this library is already present on the Linux server by typing:

```
rpm -qa | grep sysstat
```

If the rpm is present, run this command to install the library:

```
rpm -i <package name>
```

If the library or rpm is not present on the Linux server, download it from:

pagesperso-orange.fr/sebastien.godard/

You can also find the rpm on the Linux operating system media.

Download the rpm to the Linux server and install the rpm as described earlier.

NOTE: It is highly recommended that you do not compile the sysstat source.

Metrics for Performance

Performance metrics are based on the same type of counters for Windows and Linux operating systems.

Table 9-4. Metrics for Performance

Metric (Total Count=simple+compound)	Description
CPU	
%Kernel Utilization Time	The percentage of elapsed time that the process threads spend executing code in privileged mode. When a Windows system service is called, the service often runs in privileged mode to gain access to the system-private data. Such data is protected from access by threads executing in user mode. Calls to the system can be explicit or implicit, such as page faults or interrupts. Unlike earlier operating systems, Windows uses process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. Windows does some work on behalf of the application that may appear in other subsystem processes in addition to the privileged time in the process.
%Processor Utilization Time	The percentage of elapsed time that the processor spends to execute a non-idle thread. This value is calculated by measuring the duration the idle thread is active in the sample interval, and subtracting that time from the interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of the processor activity.

Table 9-4. Metrics for Performance *(continued)*

Metric (Total Count=simple+compound)	Description
%User Utilization Time	The percentage of elapsed time the processor spends in the user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. The alternative, privileged mode, is designed for operating system components and allows direct access to hardware and all memory. The operating system switches application threads to privileged mode to access the operating system services. This counter displays the average busy time as a percentage of the sample time.
Logical Disk	
Logical Disk Free Space	The percentage of the total usable space on the selected logical disk drive that was free.
Logical Disk IO/Sec	The rate of read and write operations on the disk.
Memory	
% Page File Usage	The ratio of Memory\\Committed Bytes to the Memory\\Commit Limit. Committed memory is the physical memory in use for which space has been reserved in the paging file should it need to be written to disk. The commit limit is determined by the size of the paging file. If the paging file is enlarged, the commit limit increases, and the ratio is reduced. This counter displays the current percentage value only; it is not an average.

Table 9-4. Metrics for Performance *(continued)*

Metric (Total Count=simple+compound)	Description
Available Memory	The amount of physical memory available to processes running on the system, in Megabytes, rather than bytes as reported in Memory\\Available Bytes. It is calculated by adding the amount of space on the Zeroed, Free, and Standby memory lists. Free memory is ready for use; Zeroed memory are pages of memory filled with zeros to prevent later processes from seeing data used by a previous process; Standby memory is memory removed from a process' working set (its physical memory) on route to disk, but is still available to be recalled. This counter displays the last observed value only; it is not an average.
Pages IO/Sec	The rate at which pages are read from or written to the disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. It is the sum of Memory\\Pages Input/sec and Memory\\Pages Output/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory\\Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) non-cached mapped memory files.
Network	
Incoming Bytes/Sec	The rate at which bytes are received over each network adapter, including framing characters. Network Interface\\Bytes Received/sec is a subset of Network Interface\\Bytes Total/sec.
Incoming Packets/Sec	The rate at which packets are received on the network interface.
Outgoing Bytes/Sec	The rate at which bytes are sent over each network adapter, including framing characters. Network Interface\\Bytes Sent/sec is a subset of Network Interface\\Bytes Total/sec.

Table 9-4. Metrics for Performance *(continued)*

Metric (Total Count=simple+compound)	Description
Outgoing Packets/Sec	The rate at which packets are sent on the network interface.
Physical Disk	
Average Access Time	The time, in seconds, of the average disk transfer.
Physical Disk IO/Sec	The rate of read and write operations on the disk.
System	
Context Switches/Sec	The combined rate at which all processors on the computer are switched from one thread to another. Context switches occur when a running thread voluntarily relinquishes the processor, is preempted by a higher priority ready thread, or switches between user-mode and privileged (kernel) mode to use an Executive or subsystem service. It is the sum of Thread\\Context Switches/sec for all threads running on all processors in the computer and is measured in numbers of switches. There are context switch counters on the System and Thread objects. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
Processor Queue Length	The number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than 10 threads per processor is normally acceptable, dependent of the workload.

NOTE: These definitions are for performance monitoring counters for Windows; the definitions for Linux may vary slightly.

Threshold Values for Performance Monitoring

All performance counters have default warning and critical threshold values. Exceeding these thresholds will generate an alert which will affect device roll-up health. You can view the change in device health in the **Group Health View** (Dell Management Console portal page.)

Table 9-5. Threshold Values for Performance Monitoring

Metric (Total Count (simple+compound))	Unit	Warning Threshold	Critical Threshold	Range
CPU				
%Kernel Utilization Time	%	70	80	0-100
%Processor Utilization Time	%	70	80	0-100
%User Utilization Time	%	70	80	0-100
Logical Disk				
NOTE: These counters are not available on servers running supported Linux operating systems.				
Logical Disk Free Space	%	20	10	0-100
Logical Disk IO/Sec	/Sec	5	10	any
Memory				
% Page File Usage	%	90	95	0-100
Available Memory	MB	50	20	any
Pages IO/Sec	/Sec	15	20	any
Network				
Incoming Bytes/Sec	Bytes/Sec	1250000	1875000	any
Incoming Packets/Sec	Packets/Sec	1250	1875	any

Table 9-5. Threshold Values for Performance Monitoring *(continued)*

Metric (Total Count (simple+compound))	Unit	Warning Threshold	Critical Threshold	Range
Outgoing Bytes/Sec	Bytes/Sec	1250000	1875000	any
Outgoing Packets/Sec	Packets/Sec	1250	1875	any
Physical Disk				
Average Access Time	Sec	1	2	any
Physical Disk IO/Sec	/Sec	5	10	any
System				
Context Switches/Sec	/Sec	100000	200000	any
NOTE: Context switches may vary from server to server. Use your judgment to set these values accordingly.				
Processor Queue Length		4	8	any

Enabling Monitor Policies

1. In the Monitoring and Alerting portal page, on the left hand pane, select **Monitor→ Policies→ Monitor Policies→ Dell Policies** and click on the policy you want to change.
   - Select **Device Agent Health - Dell Remote Access Controller In-Band** to monitor agent health of DRAC installed servers.
   - Select **Device Agent Health - OpenManage Storage Management** to monitor agent health of OpenManage Storage Management devices.
   - Select **Performance Monitoring for Linux** to enable performance monitoring for Linux systems.
   - Select **Performance Monitoring for Windows** to enable performance monitoring for Windows systems.
   - Select **Device Primary Health** to monitor health of a device.
   - Select **Power Monitoring** to enable monitoring power consumption.
2. Click on the **On/Off** drop-down and select **On**.

3 Click **Save changes**.

4 Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update.”

Changing a Poll Setting

1 In the **Monitoring and Alerting** portal page, on the left hand pane, select **Monitor → Policies→ Metric Library**.

2 Select the metric for which you want to change the interval and click the pencil icon to edit it.

3 Enter the time in seconds for the **Polling Interval** and click **OK**.

4 Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update“for more information.

Adding a Task to a Rule

1 In the **Monitoring and Alerting** portal page, on the left hand pane, select **Monitor → Policies→ Rule Library**.

2 Select the rule for which you want to add the task. For example, **Device Primary Health Critical** and click the pencil icon to edit.

3 In the **Actions** section of the edit rule dialog box, under **Tasks**, click the yellow star to add a new task.

4 Select the task you want to add. For example, **Send E-mail**.

5 In the right pane, enter the appropriate details you want to save with the task and click **OK**.

6 Verify the task is displayed under the **Tasks** list as part of this rule.

7 In the **Edit Rule** dialog, click **OK**.

8 Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update“for more information.

Modifying Metrics

You can modify metrics.

To edit metrics:

1. From the Monitoring and Alerting Web portal page, select **Monitor→Policies→Edit Agentless Metrics**.
2. In the **Agentless Metrics**, select the metrics that you want to edit and then click the pencil icon.
3. Make the necessary updates to the polling interval and timeout and then click **OK**.

NOTE: You can select multiple metrics and update polling interval and timeout.

4. Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update.”

To edit metric rules:

1. From the **Monitoring and Alerting** portal page, select **Monitor→Policies→Rule Library**.
2. In the **Agentless Metrics**, select the metrics that you want to edit and then click the pencil icon.
3. Make the necessary updates to the metrics and actions and then click **OK**.
4. Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update.”

To edit Smart Metrics:

1. From the Monitoring and Alerting Web portal page, select **Monitor→Policies→Metric Library**.
2. In the Agentless Metrics, select the metrics that you want to edit and then click the pencil icon.
3. Make the necessary updates to the metric value and smart key value and then click **OK**.
4. Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update.”

Performance Viewer

The Performance Viewer provides a real-time interface for viewing performance counters or other monitored data. You can view this data in real-time by selecting **Actions→ Monitor→ Real-time...** and selecting the device. To view historical data, click **Actions→ Monitor→ Historical...** and select the device.

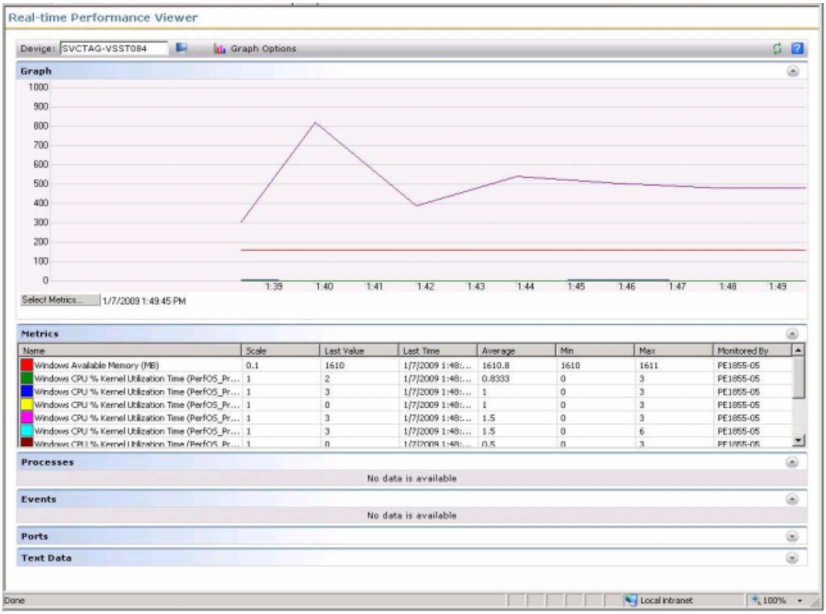
See the Symantec documentation from **Help→ Documentation Library** for more information on launching and viewing this interface.

Dell™ OpenManage™ Server Administrator Notes

- The features available in the Performance Viewer vary from the features available in OpenManage Server Administrator.
- When you launch the Performance viewer graph, for OpenManage Server Administrator metrics with the device primary health status and device connection state; other OpenManage Server Administrator metrics are also launched with value set to 99.

Dell™ OpenMange™ Storage Management Notes

- When a server is connected to a storage and there are two virtual disks already created, and the server is discovered in Dell Management Console. Then, in the Performance Viewer you can see two probes of storage virtual disk component. If another virtual disk is created using OpenManage Server Administrator, then these changes are displayed in Dell Management Console only when you restart the monitor service or re-discover the device.



Name	Scale	Last Value	Last Time	Average	Min	Max	Monitored By
🟥 Windows Available Memory (MB)	0.1	1610	1/7/2009 1:48:...	1610.8	1610	1611	PE1855-05
🟩 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	2	1/7/2009 1:48:...	0.8333	0	3	PE1855-05
🟦 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	3	1/7/2009 1:48:...	1	0	3	PE1855-05
🟨 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	0	1/7/2009 1:48:...	1	0	3	PE1855-05
🟪 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	3	1/7/2009 1:48:...	1.5	0	3	PE1855-05
🟦 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	3	1/7/2009 1:48:...	1.5	0	6	PE1855-05
🟫 Windows CPU % Kernel Utilization Time (PerfOS_Pr...	1	0	1/7/2009 1:48:...	0.5	0	3	PE1855-05

No data is available

No data is available

Health Monitoring

Health monitoring provides a common interface for monitoring the health and connection state of all discovered Dell devices. Health monitoring includes primary device health, agent health, and device connection state. The health of the device is communicated to the Symantec Notification Server® and displayed in a roll-up view on the Dell Management Console Home page. You can also view the device health through a drill-down view on the device's **Resource Manager** portal page.

When you view the device health in the Performance Viewer, numeric values are displayed in the Metrics Web part. Table 9-6 describes these values.

Table 9-6. Description of Last Values

Value	State
0	Normal
10	Undetermined
20	Informational
30	Warning
40	Major
50	Critical
99	Disconnect
1	Powered off

NOTE: In most cases, you cannot distinguish between the *Disconnect* and *Powered off* states, except for devices such as Dell Remote Access Controllers (DRAC) where you can retrieve the device status from an out-of-band interface while the device is powered off.

All health monitoring policies are agentless (they do not require an Altiris Agent installation on the devices) and are enabled by default.

Rules are defined to trigger an alert when any health state change occurs.

Dependencies for Health Monitoring

Table 9-7. Dependencies for Health Monitoring

Dependency	Description
Dell OpenManage Server Administrator	Server Administrator is required to manage the Dell server health. You can also decide to install Storage Management and Dell Remote Access Controller while installing the Server Administrator.
SNMP	SNMP is the only protocol available for monitoring most network devices.

