Dell Management Console
Version 2.0.2

Release Notes

Dell Management Console provides a central point of access to monitor and manage systems on a local area network (LAN) or the wide area network (WAN). By providing administrators a comprehensive view across the enterprise, Dell Management Console can increase system uptime, reduce repetitive tasks, and prevent interruption in critical business operations.

What's New

New Major Features:

1. This release of Dell Management Console 2.0.2 includes Symantec(R) Notification Server (NS) 7.1 SP1. The details are as follows:
   - Symantec Management Platform 7.1 SP1
     Release notes: http://www.symantec.com/business/support/index?page=content&id=DOC3696
   - Symantec Notification Server 7.1 SP1
   - Windows 2008 R2 SP1 64-bit support

2. DMC can now be installed on Windows 2008 R2 or Windows 2008 R2 SP1 64-bit operating system.
3. Support for Lifecycle Controller 1.5 Software Inventory and Remote Updates (Dell Patch).
4. DMC is now available as self-extractable executable instead of ISO on support.dell.com.
5. DMC media or self-extractable executable only includes the installer and related components. It does not include the MSIs required for product installation. You must have internet connection to download the components required for the installation of DMC through SIM.
   If you do not have access to the Internet, you can create an installation package by installing SIM on a system with internet connection. Launch SIM, click "Create installation package" and select "Dell Management Console". This will create an installation package. Copy the installation package to the server you would like to install DMC.
6. New devices are supported. Refer to DELL MANAGEMENT CONSOLE Support Matrix located in Support.dell.com.

New Operating Systems Support:

1. Microsoft Windows Server 2008 R2 (64-bit) SP1

Fixes and Enhancements

Issue 1: DMC media now contains Symantec Installation Manager (SIM) that will be pointing to online Dell private product listing by default. An internet connection is required to download and install DMC (MSIs).

Issue 2: DMC media shall not carry any third party libraries/files such as Microsoft .NET 3.5, Microsoft SQL Express 2008, EMC Navisphere CLI etc. The minimum requirements section in DMC Install screen shall point to respective web-sites hosting the software.

Issue 3: DMC media shall not contain video tutorials, Readme and DMC FAQ documents. All the video tutorials and documents are available on Dell community site. http://en.community.dell.com/dell-groups/dell-management-console/m/dell_management_console-mediagallery/default.aspx

Issue 4: The Dell OpenManage(TM) Server Administrator Agent Deploy Solution is updated to allow deployment of OpenManage(TM) Server Administrator V6.5.

Issue 5: Fixed an issue where iDrac6 Console right click action for servers was getting removed when Agentless Inventory task is run using SNMP protocol.

Hardware and Software Requirements

Minimum Hardware Requirements

Physical server:

- 4 or more Processor cores
- 4 GB RAM
- DVD Drive
- Microsoft .NET 3.5 (SP1 is supported)
- Microsoft Silverlight 3.0
- Windows Internet Information Services (IIS) 7.0
- Microsoft SQL 2005 Express or SQL 2008 Express or
  SQL Server 2005 SP1/SP2/SP3 (32-bit remote or 64-bit) or
  SQL Server 2008 R2 (32-bit remote or 64-bit) or
  SQL Server 2008 ENT (32-bit remote or 64-bit)
- Windows Internet Explorer version 7.0 or 8.0 (32-bit only)

Note: .NET 4.0 is supported only if .NET 3.5 (SP1) is present on the system.

Hardware Configurations over 500 Devices

Physical server:

- 8 or more Processor cores
- 8 GB RAM
- DVD Drive
- Microsoft .NET 3.5 (SP1 is supported)
- Microsoft Silverlight 3.0
- Windows Internet Information Services 7.0
- SQL Server 2005 SP1/SP2/SP3 or SQL Server 2008, R2 (32-bit remote or 64-bit)
- Internet Explorer version 7.0 or 8.0 (32-bit only)

Note: Dell recommends remote 64-bit database for larger environments.

Software Requirements

Additional software required to Run Some Features of Dell Management Console are:

- For Dell/EMC storage arrays, ensure the array is FLARE(R) version 26 or later.
- Navisphere(R) Secure CLI (version 26 or above) installed on the management station.

Note: This CLI software can be downloaded from https://powerlink.emc.com.