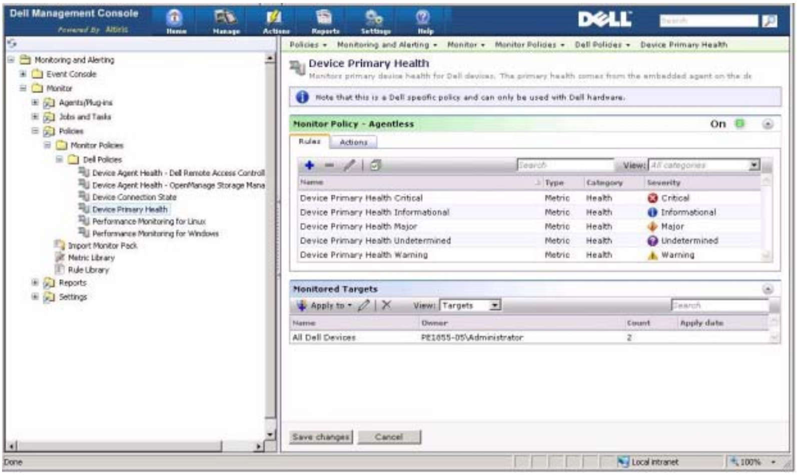
Table 9-7. Dependencies for Health Monitoring *(continued)*

Dependency	Description
Navisphere® CLI (NaviCLI)	NaviCli is required to monitor the health of EMC® devices. For the latest software and user documentation for Navisphere CLI, see powerlink.emc.com.
Symbol	Symbol is required to monitor the health of the Dell PowerVault™ MD 3000 arrays.
WMI, IPMI	These protocols can optionally be used to retrieve server health in addition to SNMP.

Health Policies

Table 9-8. Health Policies

Health Policy	Description
Device Primary Health	Overall health of the device
Device Connection state	Whether the device is connected to the network
Agent Health–Storage Management	Health of the software storage component
Agent Health–DRAC	Health of the remote access controller



Device Primary Health

Monitors primary device health for Dell devices. The primary health comes from the embedded agent on the de

Note that this is a Dell specific policy and can only be used with Dell hardware.

Monitor Policy - Agentless On

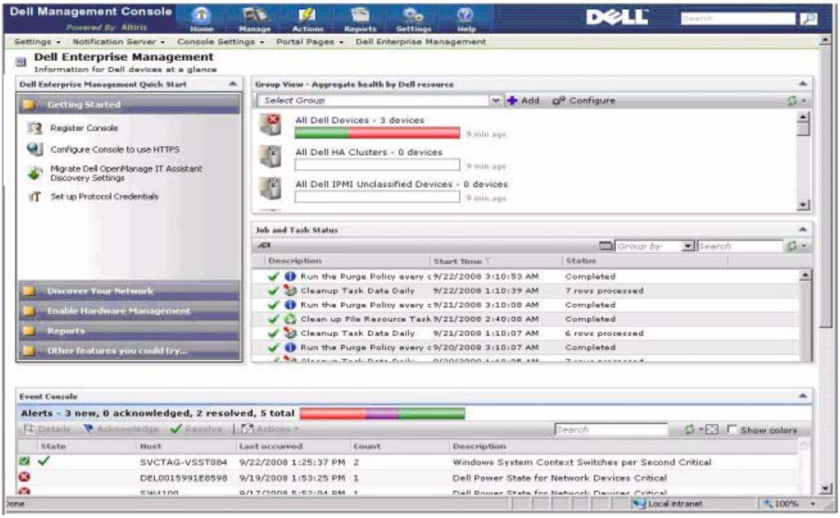
Name	Type	Category	Severity
Device Primary Health Critical	Metric	Health	Critical
Device Primary Health Informational	Metric	Health	Informational
Device Primary Health Major	Metric	Health	Major
Device Primary Health Undetermined	Metric	Health	Undetermined
Device Primary Health Warning	Metric	Health	Warning

Monitored Targets

Name	Owner	Count	Apply date
All Dell Devices	PE1855-05\Administrator	2	

Group View

The **Group View** is the primary interface for viewing device health. Device health is the worst case roll-up of the hardware health and any alert criteria met from performance monitoring.


Dell Management Console
Powered By Altiris
Home
Manage
Actions
Reports
Settings
Help
DELL
Search
Settings ▾
Notification Server ▾
Console Settings ▾
Portal Pages ▾
Dell Enterprise Management
Dell Enterprise Management
Information for Dell devices at a glance
Dell Enterprise Management Quick Start
Getting Started
Register Console
Configure Console to use HTTPS
Migrate Dell OpenManage IT Assistant Discovery Settings
Set up Protocol Credentials
Discover Your Network
Enable Hardware Management
Reports
Other features you could try...
Group View - Aggregate health by Dell resource
Select Group
Add
Configure
All Dell Devices - 3 devices
9 min ago
All Dell HA Clusters - 0 devices
9 min ago
All Dell IPMI Unclassified Devices - 0 devices
9 min ago
Job and Task Status
Group by
Search
Event Console
Details
Acknowledge
Resolve
Actions ▾
Search
□ Show colors
Done
Local intranet
100%

Description	Start Time	Status
✓ Run the Purge Policy every c	9/22/2008 3:10:53 AM	Completed
✓ Cleanup Task Data Daily	9/22/2008 1:10:39 AM	7 rows processed
✓ Run the Purge Policy every c	9/21/2008 3:10:08 AM	Completed
✓ Clean up File Resource Task	9/21/2008 2:40:08 AM	Completed
✓ Cleanup Task Data Daily	9/21/2008 1:10:07 AM	6 rows processed
✓ Run the Purge Policy every c	9/20/2008 3:10:07 AM	Completed

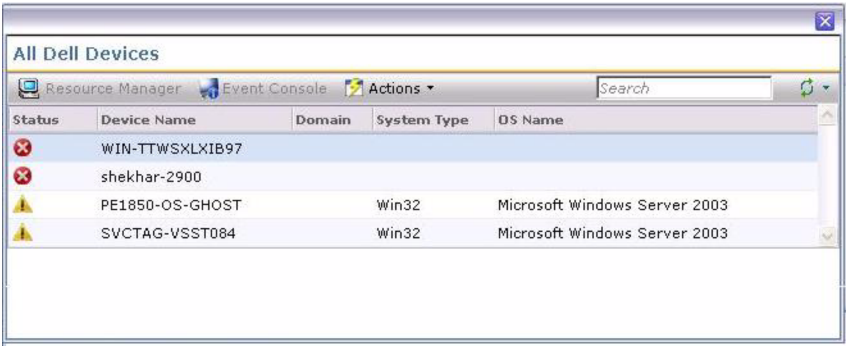
Alerts - 3 new, 0 acknowledged, 2 resolved, 5 total

State	Host	Last occurred	Count	Description
✓	SVCTAG-VSST084	9/22/2008 1:25:37 PM	2	Windows System Context Switches per Second Critical
⊗	DEL0015991E8598	9/19/2008 1:53:25 PM	1	Dell Power State for Network Devices Critical
⊗	SW4100	9/17/2008 5:52:04 PM	1	Dell Power State for Network Devices Critical

This **Group View** is based on the health values collected by the Dell health monitor policies and is updated in real-time every time there is a change in the health state of the device. The refresh control in the top right corner of this Web part allows you to specify the refresh interval. You can also click **Refresh** to update the health status view.

This Web part consists of several pre-defined groups that display the roll-up health in a bar graph view for each device class and additionally displays a summary group that rolls up the health of all Dell devices. You can also add your own custom groups or remove any existing groups from this view.

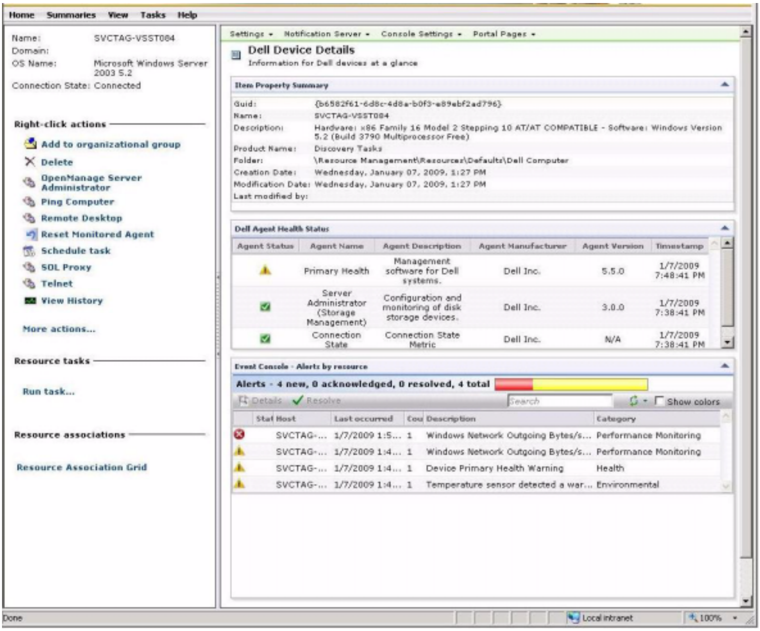
Click on a device group title or a section of a device group bar graph to launch a new window with either the full list of devices or the devices matching that specific state respectively. This window displays the specific contributors to this group's roll-up state with some additional detail.



Status	Device Name	Domain	System Type	OS Name
✖	WIN-TTWSXLXIB97			
✖	shekhar-2900			
⚠	PE1850-OS-GHOST		Win32	Microsoft Windows Server 2003
⚠	SVCTAG-VSST084		Win32	Microsoft Windows Server 2003

Click on a device in the **All Dell Devices** window to view the **Resource Manager**.

Resource Manager View for Health Monitoring



Name: SVCTAG-VSST084
Domain:
OS Name: Microsoft Windows Server 2003 5.2
Connection State: Connected

Dell Device Details
Information for Dell devices at a glance

Item Property Summary

Guid: {b6582f61-6d8c-4d8a-b0f3-e89ebf2ad796}
Name: SVCTAG-VSST084
Description: Hardware: x86 Family 16 Model 2 Stepping 10 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
Product Name: Discovery Tasks
Folder: \Resource Management\Resources\Defaults\Dell Computer
Creation Date: Wednesday, January 07, 2009, 1:27 PM
Modification Date: Wednesday, January 07, 2009, 1:27 PM
Last modified by:

Dell Agent Health Status

Agent Status	Agent Name	Agent Description	Agent Manufacturer	Agent Version	Timestamp
⚠	Primary Health	Management software for Dell systems.	Dell Inc.	5.5.0	1/7/2009 7:48:41 PM
☑	Server Administrator (Storage Management)	Configuration and monitoring of disk storage devices.	Dell Inc.	3.0.0	1/7/2009 7:38:41 PM
☑	Connection State	Connection State Metric	Dell Inc.	N/A	1/7/2009 7:38:41 PM

Event Console - Alerts by resource

Alerts - 4 new, 0 acknowledged, 0 resolved, 4 total

	Stat	Host	Last occurred	Cou	Description	Category
✖		SVCTAG-...	1/7/2009 1:5...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Windows Network Outgoing Bytes/s...	Performance Monitoring
⚠		SVCTAG-...	1/7/2009 1:4...	1	Device Primary Health Warning	Health
⚠		SVCTAG-...	1/7/2009 1:4...	1	Temperature sensor detected a war...	Environmental

The **Resource Manager** provides a detailed view of everything specific to this device that will contribute to its health.

Primary health, agent health, and connection state all combine to make up the overall device health as seen in the **Group Health View**. The breakdown of the health status is visible from the **Resource Manager** or numerically in the **Performance Viewer** (see Table 9-6.)

Agent Health Status Web Part

This Web part displays all monitored health agents and other relevant information.

Connection State Indicator

This indicator in the upper left corner of the **Resource Manager** indicates the connection state of the device, whether connected or disconnected.

Event Console Web Part

The **Event Console** Web part on the **Resource Manager** displays all alerts specific to this device. All alerts received from the monitor solution contribute to the overall health for this device. For more information on Event Console, see the *Online Help*.

Connection State Monitoring

The Connection state is part of health monitoring and affects the device roll-up health. If the connection is lost, the device roll-up health is displayed as critical.

When a device is in **Disconnect** or **Connection lost** state, the Notification Server cannot communicate with the device and this state includes the following:

- Physical power loss
- Network connectivity loss
- Protocol stops responding
- Agent stops responding

When troubleshooting a non-communicating device, consider the preceding possibilities.

Point to Note

- Dell Management Console uses the same protocols to discover and monitor a device. For example, if you use a custom connection profile, which does not include SNMP, the **Resource Manager** and **Performance Viewer** will not display performance metrics and some health metrics, such as:
  - **Device Agent Health – OpenManage Storage Management**
  - **Device Agent Health – Dell Remote Access Controller IB (In Band)**

OnDemand Monitoring

OnDemand monitoring allows the Notification Server to instantly collect a set of metrics when an SNMP alert is received.

This feature is used to poll the device health when an SNMP trap, which may affect health, is received from a device. This enables accurate and efficient update of the device health when the hardware health changes as opposed to waiting for the next poll interval to update the health.

For this feature to work, enter the IP address of the Dell Management Console system in the managed system's SNMP services configuration for SNMP Trap destination.

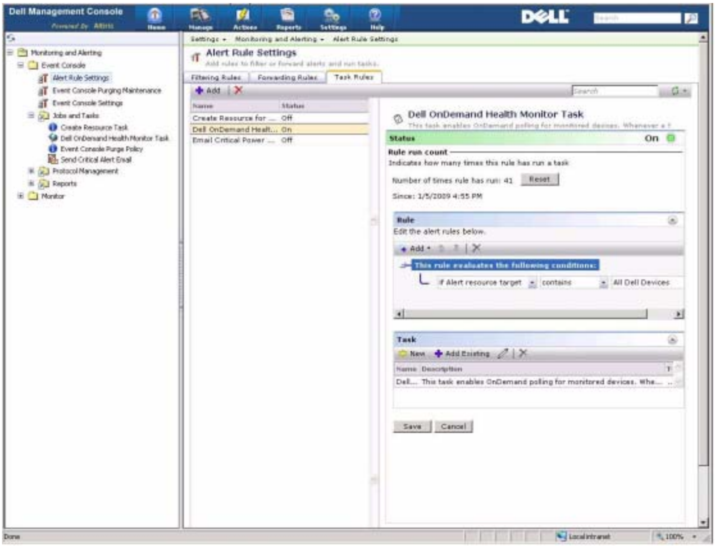
For other types of devices, see the device documentation for configuration procedures to forward traps to the Dell Management Console system.

The OnDemand feature is enabled by default.

NOTE: This feature requires that the device is configured for SNMP management as the feature is dependent on SNMP traps from the device.

You can find the OnDemand task and alert rules in the **Monitoring and Alerting** portal page. The OnDemand alert rule defines the conditions required to trigger the OnDemand task, and controls whether or not this feature is enabled. This rule is displayed on the left pane, under **Monitoring and Alerting→ Event Console→ Alert Rule Settings**. On the right hand pane, in the **Task Rules** tab, select the **Dell OnDemand Health Monitor Task**.

The OnDemand task defines which metrics should be polled when the OnDemand alert rule is triggered. This task is displayed by double-clicking the task within the alert rule or directly through the left pane, under **Monitoring and Alerting→ Event Console→ Jobs and Tasks→ Dell OnDemand Health Monitor Task**.



Alert Rule Settings

Add rules to filter or forward alerts and run tasks.

Name	Status
Create Resource for ...	Off
Dell OnDemand Healt...	On
Email Critical Power ...	Off

Dell OnDemand Health Monitor Task

This task enables OnDemand polling for monitored devices. Whenever a t

Status On

Rule run count

Indicates how many times this rule has run a task

Number of times rule has run: 41

Since: 1/5/2009 4:55 PM

Rule

Edit the alert rules below.

This rule evaluates the following conditions:

If Alert resource target contains All Dell Devices

Task

Name	Description
Del...	This task enables OnDemand polling for monitored devices. Whe...

Forcing an OnDemand Poll for a Specific Device

1 Click **Manage→ All Devices**.

2 On the right hand pane, right-click the device on which you want to force the OnDemand poll and select **Properties**.

3 On the **Properties** page, copy the Guid value.

4 Click **Home→ Monitoring and Alerting**.

5 On the **Monitoring and Alerting** portal page, click **Event Console→ Jobs and Tasks→ Dell OnDemand Health Monitor Task**.

6 On the right hand pane, in the **Task Status** Web part, click **New Schedule**.

7 In the **New Schedule** dialog box, you can schedule to run the poll right away or at a later time.

8 Under the **Monitored Resource** section, paste the Guid value that you copied in step 3.

> **NOTE:** Ensure that the Guid does not contain extra characters including spaces.

9 Click **Schedule**.

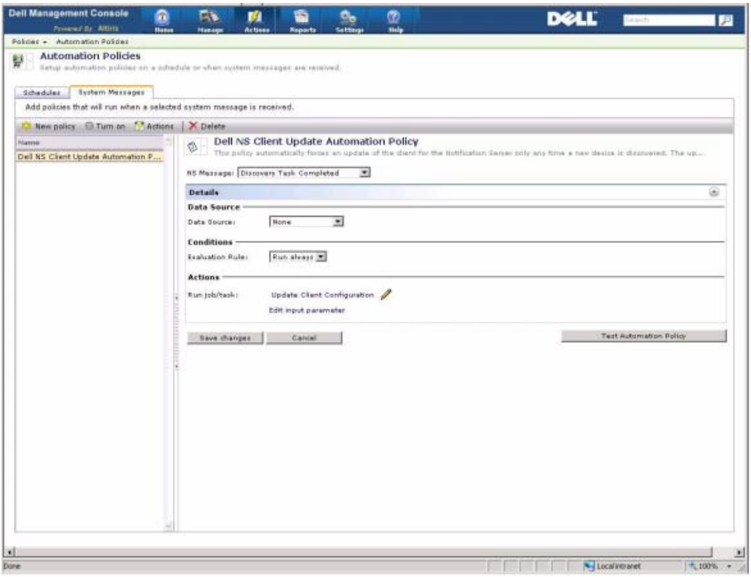
When the task is run, you can view the health updates in the health views.

Client Update Automation Policy

A client policy update is needed any time a new device is discovered or a monitor policy, metric, or rule is updated. This feature causes an automatic update of the client policy every time a new device is discovered, which restarts the monitor agent and will terminate any open connection to that agent. However, this policy causes a brief interruption to the current monitor process while the remote monitoring agent updates. You must still manually force the client update (see “Forcing a Client Policy Update“for more information) or wait for the next polled client update to occur (default every hour) after any policy, rule, or metric change.

NOTE: This feature applies to agentless monitoring only.

You can find the task defining this feature by clicking **Manage→ Automation Policies**. In the **Automation Policies** page, in the **System Messages** tab, select **Dell NS Client Update Automation Policy**.



Automation Policies

Setup automation policies on a schedule or when system messages are received.

Add policies that will run when a selected system message is received.

Dell NS Client Update Automation Policy

This policy automatically forces an update of the client for the Notification Server only any time a new device is discovered. The up...

NS Message: Discovery Task Completed

Details

Data Source

Data Source: None

Conditions

Evaluation Rule: Run always

Actions

Run job/task: Update Client Configuration

Edit input parameter

Forcing a Client Policy Update

A Client Policy update occurs every hour, by default.

1 In the Notification Server, on the Windows toolbar, right-click the **Altiris Agent** icon and select **Altiris Agent Settings**.

2 In the **Altiris Agent** dialog box, first click **Send**, then click **Update**.

3 In the **Configuration** section, verify the **requested** and **changed** times match or that the **changed** time is recent after the update.

   This indicates that the configuration has changed, but the agent still needs to reset for the changes to be observed.

   It may take a few minutes or more (time required increases with the number of devices monitored) for the monitor agent to reset. After the reset, metrics are available in the **Performance Viewer** when that data is retrieved.

   NOTE: All metrics for the same device may not be retrieved at the same time. Also, depending on the Connection Profile you use, the metrics displayed may vary. For more information on Connection Profiles, see “Creating a New Connection Profile“and “Editing the Default Connection Profile."

Cloning a Policy for Monitoring Different Devices with Different Thresholds

This procedure is only necessary if you want to have a policy or subset of a policy evaluating two or more groups of devices to different threshold values at the same time.

Metrics and rules are defined globally. This means that any modification to these values will affect all references of the metric or rule.

To make changes specific to a device or group of devices as well as maintain the original values on another group of devices, clone the metric or rule and then create a new policy to reference the *clone* instead of the original metric or rule.

Cloning a Rule

1. In the **Monitoring and Alerting** portal page, on the left pane, select **Monitor**→ **Policies**→ **Rule Library**.
2. Right-click on the rule you want to change and select the **Clone** icon.

   The rule is cloned.
3. Select the cloned rule.
4. Modify the property you want to change and click **Save**.
5. Repeat steps 1-4 for all rules you want to change.

Cloning the Original Policy

1. In the **Monitoring and Alerting** portal page, on the left pane, select the policy you want to clone.
2. Right-click the policy and select **Clone**.

   The policy is cloned.
3. Select the cloned policy.
4. Select all existing rules in the policy and delete them using the **-** button.
5. Use the + button to add all your new rules to the policy.
6. Enter a new policy name and click the **Apply to** drop down to select a new target for your policy.

   NOTE: Ensure that you select a target that does not overlap the original policy, or this may lead to wasted bandwidth in monitoring the metric on the same device twice.
7. Click the **On/Off** dropdown and select **On**.
8. Click **Save changes**.

Perform a forced client policy update (or wait the default policy update period) for the changes to take affect. See “Forcing a Client Policy Update“for more information.

Managing Server Monitoring Alerts

You can configure Dell Management Console to send e-mail alerts on the status of preselected devices' health to specific users.

You can set up a schedule to send an e-mail. If a device in a pre-defined collection has a health status change that matches the health status monitored by the task, an e-mail is sent to the specified users the next time the task is scheduled to run.

As a prerequisite to create task and send an alert, an SMTP server must be added and configured, see Scheduling Health Monitor E-mail Tasks.

Viewing Health Monitor E-mail Tasks

To view the list of health monitor tasks: From the **Dell Management Console Portal** page, select **Dell Enterprise Management Quick Start**→ **Quick Starts**→ **Health Monitor Email Task**.

Receiving Health Monitor E-mail Alerts

To receive alerts you must configure the SMTP server, create and configure a Health Monitor E-mail Task, and then schedule the Health Monitor E-mail task.

After the Health Monitor E-mail task is completed, a report is displayed and an e-mail is sent to the selected users.

The Health Monitor report lists devices that can be referenced. In the report, you can click on the device to view the resource manager page.

Configuring SMTP Server

To configure an SMTP server:

1. From the **Dell Management Console**, select **Settings**→ **All Settings**→ **Notification Server**→ **Notification Server Settings**.
2. In the **Notification Server Settings** page, on the **E-mail** tab, do the following:
   a. Provide the **SMTP Server Settings** information.
   b. Provide the **Default E-mail Addresses** information.
   c. Click **Send test e-mail** to test the settings.
3. Click **OK**.

Creating Health Monitor E-mail Task

To receive alerts on the servers' health, configure the Health Monitor E-mail task:

From Dell Management console, do any of the following:

- From the **Dell Management Console Portal** page do the following:

  a From the **Dell Enterprise Management Quick Start** Web part, select **Quick Starts→ New Health Monitor Email Task**.

  b In the **E-mail information** Web part, provide the e-mail information you want to send users during an alert. You can modify the alert criteria. To modify alert Criteria see *Dell Management Console Online Help*.

- From the **Jobs and Tasks Portal** page, do the following:

  a In the **Quick Start - Jobs and Tasks** Web part, select **Create a new job or task**.

  b In the **Create New Job or Task** page, select **Server Tasks Health Monitor E-mail Task**.

  c In the **Server Tasks Health Monitor E-mail Task** page, provide e-mail information. You can modify the alert criteria. To modify alert Criteria see *Dell Management Console Online Help*.

Scheduling Health Monitor E-mail Tasks

You can schedule the health monitor e-mail task to run on selected Dell devices. You can also schedule the alert task from the **Jobs and Tasks Portal** page.

To schedule a Health Monitor E-mail Task:

1. From the **Dell Management Console Portal** page, select **Quick Starts→ Health Monitor Email Tasks**.
2. In the **Health Monitor Email Task** page, select the e-mail task.
3. In **Task Status**, click **New Schedule**.
4. To schedule the task click **Now**, to schedule the task for a particular frequency, on a specific date and time select **Schedule**, and then provide the details.

5. When configuring the e-mail criteria for a health monitor e-mail task, If you selected fields for providing input parameters, then the selected fields are available. Provide the recipients' e-mail information in the available fields.
6. Click **Schedule**.
7. Click the completed schedule to view the health monitor reports.
8. In the report, click the devices to view the **Resource Manager** page.

10

Power Monitoring

Power monitoring enables you to monitor a standard set of power consumption counters for Dell servers; however, these servers must support power monitoring.

Power monitoring offers the following features:

- Receive data from metrics gathered by Dell OpenManage.
- View power consumption trends and data for devices in a graphical format.
- Access data over the SNMP and WMI protocols.
- Power Monitoring is supported in the yx0x and yx1x servers, and only the following x9xx servers with OpenManage Server Administrator version 5.3 or later:
    - 1950 MLK111
    - 2950 MLK111

  For more information on the supported servers see the *Support Information Matrix for Dell Management Console Version 1.1*.

  In the server name format yxxx; y denotes alphabets, for example R or T; and x denotes numbers.
- Record single probe readings like amperage per power supply (in A), energy consumption (in KWh), and so on.
- Record aggregate readings like aggregate power.
- View graphs for real-time power consumption data, historical power consumption data, and so on.
- Generate Reports for various power consumption metrics.

Dell™ OpenManage™ Server Administrator Related Notes

- For some rollup status, the OpenManage Server Administrator status may differ from the status displayed in Dell Management Console.

- For Dell Management Console, the rollup health is always a worst case rollup — so any critical status on the device will always turn the global health, that is, group view and the monitor pie chart to critical.

  For example, if one of the power supply is removed from the server. In OpenManage Server Administrator, the overall health status is displayed as warning, power redundancy status is also displayed as warning and the power supply is shown as critical. The correct events (matching with OpenManage Server Administrator status) are displayed as warning even in the Resource Manager. However, Dell Management Console server's health status is displayed as critical (color red) in the **Monitored Resource by Status** pie chart.

Power Monitoring Related Notes

- The Performance viewer currently provides real time power consumption for only one server; however, to view power consumption for multiple servers, you must see the reports.
- You cannot use Power Monitoring when you are managing more than 500 nodes. To manage up to 500 nodes, you must have the following system requirements for the Dell Management Console management station:
  - Supported Operating systems, for example, Microsoft® Windows Server® 2003 R2 SP2 (32-bit) — Standard or Enterprise Edition
  - Physical Processors — Two
  - RAM — 4 GB
  - DVD Drive
  - Microsoft .NET Framework version 3.5 or 3.5 SP1
  - Windows Internet Information Services version 6.0
  - Microsoft SQL Express 2005 or SQL Express 2008, SQL Server 2005 or SQL Server 2008 (64-bit Remote)
  - A remote database and at least 8GB memory available for larger environments.
- When you inventory a device discovered using the WMI protocol, in the hardware Summary page, in the Power supply information table, the Power Supply Type does not contain any value.

Dependencies for Power Monitoring

The following dependencies are present for power monitoring.

Table 10-1. Dependencies for Power Monitoring

Dell Policy	Agent/ Agentless	Support Coverage	Default Behavior	Dependencies
Power Monitoring	Agentless	Dell servers with supported power monitoring enabled	Disabled	SNMP and WMI protocol

Metrics for Power Monitoring

You can monitor the following metrics for power consumption by Dell servers.