Installation

Prerequisites

SQL Server Updates

The recommended SQL Server Updates are:

- SQL Server 2005 SP1 or SP2 or SP3 is required for using SQL Server 2005 as the default database.
- Optimize your SQL Server maximum memory settings as indicated in Microsoft(R) knowledge base articles KB321363 and KB319942. This configuration may significantly improve product performance.
- Altiris KB location http://www.symantec.com/business/support/index?page=home
  - #34345 "Notification Server performance issues due to SQL index fragmentation"
  - #38917 "Links to Notification Server/SQL Server Maintenance and Tuning Articles"

Note 1: Ensure that during installation of the SQL Server 2005/2008, you select a case-insensitive collation setting. If you select a case-sensitive collation setting, then the agent health Web part for an individual discovered device will not contain any information.

Note 2: The default collation setting in SQL Server 2005/2008 is case-insensitive.

Installation and Configuration Notes

- Installing Dell Management Console version 2.0.2.

  The Dell Management Console Install Guide is available on the Dell Tech Center website at www.delltechcenter.com. See the Dell Management Console page in the OpenManage Systems Management section.

  Also see the Dell Management Console User's Guide on the Dell Support website at support.dell.com/manuals for more information on installing the Dell Management Console.

- Symantec Installation Manager (SIM) is the installer for Dell Management Console. Starting DMC 2.0.2, you need to have internet connection to download the components (MSIs) required for installation through SIM.

  If you do not have access to the Internet, you can create an installation package by installing SIM on a system with internet connection. Launch SIM, click "Create installation package" and select "Dell Management Console". This will create an installation package. Copy the installation package to the server you would like to install DMC.

- When SIM is launched for first time prior to DMC install, it may throw an error dialogue box saying "Symantec Installation Manager has encountered a fatal exception and cannot continue. Please see the log file for more information". This is a known issue, this error occurs as SIM tries to point to global product listing instead of dell product listing. Work around for this is to continue the installation without clicking "ok" on the exception dialog box.

- For DMC 2.x installation we have the following three optional components:
  - 'Install Documentation'
  - 'Install Language Support' and,
  - 'Install Migration Wizard Components for migrating Dell Management Console data'

  If only some of the above three components are selected at the time of DMC installation, for the remaining non-installed components SIM may show install option as grayed out.

To enable the install option for the non-installed components, go to 'Settings' tab and click 'Update Now' button.

- To view the Tutorials online, make sure you have Windows Media Player installed. In Windows Server 2008 this comes with Desktop Experience: http://technet.microsoft.com/en-us/library/cc772567.aspx

- During install, take note of the following:
  - Do not disable or disconnect any network port while the installation is in progress.
  - Dell Management Console may require more available ports for agentless monitoring support. This change requires a system restart. http://technet.microsoft.com/en-us/library/cc758002%28WS.10%29.aspx
  - If you are using a remote SQL database on a system that has its firewall enabled, ensure that the firewall ports are open for the SQL Server instance to which the Symantec Platform will connect; otherwise you will encounter errors during installation. Alternatively, disable the firewall completely.
  - Refer to this article on How to configure SQL Server 2005 to allow remote connections: http://support.microsoft.com/kb/914277
  - Refer to this article for an overview and network port requirements for the Windows Server system: http://support.microsoft.com/kb/832017
  - To prevent Microsoft Windows Installer conflicts, do not run another install while Dell Management Console installation is in progress.
  - Register at http://www.dell.com/openmanage/register to receive a free Dell Management Console license. When installing the free Dell Management Console license, the license Web part is removed from the Dell Management Console portal page and you can customize the portal page.

- After installing Dell Management Console 2.0.2, do the following:
  - Enable the Symantec(R) Management Agent upgrade policy so that the Agent-based functionality is not interrupted.
  - For Windows Symantec management Agent:
    Go to Settings > Agents/Plug-ins > Symantec Management Agent > Windows
    Choose the appropriate policy depending on the architecture (x86/x64). Change this policy to On and save changes.
  - For Linux Symantec Management Agent:
    Go to Settings > All Settings > Agents/Plug-ins > Symantec Management Agent UNIX/Linux/Mac > Symantec Management Agent for UNIX/Linux/Mac – Upgrade.
    Change this policy to On and save changes.

  - After a successful upgrade of the Symantec Management Agent on the Dell Management Console system, if the Monitor Agent service has stopped, ensure that you restart the service manually.
  - Be aware the proper operation of the Symantec Management Agent on the managed systems may require opening ports on any firewall that may be in operation. See the Dell Management Console Ports document in the Dell Management Console section of the www.delltechcenter.com website.