NOTE: To view unavailable or initializing metrics, select the **Show unavailable/initializing metrics** check box.The numeric metrics that you selected for monitoring are available under Graph and Metrics and the text metrics that you selected is available under Text Data. Selecting this option will allow you to see other metrics the monitor agent is attempting to collect, but these metrics cannot be selected and viewed on the graph until data has been retrieved.

Table 10-2. Metrics for Power Monitoring

Metric	Description
Agentless Numeric Metrics	
Dell Power - Amperage per Power Supply (Amps)	Select to monitor Amperage Power Supply in Amperes.
Dell Power - Energy Consumption (KWh)	Select to monitor energy consumption in Kilo Watt Hour.
Dell Power - Energy Consumption (BTU/hr)	Select to monitor energy consumption in British Thermal Unit Per Hour.
Dell Power - Energy Consumption (Watts)	Select to monitor energy consumption in Watts.

Table 10-2. Metrics for Power Monitoring

Metric	Description
Dell Power - Instantaneous Headroom (BTU/hr)	Select to monitor the available instantaneous headroom in British Thermal Unit Per Hour.
Dell Power - Instantaneous Headroom (Watts)	Select to monitor the available instantaneous headroom in Watts.
Dell Power - Power Consumption (BTU/hr)	Select to monitor power consumption in British Thermal Unit Per Hour.
Dell Power - Power Consumption (Watts)	Select to monitor power consumption in Watts.
Agentless Text Metrics	
Dell Power - Energy Consumption Start Time	Select to view text data for energy consumption start time.

Threshold Values for Power Monitoring

Power consumption is very specific to the hardware being used. A critical consumption on one system may be well within the bounds on another system. For convenience, rules have been defined to trigger alerting on the power metrics, but due to this tight coupling to the hardware, you must define proper thresholds specific to the hardware being monitored in order to see any of these rules trigger as the default settings are set well above any real hardware values.

Managing Power Monitoring

To work with power consumption monitoring, enable the power monitoring policy, see “Enabling Monitor Policies.”

After you have confirmed that the power monitoring is activated, you can monitor power consumption for a device using the available power consumption metrics. You can do any of the following:

- View real time data, see “Managing Power Monitoring Metrics.”
- View historical data, click **Actions→ Monitor→ Historical** and select the device.

- View reports for various power consumption metrics, see the “Reporting“chapter.

You can modify rules and actions for the power consumption monitoring metrics, see “Modifying Metrics.”

Managing Power Monitoring Metrics

You can monitor power consumption of devices by selecting the required metrics from a list of agentless numeric and text metrics. You can modify the rules and actions defined for the various metrics.

To view power consumption for devices:

1 Do any of the following:

   - From Dell Management Console, select **Actions** → **Monitor** → **Real-time**.
   - From the **Monitoring and Alerting** portal page, in **Launch Performance Viewer**, click on the device icon to select the device, and then click **Launch**.
   - From the **Monitoring and Alerting** portal page, in **Monitored Resources by Status**, select the device and then click **Performance Viewer**.

   The Real-time Performance Viewer page along with the **Registered Metrics** page is displayed.

2 In the **Registered Metrics** page, select the required metrics and then click **OK**. For more information see, “Metrics for Power Monitoring.”

Group Metrics

This feature will be available in later versions of Dell Management Console. The group metric provides an interface that allows efficient data collection, collecting data efficiently enables faster calculation for the report when compared with the same group viewed in the Smart metric report. This interface also allows for creating thresholds at the group level. All group metrics will calculate sum of the specified group's values. The group metric can only have one target at any time and this target must be the same or contained within the policy target, both of which default to the group **All Devices with Power monitoring support** that is automatically determined at discovery time.

Table 10-3. Group Metrics

Metrics	Description
Dell Power - Group Energy Consumption (KWh)	Enables you to monitor energy consumption for a group.
Dell Power - Group Instantaneous Headroom (BTU/hr)	Enables you to monitor the instantaneous headroom available for a group in British Thermal Units per hour.
Dell Power - Group Instantaneous Headroom (W)	Enables you to monitor the instantaneous headroom available for a group in Watts.
Dell Power - Group Power Consumption (BTU/hr)	Enables you to monitor the power consumed by the group in British Thermal Units per hour.
Dell Power - Group Power Consumption (W)	Enables you to monitor the power consumed by the group in Watts.

Viewing Group Metric Reports

Group metric data is not visible in the real-time or historical viewer. This data is only visible from the group metric report.

To view group metrics: From Dell Management Console, select **Reports**→ **All Reports**→ **Group Metric Report**.

Managing Group Metrics

The predefined group metrics are all part of the power monitoring policy. These metrics are the same as the smart metrics and are modified in the same way with one key difference - they allow for specifying the target for the group metric. Similarly the rules used to monitor group metrics can be modified in the same way as the rules for smart metrics. See section Managing Power Monitoring for more information on monitoring metrics and rules.

11

Dell Patch Management Solution

The Dell Patch Management solution enables you to scan your operating environment to determine if the supported Dell™ PowerEdge™ systems meet the minimum patch requirements for accepting the Dell Update Packages (DUPs) for BIOS, drivers, and firmware; the solution also automates the download and distribution of DUPs.

Dell Management Console supports patch updates for servers with Lifecycle Controller. For more information on the minimum supported Lifecycle Controller, and *Integrated Dell Remote Access Controller* (iDRAC) firmware required for patch updates, see the *Support Information Matrix for Dell Management Console*.

The Symantec Management Agent, formerly Altiris Agent, is not required to perform patch server update on servers with Lifecycle Controller.

The Lifecycle Controller enabled patch server update allows you to gather information on the existing versions of BIOS, firmware, or both, Application Dell Update Packages (APAC DUPs) such as operating system driver pack, 32-bit diagnostics, and Unified Server Configurator (USC), and apply the latest updates to various hardware components in Dell servers. You can also schedule and deploy the required updates.

For systems that require updates, use the *Dell Server Updates* DVD or download the appropriate DUPs from the Dell Support website at **ftp.dell.com**.

Dell Patch Management Related Notes

- For a server selected as a Windows target during Stage and Distribute (With Default Connection profile), a Rollout job will fail if you selected the priority as Apply Updates using Lifecycle Controller. To resolve; For LifeCycle Controller based *updates*, use Lifecycle controller based targets.
- For a server selected as a Lifecycle Controller enabled target during Stage and Distribute (With appropriate connection profile), a Rollout job will fail if you selected the priority as Apply Updates using Altiris Agent. To resolve; For Altiris Agent based updates, use Windows targets in stage and distribute wizard.

- You must re-stage a bundle after upgrade. Whenever you upgrade to Dell Management Console version 1.1, the staged bundles are deleted. To get the staged bundles, you must run the staging task again.

  To run the staging task:

  1. From Dell Management Console, select **Manage→ Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Server→ Download Software Update Package**.

  2. Select the staging task used for staging of bundles before upgrade, right click the staging task and select **Start now**. The re-staging task of the bundles starts.

- For a server to support both Altiris Agent and Lifecycle Controller enabled patch updates simultaneously. Discover the server and the iDRAC of the server using a connection profile that includes SNMP or WMI, and WS-MAN protocol. OpenManage Server Administrator must be installed on the server before you discover the server.

  After you discover the server, complete the prerequisites for Altiris Agent and Lifecyle Controller enabled patch.

About the Dell Patch Management Solution

The Dell Patch Management solution provides the following:

- Support for individual and system update sets updates.

  For convenience and efficiency, it is recommended that you create bundle rollout jobs. Bundle rollout jobs distribute entire software update sets, or bundles, as opposed to a single DUP.

- Support for rollback updates on servers with Lifecycle Controller. You can only rollback to the previous update.
- Support for the Dell PowerEdge™ systems running supported Microsoft® Windows® and Linux operating systems.
- Support for the Dell PowerEdge systems with Lifecycle Controller enabled patch updates independent of an operating system.
- Support for the single server jobs for discovering a Dell system and updating the Dell server to a level required to receive updates.

Prerequisites for Altiris Agent Enabled Patch Management

You must complete the following prerequisites:

- Install Altiris Agent on the managed systems.
- Import DUP catalog from **ftp.dell.com** or the latest version of the Dell™ Server Update Utility.
- Download inventory collector.
- Run compliance assessment as shown in the Getting Started Web part configuration section.

Prerequisites for Lifecycle Controller Enabled Patch Management

The applicable DUPs are limited to BIOS, firmware updates, and Application Dell Update Packages (APAC DUPs) as supported by Lifecycle Controller. The APAC DUPs includes OS driver pack, 32-bit diagnostics, and Unified Server Configurator (USC).

You must complete the following prerequisites:

- The supported servers must contain the required firmware version of iDRAC6 Enterprise and USC. For more information, see the Support Information Matrix for Dell Management Console. If you upgraded to the current version of iDRAC, then you must re-discover iDRAC.

  NOTE: iDRAC6 must be configured and auto discovery is not supported in Dell Management Console.

- Configure the WS-MAN protocol in the connection profile.
- The iDRAC 6 of the Lifecycle Controller enabled server must be registered to the DNS server. Network communication to the Dell Management Console server and iDRAC6 should be possible using their hostnames. For example, you must be able to ping the Dell Management Console server and the iDRAC6 using their respective hostnames.
- Discover the iDRAC 6 Enterprise using the WS-MAN connection profile and the discovered device must be classified as a Dell server.
- Gather the discovered device's information using Agentless Inventory.

- Download DUP catalog.
- Run compliance assessment for Lifecycle Controller enabled servers.

Patch Management Solution User Interface

To access the Patch Management solution user interface (UI): select **Home→ Patch Management for Dell Servers Home**.

Getting Started with Patch Management

The **Getting Started Web** part has links to common configuration and patch management process items:

Configuration

- **Configure Proxy** (Click to view the **Notification Server Settings** page.)
- **Download Updates Catalog** (Click to view the **DUP Catalog Import** page.)
- **Download Inventory Collector** (Click to view the **Dell Inventory Collector Import** page.)

  NOTE: The **Dell Inventory Collector Import** page is required only for an Altiris Agent enabled patch update.
- **Solution Global Settings** (Click to view the **Dell Vendor Configuration** page.)
- **Install Altiris Agent** (Click to view the **Altiris Agent Install** page.)

  NOTE: The **Altiris Agent Install** page is required only for an Altiris Agent enabled patch update.

Patch Process

- **Run compliance check on**
  - **Windows Servers** (Click to view the **Determine Windows Patchable Dell Servers Job** page.)
  - **Linux Servers** (Click to view the **Determine Linux Patchable Dell Servers Job** page.)
  - **Lifecycle Controller Enabled Servers** (Click to view the **Compliance Assessment Task for Lifecycle Controller enabled Servers** page; Required for the Lifecycle Controller enabled patch.)

- **Check applicable updates by computers** (Click to view the **Hardware Update Compliance report** page.)
- **Manage Updates** (Click to view the **Manage Dell Hardware Updates** page.)

The **Identify Supported Servers Web** part displays a report that contains the following information:

- The **Identify servers that support automated updating** section contains these reports:
  - **Computers scanned**: This report is generated when a compliance check is done. The report provides a link to the **Computers Evaluated for Dell Automated Patching Support** page that lists servers (with Lifecycle Controller or Symantec Management Agent) discovered by Dell Management Console. The list contains servers that support the updates.
  - **Supported servers**: This report is generated when a compliance check is done. The report provides a link to the **Computers Evaluated for Dell Automated Patching Support** page that contains a list of servers that support Altiris Agent, Lifecycle Controller enabled patch updates, or both.
- The **Schedule or begin an identification scan** section enables you to discover Dell systems with supported operating systems, server models, and the Altiris Agent. If an Altiris Agent is not installed on the managed systems, you can complete the task by clicking **Install Altiris Agent**.

The **Inventory Supported Servers** Web part displays a report that contains a list of Dell systems on which the inventory is successfully performed. The listed Dell systems are either ready to receive the updates, do not meet prerequisites, or fail to return inventory. To schedule or begin an inventory scan:

- Click **Windows Compliance Assessment Task to** determine the patch updates supported Windows operating system installed Dell Servers.
- Click **Linux Compliance Assessment Task** to determine patch updates supported Linux operating system installed Dell Servers.
- Click **Compliance Assessment Task for Lifecycle Controller enabled Servers** task to determine patch updates supported Lifecycle Controller enabled Dell servers.

The **Review update compliance of servers that are ready to receive updates** Web part displays the compliance of supported Dell systems and distributes updates. The pie chart lists servers that are up-to-date, missing one or more recommended updates, One or more optional update, and missing one or more urgent updates. Click sections of the pie chart to distribute applicable updates.

The **Review Status of update tasks** Web part, for Altiris Agent and Lifecycle Controller enabled patch updates, displays the status of the Rollout jobs for individual or bundle updates for Altiris Agent enabled patching and it displays the status of the Rollout jobs for Lifecycle Controller enabled servers.

DUPs and System Bundles

A Dell Update Package (DUP) is designed to update system components, such as the BIOS, drivers, and firmware of a Dell system. A collection of DUPs is released in a *bundle* as a Dell System Update Set.

In the Patch Management solution interface, System Update Sets are referred to as *Bundles*. It is recommended that you distribute system update sets to your Dell systems instead of distributing individual DUPs. DUPs are used to create DUP rollout jobs, and system update sets are used to create bundle rollout jobs.

The Symantec Management Agent must be installed to update system components using Altiris Agent enabled patch updates. The agent is not required for Lifecycle Controller enabled updates; however, Lifecycle Controller must be available to complete the system component updates.

To perform a bundle update, Altiris Agent enabled patch is preferred as Lifecycle Controller enabled patch will not support all the updates that are supported by Altiris Agent enabled patch management.

NOTE: By Default, Dell Management Console assigns priority to the Altiris Agent enabled patch over the Lifecycle Controller enabled patch update.

To update a server using an Altiris Agent, do the following:

1. Create and configure a connection profile.
2. Discover a Dell system that requires an Altiris Agent enabled patch update.
3. Configure network connections or internet settings with **Configure Proxy**.

4 Import DUP catalog with **DUP Catalog Import**.

   If you upgraded to this release of Dell Management Console then you must re-import DUP catalog.

5 Download the **Dell Inventory Collector Tool** from the URL provided in the **Download Inventory Collector**.

6 Configure vendor information with **Solution Global Settings**. You can download DUPs from **ftp.dell.com** or the Server Update Utility.

7 Install agent with **Altiris Agent Installation**.

8 Perform Windows, Linux, or both compliance with Compliance Check. The system inventory information is collected during the compliance check.

9 View data using Reports and initiate the Altiris Agent enabled patch update from the **Hardware Update Compliance** reports or perform Altiris Agent enabled patch updates with **Manage Updates**. To view reports, click **Check applicable updates by computers**.

To update a server using Lifecycle Controller for rolling out updates or bundles, do the following:

1 Create and configure a connection profile using the WS-MAN protocol.

2 Discover a Dell system that requires a Lifecycle Controller enabled patch update. (Discover iDRAC 6 Enterprise using the WS-MAN connection profile, the discovered device must be classified as a Dell computer; Gather the discovered device’s information using Agentless Inventory.)

3 Configure network connections or internet settings with **Configure Proxy**.

4 Import DUP catalog with **DUP Catalog Import**.

5 Collect the system inventory information by running Agentless Inventory against these systems.

6 Run the Lifecycle Controller enabled servers’ compliance assessment task.

7 View data using Reports and initiate Lifecycle Controller enabled patch update from the **Hardware Update Compliance** reports or perform Lifecycle Controller enabled patch updates with **Manage Updates**. To view reports, click **Check applicable updates by computers**.

To use the Rollback for a server updated using Lifecycle Controller, do the following:

1 To view reports, do any of the following:

- Select **Reports**→ **All Reports**→ **Software**→ **Patch Management for Dell Servers**→ **Hardware Update Compliance**.
- In the **Patch Management for Dell Servers Home** portal page, in the **Getting Started** Web part, click **Check applicable updates by computers**.

2 View data in the **Available Updates for Rollback** report.

3 Perform a Lifecycle Controller enabled patch rollback using Stage and Distribute wizard.

DUP Catalog Import

Use the **DUP Catalog Import** page to get the Dell software management packages available for download.

Run the compliance assessment for an Altiris Agent or Lifecycle Controller enabled patch update to determine the DUPs applicable for the managed systems.

Based on the assessment, applicable DUPs are downloaded to the Dell Management Console only when you select a stage or stage and distribute action. Downloading the catalog is imperative to get the latest recommended DUPs.

The DUP Catalog Import task allows you to automate the catalog download; To ensure that you have the latest DUPs released by Dell, specify a schedule to run this task.

Downloading Dell Update Catalog

You can download the required software management resources for populating the **Manage Dell Hardware Updates** page with the DUP Catalog Import task.

To download the Dell Update Catalog:

1 In the **Home** menu, click **Patch Management for Dell Servers Home**.

2 From the **Getting Started** Web part, under **Configuration**, click **Download Updates Catalog**.

3 In the right pane, select one of the following:

- **Dell site**
- **Local storage** (if you have the DUPs stored locally)
- **Only if modified** is selected by default to ensure that only updated files are downloaded, thus avoiding unnecessary downloads.

4 Click **Save changes**.

5 Click **New Schedule** to specify a schedule for the task. In the **Schedule Task** dialog box, specify a schedule to run the task, or, run the task immediately by selecting **Now**.

Dell Inventory Collector Tool

The Dell Inventory Collector tool enables you to gather information on current operating system and hardware firmware. The Dell Inventory Collector task is required only for Altiris Agent enabled patch updates.

This tool determines if your Dell systems can receive updates. Dell provides separate tools for Dell servers with Windows and Linux operating systems. The tools are updated every three months and you can download these tools from a public Symantec download portal as **.cab** files. However, The Dell Inventory Collector task downloads each tool automatically.

To download Dell Inventory Collector:

1 From the **Home** menu, click **Patch Management for Dell Servers Home**.

2 From the **Getting Started** Web part, under **Configuration**, click **Download Inventory Collector**.

3 In the right pane, select one of the following:

- **Web URL: To** download the Dell Inventory Tool from **solutionsam.com/imports/7_0/Patch/Dell/dellinvtool_windows.cab** or **solutionsam.com/imports/7_0/Patch/Dell/dellinvtool_linux.cab**.
- **Local storage** (If the **.cab** files are locally available.)

4 Click **Save changes**.

5 Click **New Schedule** to specify a schedule for the task. In the **Schedule Task** dialog box, specify a schedule to run the task, or, run the task immediately by selecting **Now**.

Dell Vendor Configuration Page

In the DUPs Update Preference Settings option, priority is given to the Altiris Agent enabled patch updates over the Lifecycle Controller enabled patch updates.

1. In the **Home** menu, click **Patch Management for Dell Servers Home**.
2. From the **Getting Started** Web part, under **Configuration**, click **Solution Global Settings**.
3. In the right pane, make changes on the **Dell Vendor Configuration** page.
4. Click **Apply**.

Configure this page to set up the DUP distribution method; some of these settings are used as default values in the **Rollout Job** wizard. All new DUPs that are downloaded have these settings by default. If you change the settings, the existing software update tasks and packages are not updated with these defaults. You can force them to update by re-creating packages from the **Manage Software Updates** page.

Options on the General tab

Option	Description
DUPs Download Verification	Ensures that all DUPs are Dell certified. This option is selected by default.
DUPs Download Location	The Dell FTP site is selected by default so that DUPs are downloaded directly from this website. Click **Local storage** if you want to download DUPs from another location and specify the location in the field.
DUPs Update Preference Settings	By default, the preference is set to **Apply updates using Altiris Agent**. To set Lifecycle Controller as preference, select **Apply updates using Lifecycle Controller**. **NOTE:** When you can update a server using both Altiris agent and Lifecycle Controller, the update is performed based on the preference setting.
DUPs Distribution Options	Specify the target servers to receive distributed DUPs for the Windows operating system, Linux operating system, or Lifecycle Controller.

Options on the Advanced tab

Option	Description
Package Defaults	Enables you to determine how often to delete software update packages.
Package distribution	**Allow Package Server distribution** — Selected by default to ensure that a package server processes all software update packages. For more information, see the Symantec Management Platform documentation. **Use alternate download location on Package Server** — Enables you to specify a different location to download packages to a package server, and then specify the locations for Dell systems running Windows and Linux operating systems. **Use alternate download location on client** — Enables you to specify a different location to download packages on a client system, and then specify the locations for systems running Windows and Linux operating systems.

Options on the Programs tab

Option	Description
Program Defaults	**Run with rights** — Specify whether the program is run with the **System Account**, **Logged in User**, or **Specified User** account. If you select **Specified User** — Specify the user domain in the field. This option is applicable only on systems running Windows. **Program can run** — Specify the conditions in which the program can run. The options are **Only when a user is logged on**, **Whether or not a user is logged on**, and **Only when no user is logged on**. This option is applicable only on systems running Windows. **Minimum connection speed** — **Use Agent settings** is selected by default; however, you can specify a different speed. **Terminate after** — Specify a time after which to terminate software update tasks.
Agent Events	Choose to send relevant events from the managed system to the Dell Management Console system.

Downloading Dell Update Packages

You can download DUPs from the **ftp.dell.com** or from the Server Update Utility. The DUPs download location can be configured in the Dell Vendor Configuration Page.

Discovering Patch Updates Supported Linux Dell Servers

You can discover all supported Dell systems running Linux operating system that are ready to receive DUPs.

To discover patch updates supported Dell systems running Linux operating system:

1. From the **Home** menu, click **Patch Management for Dell Servers Home**.
2. From the **Getting Started** Web part, under **Run compliance check on**, click **Linux Servers**.
3. In the **Determine Linux Patchable Dell Servers Job** page, click **Quick Run and** select the server to run the job immediately, or click **Schedule** to specify a schedule for the job to run periodically.

Discovering Patch Updates Supported Windows Dell Servers

You can discover Dell systems running Windows operating system that are ready to receive DUPs.

To discover patch updates supported Dell systems running Windows operating system:

1. From the **Home** menu, click **Patch Management for Dell Servers Home**.
2. From the **Getting Started** Web part, under **Run compliance check on**, click **Windows Servers**.
3. In the **Determine Windows Patchable Dell Servers Job** page, click **Quick Run and** select the server to run the job immediately, or click **Schedule** to specify a schedule for the job to run periodically.

Discovering Patch Updates Supported Lifecycle Controller Enabled Dell Servers

You can discover Dell servers that support the Lifecycle Controller enabled patch updates.

To discover patch updates supported Dell servers installed with Lifecycle Controller:

1. From the **Home** menu, click **Patch Management for Dell Servers Home**.
2. From Dell Management Console, using the device discovery wizard, discover a Dell server.
3. On the discovered server that contains Lifecycle Controller, run inventory using the Agentless inventory wizard.
4. From the **Getting Started** Web part, under **Run compliance check on**, click **Lifecycle Controller Enabled Servers**.
5. In the **Compliance Assessment Task for Lifecycle Controller enabled Servers** page, select the server or servers to run the Lifecycle Controller enabled patch and click **New Schedule** to specify a schedule for the job to run periodically. By default, all Dell servers with Lifecycle Controller are selected for this task.

Accessing Dell Patch Management Reports

You can view and manage your Altiris Agent and Lifecycle Controller enabled Patch Management data through reports.

To access Dell Patch Management reports:

1. On the **Reports** menu, click **All Reports**.
2. In the left pane, click **Reports→ Software→ Patch Management for Dell Servers**.
3. Select the folder with the reports you require.

   For example, **Dell Server Patching Inventory** reports, **Hardware Update Compliance** reports, and **Update Installation Results** reports.

Compliance Assessment Task

Compliance assessment task for Lifecycle controller enabled servers compares the available updates from the update catalog to the currently installed updates on the server and determines the applicable updates for various components in the target server. This task relies on the information gathered during inventory and the information present in the updates catalog. As a result, running inventory task against the target server and downloading catalogs are the prerequisites for the compliance assessment task.

The compliance assessment task can be scheduled by clicking the link on the **Getting started** Web part and selecting the schedule and target server information. After the compliance assessment task is successful, users can look at various hardware compliance reports which display the installed version and available version of updates for various components in the server.

Manage Dell Hardware Updates

The **Manage Dell Hardware Updates** page enables you to view and stage all system update sets. You can download the DUP catalog file (**.cab**) from **ftp.dell.com** or the *Dell Server Updates* DVD in the DUP Catalog Import task. When you stage a system update set, associated DUPs are downloaded to the Dell Management Console system. After all DUPs for the system update set are downloaded, the DUPs are ready to be distributed in the bundle rollout jobs. The **Manage Dell Hardware Updates** page lets you create a Stage and Distribute task. See “Stage and Distribute Wizard.”

Options Available on the Manage Dell Hardware Updates Page

Option	Description
Manage Bundles **Manage Updates**	Enables you to choose to distribute bundles of DUPs (Manage Bundles), or individual DUPs (Manage Updates).
Filter by	Enables you to filter by system model or name.
OS Type	Enables you to filter by Windows, Linux, or all operating system types.
Group	Enables you to search in an organizational group.
Updates	Enables you to view all updates by default, or view applicable updates only.

Options Available on the Manage Dell Hardware Updates Page

Option	Description
Severity	Enables you to choose a severity level to filter updates.
Stage and Distribute All Bundles	Enables you to stage and distribute all listed bundles.
Stage and Distribute Selected Bundles	Enables you to stage and distribute only selected bundles.
Manage Selected Bundle	Opens a bundle and then creates a rollout job for a single DUP.
Bundle Name	The name of the system update set or bundle.
Release Date	The date the bundle was released.
Severity	The severity level of the bundle. For example, **Urgent**.
Calendar	Enables you to specify beginning (From) and end (To) dates to display the bundles released between the specified dates.
# of Computers	The number of affected Dell systems.
# Updates	The number of DUPs in a bundle.
# Downloaded	The number of DUPs already downloaded for the relevant bundle.

Staging and Distributing DUPs

You can stage and distribute bundles from the **Manage Dell Hardware Updates** page, where all available bundles are listed. When you *stage* a bundle, all associated DUPs are downloaded from the Dell website at **ftp.dell.com** to the Dell Management Console system and selecting *distribute* enables you to deploy and update the bundles to the selected systems. You can also download DUPs from a local storage (for example, the *Dell Server Updates* DVD).

You can filter DUPs by Dell system types, operating systems, severity, and group.

To stage and distribute all displayed DUPs:

1 From the **Home** menu, click **Patch Management for Dell Servers Home**.

2 From the **Getting Started** Web part, click **Manage Updates**.

3. In the right pane, select the devices you want to apply the update to and do any of the following:
   - Select **Stage and Distribute All Updates** — All the applicable bundles for all the servers are staged and the individual DUPs, based on the servers' requirements, are pushed and installed on the server.
   - Select **Stage and Distribute Selected Updates** — Only the selected bundles are staged and the individual DUPs, based on the servers' requirements, are pushed and installed on the server.
   - Select **Manage Selected Updates** — Only the DUPs you selected from the bundles are staged and the selected DUPs are pushed and installed on the server.

Stage and Distribute Wizard

The **Stage and Distribute** wizard creates rollout jobs. Rollout jobs distribute Dell Update Packages (DUPs) to managed systems. This wizard automatically filters targets to install only DUPs on applicable systems.

Select the server to be updated under one target only in case of Windows servers that support both Altiris Agent and Lifecycle Controller enabled patching. For example, To apply DUPs or a bundle using Altiris Agent enabled patch updates for a Windows server, then the server needs to be added to the Windows target only.

Update options are based on the target selected:

- The **Windows Targets** option is available when a Windows DUP or bundle is selected from the report.
- The **Linux Targets** option is available when a Linux DUP or bundle is selected from the report.
- The **Lifecycle Controller Enabled Targets** option is available when a Windows DUP or bundle, or both; or a Rollback update is selected from the report.

Options on the Stage and Distribute Wizard

Option	Description
Reboot Options	**Reboot immediately** — Select to restart immediately after installing DUPs. For Lifecycle Controller enabled servers, if the Reboot immediately option is not enabled, the server will update only when you restart the server. **Do not Reboot** — Select if you do not want to restart after installing DUPs.
Installation Options	**Silent** — Select to perform a silent installation. **Silent, allow downgrade** — Select to install a superseded DUP.
Choose Connection Profile for Lifecycle Controller enabled Servers	**Connection profile** — Select to choose and edit an existing profile. **New** — Select to create a new connection profile. This is required for Lifecycle Controller based updates only. The selected WS-MAN connection profile can be different from the one that is used for discovery of the server to be updated. The WS-MAN connection profile used for patch must have Administrator privileges on the iDRAC of the target server to perform a Lifecycle Controller based patch.
Schedule	**Now** — Select to immediately install DUPs. **Schedule** — Select to schedule the DUPs installation.
Windows Targets	Select to choose a target to apply the rollout job. Only applicable computers in a target receive DUPs from the rollout job.
Lifecycle Controller Enabled Targets	Select to choose a target to apply the rollout job. Only applicable target receive DUPs from the rollout job.
Linux Targets	Select to choose a target to apply the rollout job. Only applicable computers in a target receive DUPs from the rollout job.
Distribute Bundles List	A list of DUP bundles distributed by the rollout job.
Create	Finishes the wizard and creates a Stage and Distribute job.

Rollout Jobs

Rollout jobs consists of a sequence of tasks that enable you to distribute Dell Update Packages to managed systems.

You can view the following rollout jobs:

- DUP Rollout Jobs

  DUP Rollout Jobs contain a single DUP and are stored in the **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Rollout Jobs→ DUPs** folder.

- Bundle Rollout Jobs

  Bundle rollout jobs contain all the DUPs in a system update set and are stored in the **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Rollout Jobs→ Bundles** folder.

Rollout Jobs only update server components to newer versions. A rollout job with an older update than the one that is currently installed on the target server fails. You have the option to force a downgrade.

Creating a Rollout Job

Rollout jobs are created to install updates on managed systems.

To create a DUP Rollout Job:

1. Click **Manage→ Software**.
2. In the left pane, click **Software→ Manage Dell Hardware Updates**.
3. In the right pane, select a bundle.
4. Click **Manage Selected Updates**.

   All DUPs in the selected bundle are displayed.

5. Right-click the updates you want to distribute, and click **Stage and Distribute Selected Updates**.

   NOTE: When you select multiple DUPs, a single rollout job is created when updates are performed using Lifecycle Controller.

6. After creating DUP Rollout Jobs, navigate to the folder **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Rollout Jobs→ DUPs** to view the status of DUP Rollout Jobs.

To create a bundle rollout job:

1. Click **Manage→ Software**.
2. In the left pane, click **Software→ Manage Dell Hardware Updates**.
3. In the right pane, select a bundle in the table.
4. Click **Stage and Distribute Selected Updates**.
5. The stage and distribute task is displayed in the **Stage and Distribute** job in the folder **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Server**. The job is read only and used for viewing the progress of the rollout job. After the stage and distribute task is completed, the rollout job is created.
6. After creating bundle rollout jobs, navigate to the folder **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Rollout Jobs→ Bundles** to view the status of bundle rollout jobs.

Viewing Status of Rollout Jobs

The **Stage and Distribute Updates** job processes the DUPs and creates a Rollout Job for individual DUPs or bundle updates.

To view status of rollout jobs:

1. In Dell Management Console, do any of the following:

- Click **Manage→ Jobs and Tasks**.
- Click **Patch Management for Dell Servers Home**. The rollout job status is displayed in the **Review status of update tasks** Web part.

To view rollout jobs: select **Jobs and Tasks→ System Jobs and Tasks→ Software→ Patch Management for Dell Servers→ Rollout Jobs→ DUPs/Bundles**.

Lifecycle Controller Enabled Rollout Job

A Lifecycle controller enabled rollout job is an Altiris Jobs infrastructure based job that consists of all the Lifecycle controller enabled patch tasks. You can run a single rollout job to apply many updates.

For example, if *n* number of updates are applied, then the rollout job contains the following:

- *n* number of Lifecycle controller enabled Send Update tasks
- One Lifecycle controller enabled Execute Update task

- *n* number of Lifecycle controller enabled Poll Status tasks

A Lifecycle controller enabled rollout job is created when you choose one or more DUPs to be applied to a managed system, through one of the **Hardware Update Compliance** reports. Within the job, each task has a specific function. The **Send Update** task causes the DUP to be downloaded from the Dell Management Console to the Lifecycle controller on the target. The **Execute Update** task initiates the Lifecycle controller to begin application of the particular DUP. The **Poll status** task checks on the DUP application status - whether the DUP application is completed successfully or not. After the update, a status message is displayed.

Rollback Report

The Rollback report lists previously installed version of BIOS or firmware updates available on the Lifecycle controller enabled servers. Only BIOS and firmware can be rolled back.

You cannot rollback the following:

- Universal Server Configurator (USC)
- Dell Diagnostics applications
- Drivers for operating system (OS) installations

Viewing Rollback Report

1 To view reports, do any of the following:
   - Select **Reports→ All Reports→ Software→ Patch Management for Dell Servers→ Hardware Update Compliance**.
   - In the **Patch Management for Dell Servers Home** portal page, in the **Getting Started** Web part, click **Check applicable updates by computers**.
2 View data in the **Available Updates for Rollback** report.

In the Rollback Report you can do the following:

- To Rollback to a previously installed version of BIOS or firmware: Select the rollback update that you want to apply to the system and click **Rollback Selected Updates**.
- To apply all the rollback updates: click **Rollback All Updates**.

- To compare the version of the rollback update with the version currently installed on the system, compare the versions in the **Installed Version** and **Available Version** fields.
    - Server — Displays the server name for which the rollback update is applicable.
    - Device — Displays the device name on the server for which the rollback update is applicable.
    - Type — Displays the component type (BIOS or Firmware).

Troubleshooting Patch Management Solution

To assist in troubleshooting, error codes are generated in reports and execution instance details.

Dell Update Package exit codes

After running Update Packages, exit codes are generated. They appear in the **Dell Update Execution Details** report. The exit codes help you determine and analyze the execution results after you run Update Packages.

Table 11-1. DUP Exit Codes

Value	Message	Description
0	SUCCESSFUL	The update was successful.
1	UNSUCCESSFUL	An error has occurred during the update process; the update was unsuccessful.
2	REBOOT REQUIRED	Restart the system to apply updates.
3	DEP_SOFT_ERROR	Possible explanations are as follows: • You attempted to update to the same version of the software. • You tried to downgrade to a previous version of the software.
4	DEP_HARD_ERROR	The required prerequisite software was not found on the system.

Table 11-1. DUP Exit Codes

Value	Message	Description
5	QUAL_HARD_ERROR	The Update Package is not applicable. Possible explanations are as follows: • The Update Package does not support the operating system. • The Update Package is not compatible with the devices found in your system
6	REBOOTING_SYSTEM	Restarting system

Windows Dell Servers Discovery Task Failed Error Codes

These error codes appear when the Windows Dell Servers Discovery Task fails. The codes can be found in the task's execution instance details.

Table 11-2. Windows Dell Server Discovery Task Failed Error Codes

Value	Message	Description
10	Err_OK_IsDellServer	Successfully executed – system is a Dell server.
11	Err_OK_IsNotDellServer	Successfully executed – system is not a Dell server.
12	Err_OK_IsNotSupported DellServer	Successfully executed – system is a Dell computer but is not a supported Dell server or does not have a supported operating system.
-20	Err_EndofScript	Err_EndofScript Not used at the moment.
-21	Err_FileNotFound	Server list file (DellServers.ini) was not found.
-22	Err_FailedStringSearch	Not used at the moment.
-24	Err_InvalidCmdArgument	Command-line arguments wrong. Must be blank, “/model” or “/omsa”.
-25	Err_CantAccessWMI	Could not execute WMIquery. Either not installed or not running.

Linux Dell Servers Discovery Task Failed Error Codes

These error codes appear when the Linux Dell Servers Discovery Task fails. The codes can be found in the task's execution instance details.

Table 11-3. Linux Dell Server Discovery Task Failed Error Codes

Value	Message	Description
7	RPM_VERIFY_FAILED	RPM verification has failed.
10	Err_OK_IsDellServer	Successfully executed – system is a Dell server.
11	Err_OK_IsNotDellServer	Successfully executed – system is not a Dell server.
12	Err_OK_IsNotSupported DellServer	Successfully executed – system is a Dell computer but is not a supported Dell server or does not have a supported operating system.
21	Err_FileNotFound	Failure. Server list file (DellServers.ini) was not found. File name is not as specified in SupportedDellServers.txt.
24	Err_InvalidCmdArgument	Failure. Command-line arguments are wrong.
25	Err_CantAccessDMI	Could not execute DMIquery.

12

Reporting

The Reports module of Dell™ Management Console enables you to view pre-defined reports and create custom reports against data collected on the various devices discovered and monitored by Dell Management Console.

The pre-defined reports are device specific and can be saved in the CSV (spread sheet), XML, and HTML formats.

Use the Reports module to view reports. Reports process the collected information and display the following information:

- Tasks that have run and the tasks that have succeeded or failed.
- Assets owned, where it is, and who has it.

NOTE: The data that is available in reports is not real time data and there is a time lag present.

Reports Related Notes

- Power budget and power profile information are not supported for the following platforms:
  - R805 (Dell OpenManage 5.5, OpenManage 6.1, or OpenManage 6.2)
  - R905 (OpenManage 6.1 or OpenManage 6.2)

  Therefore, power budget and power profile information is not available in the inventory (SNMP discovery) and in the power budget report.

About the Reporting Module

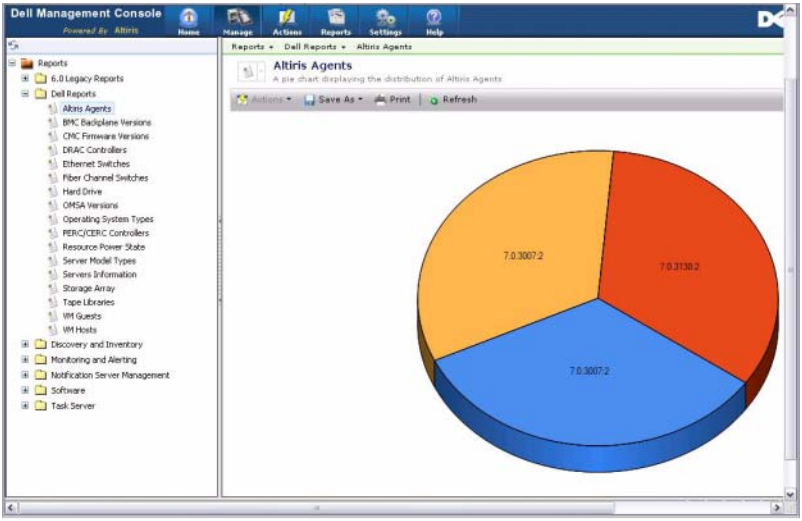
Use the Reports module to view inventory, monitoring, and performance details associated with a device.

You can run a variety of reports that are already available in the Dell Management Console Report Packs. You can also create custom reports using a simple wizard-based flow. The custom reports can be very simple or include SQL-like queries for more complex reports. For more information, see the Symantec™ User's Guide.

The Reporting User Interface

To access the **Reports** portal page: select **Reports**→ **All Reports**.

Knowing Your Reports User Interface



A pie chart displaying the distribution of Altiris Agents

The left pane displays the **Reports** tree. From this tree, you can access the pre-defined Dell Reports.

Click **Dell Reports**. The pre-defined dell reports and their description are displayed on the right pane.

For each pre-defined Dell report, the right pane displays graphical representation of the selected report. From the right pane, you can do the following:

- View the displayed report in another format, for example XML.
- Export the displayed report.
- Save the displayed report, specifically as a Web part. See “Saving a Report.”
- Print the displayed report.

Click any part of the pie-chart to get more information about the report.

NOTE: If you have newly discovered a system, the Resource Connection State report does not display the connection state data immediately.

Creating a New SQL Report

If you do not find a report that suits your needs, you can create a new report and present data in a way you want.

For example, if you want a report on the operating systems present on the servers on your network.

1. On the left pane, on the **Reports** tree, right-click **Reports** and select **New→ Report→ SQL Report**.
2. On the New SQL Report page, in the Data Source tab, enter:

   ```
   select [OS Name] from DiscoveredMachines
   ```
3. Click **Apply**.

   The report displays the operating systems on each discovered system.

Creating a New Dell Computer Report

To create a new Dell computer report:

1. On the **Reports** portal page, right-click **Reports** and select **New→ Report→ Computer Report**.
2. In the **Data Source** tab, Query sub-tab, select the **Base Query** and choose **Dell Computer** from the **Base Resource Type** drop-down menu.

   NOTE: You can also create other Dell reports from this drop-down.
3. In the **Fields** sub-tab, click **Add** to include the attributes. See “Attributes for Inventory”for all Dell attributes.

   NOTE: All Dell attributes are prefixed with **Dell Computer** or **Dell Management Console**.
4. Click **Save changes**.

   A tabular report is displayed with all the attributes you selected.

   For advanced reports, see the Symantec documentation available under **Help→ Document Library**.

Editing a Dell Report

All Dell reports are read only by default. However, to edit these report, first clone these reports.

Running a Report

On the left pane select a report. The report is displayed on the right hand pane.

Some reports will allow you to enter parameters. These report parameters enable you to filter the report based on the values you choose or enter.

NOTE: The "%" sign is a wildcard and matches any string of zero or more characters.

Saving a Report

You can save a report in multiple formats. For example, as an HTML file, XML file, CSV, or a Web part.

If you want to save the above report as a Web part:

1 On the **New SQL Report** page, from the **Save As** drop-down menu, select **Web part**.

2 On the **Save As Web part** dialog box, enter a Name for the new report.

3 Select the size of Web part and click **Save**.

The report is saved under the **Web Parts** folder in the **Settings→ Console Settings Web Parts** menu.

To add this Web part to the Dell Management Portal page, see “Modifying the Dell Management Console Portal Page.”

Viewing Reports

To view reports:

1 From Dell Management Console, select **Reports→ All Reports→ Dell Reports**.

2 Click the report you want to view.

Metrics Reports

These reports are available for monitoring metrics for device groups.

- Peak Power — Provides information on the peak power consumption values for devices, contains other details like time, unit, and so on.
- Power Budget — Provides information on the power budget, headroom, idle power, and so on for devices.

  The Peak Power and Power Budget reports are displayed in a tabular format.
- Smart Metric Report — This feature will be available in later versions of Dell Management Console. Provides information on the trends of the metric values of devices over time, by selecting the duration, devices, and metric you can view the details in a graphical format. By clicking on a point on the graph, you can drill-down to a table to see the values for each device. This graph is derived from Smart metric data. When you are using the Dell Management Console to manage a large number of devices, the group metric report will provide much quicker response for group data, and should be used to view groups where possible. Alternatively, the scheduling option can be used for a report to run the report overnight so that the data is readily accessible in the morning.

  The Smart Metric report supports only these metrics: Power Monitoring and Performance Monitor.

  The Smart Metric report supports Performance Monitor metrics for the WMI connection profile for servers with Windows operating systems, and SNMP connection profile for servers with Linux operating systems.

  However, the Smart Metric report does not support Health metrics.
- Group Metric Report — This feature will be available in later versions of Dell Management Console. Provides information on the trends of the metric values of groups over time, by selecting the duration and group metric you can view the details in a graphical format. By clicking on a point on the graph, this allows drilling down to a table to see the values for each device which made up this point. This graph is derived from Group metric data.

Viewing Group Metric Reports

To view group metric report graph for a custom group, do the following:

1. From Dell Management Console, select **Manage**→ **Organizational Views and Groups**.
2. In the **Organizational Views** page, create a New Organization View.
3. Create a group under newly created organizational view (For example, group-report).
4. Add servers under this newly created group.
5. Enable the Power Monitoring policies.
6. In Power Monitoring policies, Under **Monitored Targets,** click **Apply to**→ **Resources**.
7. In the add resource wizard, add a rule, in the **Then** criteria drop-down lists, select **exclude resources not in**, **Group**, and then the group report created in step 3.
8. Click **Update results** and click **Save as**, Provide a name (for example: GM) and then click **OK**.

   NOTE: If you do not save the rule settings then the graph is not displayed.

9. From the **Monitoring and Alerting** page, select **Metric Library**.
10. For the group metrics present in the **Metric Library** select **Target as**, click **Apply to**→ **Quick apply** and select the group (GM).

A

Virtualization

Dell™ Management Console can discover virtualization servers. It also supports hardware inventory and health monitoring for the host servers.

Dell Management Console displays the physical hosts and the virtual machines under the **Servers** node in the **All Devices** tree.

Create a new group to display the *virtual machine to host* association in the **All Devices** tree.

Each virtual machine is displayed under this node and when you select a host, all virtual machines running on that server are displayed on the right pane.

You can view the Hardware Inventory in the **Resource Manager** under **Summary**→ **Hardware Summary**.

Supported Virtualization Operating Systems

- Classic ESX
- Embedded ESX
- HyperV

Supported Features for Virtualization Servers

- Discovery
- Host-Virtual Machine association
- Hardware Inventory

Discovery

Guest and host machines are discovered separately over the network.

NOTE: If you add a virtual machine after discovering the virtual server, Dell Management Console does not correlate the guest with the host. To resolve this issue, rediscover the virtual server.

Classic ESX

Dell Management Console discovers the host device by using the VMware® SNMP agent.

The prerequisites to discover the host are:

- Enabling SNMP service on the server
- Enabling SNMP in the connection profile that is used in the Discovery task.

HyperV

Dell Management Console discovers the host device by using a WMI provider.

The prerequisites to discover the host are:

- Enabling WMI service on the server
- Enabling WMI in the connection profile that is used in the Discovery task.

Embedded ESX

Dell Management Console discovers the host device by using the CIM providers provided by VMware.

The prerequisites to discover the host are:

- Enabling WSMAN service on the server.
- Enabling WSMAN in the connection profile that is used in the Discovery task.

Host-Virtual Machine Association

- Virtual host server is identified based on the hypervisor operating system running on these host servers.
- Virtual host servers are shown in the **All Devices** tree under the **Virtual Host** node.
- Virtual machines running on the server are discovered independently over the network.
- The association between the host and virtual machines running on the host are created post discovery using the MAC address, IP address, and UUID of the virtual machines.

- Virtual machines associated to a host are shown on the right pane when you click the host server in the left pane.

Inventory

Classic ESX

The hardware inventory is shown using Dell OpenManage™ Server Administrator SNMP agent.

Prerequisites for inventorying the Classic ESX servers are as follows:

- Server Administrator is installed on the server
- SNMP service is enabled on the server
- SNMP is enabled in the connection profile that is used in the inventory task.

HyperV

The hardware inventory is shown using Server Administrator SNMP or WMI agent.

Prerequisites for inventorying the HyperV servers are:

- Server Administrator is installed on the server
- SNMP or WMI service is enabled on the server
- SNMP or WMI or both are enabled in the connection profile that is used in the inventory task.

Embedded ESX

The hardware inventory is shown using the CIM providers provided by VMware. The information will be gathered using the WSMAN protocol.

Prerequisites for inventorying the Embedded ESX servers are:

- WSMAN service is enabled on the server.
- WSMAN is enabled in the connection profile that is used in the inventory task.

ESXi Configuration

Enabling CIM OEM Providers

To receive the health information (reported in the Dell Management Console monitor) from the ESXi server, enable the CimOemProvidersEnabled configuration setting (set to value 1), and restart the Management Agents for the first time after the ESXi installation.

To enable CIM OEM providers:

1. Download and install the RCLI tools from the VMware website at vmware.com/go/remotecli/).
2. Run the following VmWare RCLI command from a remote Windows or Linux server:

   ```
   vicfg-advcfg.pl --server <ip_address> --username <user_name> --
   password <password> --set 1 Misc.CimOemProvidersEnabled
   ```

3. Restart the Management Agents from the ESXi server Direct Console User Interface (DCUI) menu or reboot the server.

   NOTE: You can also set the CimOemProvidersEnabled property using VI Client (**Configuration**→ **Software**→ **Advanced Settings**→ **Misc**→ **Enable OEM Providers**).

Dell Management Console Configuration

Secure Deployment Mode - Connecting to WSMAN over HTTPS

The following configurations are required in Dell Management Console to connect to WS-MAN running in secure mode on the ESXi servers:

1. A WS-MAN credential set is created using Credential Manager.

   Only one set of credentials is required if all of the ESXi servers have the same username and password settings.

2. A connection profile with the WS-MAN protocol is enabled and the following settings are applied:

   a The credential set is created as described in step 1.

   b The Secure mode is selected.

c The Secure port text box has the port number defined for the HTTPS service on the ESXi server. By default, this value is 443.

d The SSL certificate file is pointing to the SSL certificate (self-signed) downloaded from the ESXi server. Refer to the section procedure to import multiple SSL Certificates in to Dell Management Console Connection Profile.

NOTE: You can use the same Connection Profile to discover multiple ESXi servers if the self-signed certificates (installed by default) from multiple ESXi servers are combined into a single certificate that is imported into the Connection Profile and the credentials are the same across all the ESXi servers.

NOTE: With the ESXi servers using the same credentials, you can use a single connection profile to discover multiple ESXi servers by enabling the Trusted Site option in the Connection Profile and an ESXi certificate import into the Connection Profile is not required.

If all the ESXi servers have certificates generated by the same CA, importing the certificate for the CA, instead of individual certificates, into Dell Management Console Connection Profile is sufficient.

Procedure to Import Multiple SSL Certificates into Dell Management Console Connection Profile

Dell Management Console enables you to import an SSL certificate when configuring WS-MAN (in secure mode) as part of the Connection Profile.

When there is a need to discover multiple devices using WS-MAN over https, you can import into Dell Management Console Connection Profile a single file that contains self-signed certificates (installed by default) from the different servers.

You can create multi-certificate file using the SSL certificates retrieved from multiple ESXi servers. Then import the multi-certificate file into the Connection Profile to enable discovery of multiple ESXi servers using a single Connection Profile (assumption: credentials are same across all the ESXi servers).

The following procedure explains self-signed certificates (installed by default); although this is valid for CA signed certificates also. If all the ESXi servers have certificates generated by the same CA, importing the certificate for the CA into Dell Management Console Connection Profile is sufficient, and you can skip the following procedure.

Step 1: Installing Remote CLI tools from VMware

Download and Install VMware Infrastructure Remote CLI on a Windows computer.

1 Download Infrastructure Remote CLI tools from VMware website: **vmware.com/go/remotecli/**.

  Search for link to Download in section VMware Infrastructure Remote CLI on the page.

2 Install the tools at the default location (for example, **C:\Program Files\VMware\VMware VI Remote CLI**). Later steps assume the default install path. If you change the install path, make changes accordingly in the following steps.

3 Run following command in a command window:

  Set path=%path%;"C:\Program Files\VMware\VMware VI Remote CLI\Perl\bin"

Step 2: Creating the Multi-Certificate file

1 Create the **combinecerts.bat** DOS batch file.

2 Run the combinecerts.bat file:

  combinecerts <userName> <password> <servers ip list file> <output certificate file> [create|append]

  userName: user name with which to login to the ESXi server

  password: password for user

  servers ip list file: ASCII file with one IP Address on each line (see sample file in document)

  output certificate file:name of file that will contain all the certificates

  create|append:

  create: causes the script to create a new output certificate file

  append: causes the script to append new certificates to the output certificate file. The default is `append`, when this parameter is not specified.

  Use this batch file to import a single certificate from an ESXi server by specifying only one IP address in servers IP list file and with create option.

Combinecerts.bat DOS Batch file

Copy the following text into a file named combinecerts.bat.

```
------ START OF DOS Batch File -----
@echo off
rem Usage: combinecerts <user> <password> <servers ip list file> <output certificate file> [create|append]
rem       (assuming same user and password for all servers)
rem   option "create" causes the script to create a new <output certificate file>.
rem   option "append" causes the script to append new certificates to the <output certificate file>.
if "%5"=="create" (del /F /Q %4 2>NUL)
for /f  %%X in (%3) do (
       echo.
       echo.
 echo Importing certificate from server: %%X
       vifs.pl --server %%X --username %1 --password %2 --get /host/ssl_cert tmpcert.crt
       if not errorlevel 1 (type tmpcert.crt >> %4)
       del /F /Q tmpcert.crt 2>NUL
   )
echo.
------ END OF DOS Batch File -----
```

Sample Servers IP list file Copy

```
------ START OF SAMPLE servers IP list file -----
192.168.22.243
192.168.11.45
192.168.22.31
192.168.22.65
```

------ END OF SAMPLE ”servers IP list file” -----

Points to Note

- To delete a virtual machine displayed in the **All Devices** tree; first delete the devices under the group and then delete the group. Remove the group from the discovery range too; other wise, the group will still be displayed after every discovery cycle.
- If you add a guest to a virtual machine after the virtual machine is discovered, the guest is not associated with the host. To associate the guest with the host, rediscover the host.

B

Dell Management Console Security

Built-in Security Features

Dell Management Console provides these ports.

Ports

Table B-1 lists the ports used by Dell Management Console, standard operating system services, and other agent applications.

Correctly configured ports are necessary to allow Dell Management Console to connect to a remote device through firewalls.

The version of the systems management software mentioned in Table B-1 indicate the minimum version of the product required to use that port.

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSH	TCP	1.x	128-bit	None	SSH client Remote software updates to Server Administrator—for systems supporting Linux operating systems Performance monitoring in Linux systems	Yes

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
23	Telnet	TCP	1.x	None	In/Out	Telnet to Linux device	No
25	SMTP	TCP	1.x	None	In/Out	Optional e-mail alert action from Dell Management Console	No
67,68, 69, 4011	PXE	UDP				PXE and DHCP	
68	UDP	UDP	1.x	None	In/Out	Wake-on-LAN	Yes
53, 80, 135, 137, 139, 150, 1433, 2500		TCP				Altiris Console: Console using a remote computer	
80	HTTP	TCP	1.x	None	In/Out	Application launch—PowerConnect™ Console	No
ICMP						Ping	

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
135, 137, 139, 445		TCP/UDP				Non-HTTP communications (for example, client package download using UNC)	
135	RPC/DCOM	TCP/UDP	1.x	None	In/Out	WMI/CIM management queries	No
138		UDP				NS client installation	
161	SNMP	UDP	1.x	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.x	None	In/Out	SNMP Event Reception and Trap Forwarding	No
389	LDAP	TCP	1.x	128-bit	In/Out	Domain authentication for IT Assistant log on	
401-402		TCP/UDP			In/Out	Deployment Solution	
443	Proprietary/Altiris Agent, WSMAN	TCP	1.x	None	In/Out	EMC Storage discovery and inventory, Altiris Agent once installed	No

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
445		UDP				Non-HTTP communications (for example, client package download using UNC)	
623	RMCP	UDP	1.x	None	In/Out	IPMI, WS-MAN, and ASF management	Yes
664	RMCP	UDP			In/Out	Secure ASF management	Yes
1010	PXE	TCP				Deployment Solution: PXE configuration to talk with PXE configuration Service	
1011		TCP				Monitor Solution	
2070 - 2073, 1758 - 1759	PXE	UDP				Deployment Solution: PXE for TFPT and MTFTP transfer of PXE image	
3389	RDP	TCP	1.x	128-bit SSL	In/Out	Application launch—Remote desktop to Windows terminal services	Yes

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
3829, 4949, 4950, 4951		TCP				Used by Altiris Deployment Solutions and PCT Real Time to communicate between PCTWiz and RTDestAgent and to search for RTDestAgent	
4952		TCP				Deployment Solutions communication used for managing the connection drops	
6389	Proprietary	TCP	1.x	None	In/Out	Enables communication between a host system (through NaviCLI/NaviSecCLI or Navisphere Host Agent) and a Navisphere Array Agent on a Storage system.	No
8080						Deployment Solutions Web Console	
16992					Out	AMT management unsecure	No

Table B-1. Dell Management Console Ports

Port	Protocol	Port Type	Dell Management Console Version	Maximum Encryption Level	Direction	Usage	Configurable
16993					Out	AMT management secure	No
16994					Out	AMT management redirection service unsecure	No
16995					Out	AMT management redirection service secure	No
50120-50124						Task Server	
52028, 52029		TCP				NS Client Multicast	
1024-65535	DCOM	TCP/UDP	Unknown	None	In/Out	WMI query management (Random port)	OS - msdn.microsoft.com/enus/library/ms809327.aspx

C

Attributes for Inventory

This section displays the attributes used by Dell Management Console to create a report.

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports

Component	Attribute
Agent	AgentDescription
	AgentGlobalStatus
	AgentId
	AgentManufacturer
	AgentName
	AgentURL
	AgentVersion
Contact	ContactInformation
	ContactLocation
	ContactName
Device	DeviceAssetTag
	DeviceChassisServiceTag
	DeviceDescription
	DeviceLocation
	DeviceLocationInChassis
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemId
	DeviceSystemModelType

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
Firmware	FirmwareChassisIndex
	FirmwareIndex
	FirmwareName
	FirmwareReleaseDate
	FirmwareType
	FirmwareVersion
Network	NICIPAddress
	NICMACAddress
	NICDescription
	NICManufacturer
	NICNetmask
	NICPingable
	NICTOECapable
	NICTOEEnable
BIOS	BIOSChassisIndex
	BIOSReleaseDate
	BIOSVersion
	BIOSName
	BIOSType
	BIOSIndex
Operating System	OSTotalPhysicalMemory
	OSType
	OSRevision
	OSMajorVersion
	OSMinorVersion
	OSArchitecture

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
	OSVendor OSSPMajorVersion OSSPMinorVersion
Memory	MemoryDeviceSize MemoryDeviceFormFactor MemoryDeviceManufacturerName MemoryDeviceSerialNumberName MemoryDeviceAssetTagName MemoryDeviceStatus MemoryDeviceType MemoryDevicePartNumberName MemoryDeviceFailureMode MemoryDeviceBankName MemoryDeviceIndex MemoryDeviceLocationName
PowerSupply	PowerSupplyLocation PowerSupplyType PowerSupplyOutputWatts PowerSupplyStatus PowerSupplyState PowerSupplyRedundancyState PowerSupplyChassisIndex PowerSupplyIndex

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
Processor	ProcessorBrandName
	ProcessorFamily
	ProcessorSteppingName
	ProcessorCores
	ProcessorMaxSpeed
	ProcessorSlotNumber
	ProcessorStatus
	ProcessorCurrentSpeed
	ProcessorModelName
	ProcessorChassisIndex
FRU	FruIndex
	FruStatus
	FruState
	FruDeviceName
	FruManufacturer
	FruSerialNumber
	FruPartNumber
	FruRevision
	FruManufacturingDate
DeviceCard	DeviceCardAdapterSpeed
	DeviceCardManufacturer
	DeviceCardDescription
	DeviceCardSlotNumber
	DeviceCardDataBusWidth
	DeviceCardBusSpeed
	DeviceCardSlotLength

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
ArrayDisk	ArrayDiskNumber
	ArrayDiskName
	ArrayDiskVendorName
	ArrayDiskState
	ArrayDiskStatus
	ArrayDiskModelNumber
	ArrayDiskSerialNumber
	ArrayDiskRevision
	ArrayDiskEnclosureId
	ArrayDiskChannel
	ArrayDiskLength
	ArrayDiskFreeSpace
	ArrayDiskUsedSpace
	ArrayDiskBusType
	ArrayDiskSpareState
	ArrayDiskTargetId
	ArrayDiskLUNId
	ArrayDiskPartNumber
Controller	ControllerNumber
	ControllerName
	ControllerVendor
	ControllerType
	ControllerState
	ControllerStatus
	ControllerFWVersion
	ControllerCacheSize
	ControllerPhysicalDeviceCount

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
	ControllerLogicalDeviceCount
	ControllerPartnerStatus
	ControllerMemorySize
	ControllerDriveChannelCount
	ControllerChargeCount
	ControllerDriverVersion
	ControllerPatrolReadState
Enclosure	EnclosureNumber
	EnclosureName
	EnclosureVendor
	EnclosureState
	EnclosureStatus
	EnclosureId
	EnclosureServiceTag
	EnclosureAssetTag
	EnclosureAssetName
	EnclosureProductId
	EnclosureType
	EnclosureChannelNumber
	EnclosureBackplanePartNum
	EnclosureSCSIId
	EnclosurePartNumber
	EnclosureSerialNumber
EMM	EMMNumber
	EMMName
	EMMRevision
	EMMVendor

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
	EMMState
	EMMPartNumber
	EMMFWVersion
	EMMStatus
Virtual Disk	VirtualDiskNumber
	VirtualDiskName
	VirtualDiskDeviceName
	VirtualDiskState
	VirtualDiskStatus
	VirtualDiskLength
	VirtualDiskWritePolicy
	VirtualDiskReadPolicy
	VirtualDiskCachePolicy
	VirtualDiskLayout
	VirtualDiskStripeSize
	VirtualDiskTargetId
Ownership	PurchaseCost
	WayBillNumber
	InstallationDate
	PurchaseOrderNumber
	PurchaseDate
	SigningAuthorityName
	OriginalMachineConfigurationExpensed
	OriginalMachineConfigurationVendorNmae
	CostCenterInformationVendorName
	UserInformationUserName
	ExtendedWarrantyStartDate

Table C-1. Inventory Attributes of Servers and MD1000 Storage for Reports *(continued)*

Component	Attribute
	ExtendedWarrantyEndDate
	ExtendedWarrantyCost
	ExtendedWarrantyProviderName
	OwnershipCode
	CoroporateOwnerName
	HazardousWasteCodeName
	DeploymentDurationUnitType
	TrainingName
	OutsourcingProblemDescription
	OutsourcingServiceFee
	OutsourcingSigningAuthority
	OutsourcingProviderFee
	OutsourcingProviderServiceLevel
	InsuranceCompanyName
	BoxAssetTagName
	BoxSystemName
	BoxCPUSerialNumberName
	DepreciationDuration
	DepreciationDurationUnitType
	DepreciationPercentage
	DepreciationMethod
	RegistrationisRegistered

Table C-2. Inventory Attributes of EMC and MD3000 Storage for Reports

Component	Attribute
ArrayDisk	ArrayDiskNumber
	ArrayDiskName
	ArrayDiskLength
	ArrayDiskBusType
	ArrayDiskLUNId
	ArrayDiskPartNumber
	ArrayDiskUserCapacity
	ArrayDiskVendorName
	ArrayDiskState
	ArrayDiskModelNumber
	ArrayDiskSerialNumber
	ArrayDiskRevision
	ArrayDiskChannel
	ArrayDiskEnclosureId
Controller	ControllerNumber
	ControllerName
	ControllerMemorySize
	ControllerDriveChannelCount
	ControllerChargeCount
	ControllerSPAReadCacheSize
	ControllerSPAWriteCacheSize
	ControllerSPBReadCacheSize
	ControllerSPBWriteCacheSize
	ControllerCachePageSize
	ControllerVendor
	ControllerSPAReadCachePolicy

Table C-2. Inventory Attributes of EMC and MD3000 Storage for Reports *(continued)*

Component	Attribute
	ControllerSPAWriteCachePolicy
	ControllerSPBReadCachePolicy
	ControllerSPBWriteCachePolicy
	ControllerFWVersion
	ControllerCacheSize
	ControllerPhysicalDeviceCount
	ControllerLogicalDeviceCount
	ControllerType
	ControllerNumberOfPorts
Enclosure	EnclosureNumber
	EnclosureName
	EnclosureType
	EnclosurePartNumber
	EnclosureSerialNumber
	EnclosureVendor
	EnclosureLocationOfManufacture
	EnclosureServiceTag
	EnclosureProductId
	EnclosureNumberOfFanPacks
	EnclosureNumberOfControllers
	EnclosureNumberOfDisks
	EnclosureId
	EnclosureAssetTag
StorageGroup	StorageGroupIndex
	StorageGroupLUNId
	StorageGroupName
	StorageGroupHostName

Table C-2. Inventory Attributes of EMC and MD3000 Storage for Reports *(continued)*

Component	Attribute
VirtualDisk	VirtualDiskNumber
	VirtualDiskName
	VirtualDiskStripeSize
	VirtualDiskTargetId
	VirtualDiskStripeElementSize
	VirtualDiskLUNId
	VirtualDiskDeviceName
	VirtualDiskLength
	VirtualDiskWritePolicy
	VirtualDiskReadPolicy
	VirtualDiskLayout
SoftwareAgent	SoftwareType
	SoftwareVersion
	SoftwareDescription

Table C-3. Inventory Attibutes of Tape Libraries for Reports

Component	Attribute
Contact	ContactInformation
	ContactLocation
	ContactName
Device	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName

Table C-3. Inventory Attibutes of Tape Libraries for Reports *(continued)*

Component	Attribute
	DeviceSerialNumber DeviceServiceTag DeviceSystemModelType
Firmware	FirmwareName FirmwareVersion
Network	NICIPAddress NICMACAddress NICDescription
TapeDrive	TapeDriveCleaningRequired TapeDriveFirmwareVersion TapeDriveIndex TapeDriveModel TapeDriveMotionHrs TapeDriveSerialNumber TapeDriveType TapeDriveVendor
TapeLibrary	TapeLibraryFirmwareVersion TapeLibraryScsiId TapeLibrarySerialNumber TapeLibrarySlotCount TapeLibraryVendor TapeLibraryDriveCount TapeLibraryModel

Table C-4. Inventory Attributes of FC and Ethernet Switches for Reports

Component	Attribute
Contact	ContactInformation
	ContactLocation
	ContactName
Device	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
Firmware	FirmwareName
	FirmwareVersion
Network	NICIPAddress
	NICMACAddress
	NICDescription

Table C-5. Inventory Attributes of KVM for Reports

Component	Attribute
Contact	ContactInformation
	ContactLocation
	ContactName
Device	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName

Table C-5. Inventory Attributes of KVM for Reports *(continued)*

Component	Attribute
	DeviceSerialNumber DeviceServiceTag DeviceSystemModelType
Firmware	FirmwareName FirmwareVersion
Network	NICIPAddress NICMACAddress NICDescription

Table C-6. Inventory Attributes of DRAC for Reports

Component	Attribute
Contact	ContactInformation ContactLocation ContactName
Device	DeviceAssetTag DeviceDescription DeviceManufacturer DeviceName DeviceSerialNumber DeviceServiceTag DeviceSystemModelType
Firmware	FirmwareName FirmwareVersion
Network	NICIPAddress NICMACAddress NICDescription

Table C-7. Inventory Attributes of CMC for Reports

Component	Attribute
Contact	ContactInformation
	ContactLocation
	ContactName
Device	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
Firmware	FirmwareName
	FirmwareVersion
Network	NICIPAddress
	NICMACAddress
	NICDescription

\

Table C-8. Inventory Attributes of Printers for Reports

Component	Attribute
PRINTERSUPPLY	PrinterSupplyIndex
	PrinterSupplyDescription
	PrinterSupplyType
	PrinterSupplyLevel
	PrinterSupplyMaxLevel
PRINTERINPUTTRAY	PrinterInputIndex
	PrinterInputName
	PrinterInputVendorName
	PrinterInputModel
	PrinterInputDescription
	PrinterInputMaxCapacity
PRINTEROUTPUTTRAY	PrinterOutputIndex
	PrinterOutputName
	PrinterOutputVendorName
	PrinterOutputModel
	PrinterOutputDescription
	PrinterOutputMaxCapacity
PRINTERCOVERENTRY	PrinterCoverIndex
	PrinterCoverDescription
	PrinterCoverStatus
Agent	AgentDescription
	AgentGlobalStatus
	AgentId
	AgentManufacturer
	AgentName
	AgentVersion

Table C-8. Inventory Attributes of Printers for Reports *(continued)*

Component	Attribute
Contact	ContactInformation ContactLocation ContactName
Device	DeviceLocation DeviceSystemModelType
Firmware	FirmwareChassisIndex FirmwareIndex FirmwareName FirmwareReleaseDate FirmwareType FirmwareVersion
Network	NICIPAddress NICMACAddress NICDescription

Table C-9. Inventory Attributes of Power

Component	Attribute
Power Monitoring (for xx0x and xx1x servers)	PeakAmperage PeakPowerWatts PeakPowerBTUH PeakAmperageStartTime PeakAmperageTime PeakPowerStartTime PeakPowerTime

Table C-9. Inventory Attributes of Power

Component	Attribute
Power Budget (for xx0x and xx1x servers)	PeakHeadroomWatt
	IdlePowerWatt
	MaxPotentialPowerWatt
	CapValueWatt
	PeakHeadroomBTUHr
	IdlePowerBTUHr
	MaxPotentialPowerBTUHr
	CapValueBTUHr
Power Profile	ProfileSetting