    Refer to this whitepaper for information on network ports used DMC:
    http://en.community.dell.com/groups/dell_management_console/media/p/19527831.aspx

Installing Dell Management Console into a Virtual Machine (VM)

Dell Management Console is tested to install in the following VM environment:

- ESX 3.5 U4
- ESX 4.0
- ESX 4.1

Prerequisites for the VM install:

- Minimum 4GB Virtual RAM
- Minimum 4 Virtual Processors
- Physical server should have VT enabled processors
- Use a remote SQL database
- Variations on this configuration may work, but have not been tested.
- See http://www.symantec.com/business/support/index?page=home - 45258 and 45257 for additional details.

Upgrade

When upgrading to Dell Management Console 2.0.2, take note of the following:

- Launch Symantec Installation Manager (SIM).
  Start -> All Programs -> Symantec -> Symantec Installation Manager -> Symantec Installation Manager

  You may have to update the SIM first.

- After SIM launches, click Install New Products and select Dell Management Console.

- After an upgrade, it is recommended to import the Dell catalog before running applying updates to managed node using Dell patch.

- On upgrading to DMC 2.0.2, running previously created patch rollout job to apply the updates will fail. It is strongly recommended to apply the updates by creating a Stage and Distribute task.

Note: You will need internet connection on the server where the upgrade is being performed.

Open Issues and Resolutions

Issue 1: DMC only supports 32-bit Internet Explorer. 64-bit Internet Explorer is not supported.

Issue 2: You must restart the Symantec Management Agent after the network card is disabled in a dual-homed environment

The Symantec Management Agent does not bind to a particular network card, but it attempts to connect to the fully-qualified domain name. So, if you are using a connection-specific DNS name and disable the connection, you may experience an issue.

Resolution: Reset the Symantec Management Agent.
To reset the Symantec Management Agent, do the following:

1. Right-click the round yellow icon in the lower right-hand corner of the screen and select Symantec Management Agent.

2. Select the Task Status tab and click Reset Agent.

3. Wait until this message is displayed: Registered with <your_NS_server_name>. The agent is now reset.

Issue 3: Dell Management Console may experience multiple longevity issues when opened for extended periods. It is recommended to close the console (browser) when not in use.

Issue 4: After an upgrade, it is recommended that you restart the system.

Issue 5: If you see an E11: Object expected error message in the console, to resolve the issue restart the IIS Service.

Issue 6: When creating a WS-MAN connection profile using remote browser, the certificate file cannot be uploaded to the Dell Management Console server. The connection profile for WS-MAN protocol must be created on the server where Dell Management Console is installed.

Manually delete the device from the console and re-discover the device to render accurate health.

Database Migration

When upgrading from DMC 1.x to DMC 2.x you are moving from a 32 bit to a 64 bit platform. The change in platform does not support a direct upgrade path instead you must run a database migration. Before installation of DMC 2.x and running the migration please read DMC User Guide available at: http://support.dell.com/support/edocs/software/smdmc/

Issue 7: After Database Migration, Symantec Management Agent Report will still be present even though the feature is obsolete in DMC 2.x.

Issue 8: After DMC 1.x to DMC 2.x migration, if you are not able to use the already imported Server Administrator packages in the Agent Deploy Wizard then you have to delete them from the Software Repository, re-import the packages and use them for Server Administrator Deployment Task Wizard.

Issue 9: In the Altiris Log Viewer if you see "Authentication: Response to server challenge denied, check credentials are correct. Error code: -2146893048", there is no functional impact, and you may ignore this error message.

Issue 10: In the Altiris Log Viewer, if you see "Unable to get product details for the specified product (Product Guid: Symantec Management Agent for UNIX, Linux, and Mac 7.1 (c98d8bbb-70b9-4c39-ba55-110b2d07cbd6), MSI Product Guid: 8aa030b3-917a-49d8-a19b-f63c47ee23a0)", there is no functional impact, and you may ignore this message.

Issue 11: In the Altiris Log Viewer, if you see "Failed to load row from MSI Upgrade table", there is no functional impact, and you may ignore this message.

Issue 12: In the Altiris Log Viewer, if you see "Failed to load row from MSI Upgrade table", there is no functional impact, and you may ignore this message.

Issue 13: When you run the migration wizard import process, you might see "Failed to meet baseline requirements" message. There is no functional impact, you may ignore this message.

Issue 14: Associated Dell devices task created prior to Migration will no longer function after the Migration. A new associate Dell devices task has to be created.

Issue 15: After database migration, the migrated ESXi device primary health is displayed as Undetermined and the Connection state is displayed as Disconnected.

Install & Upgrades

Issue 16: In the Install New Products screen of Symantec Installation Manager (SIM), there is a check-box for Show all available versions. To view the previous versions of Dell Management console, make sure SIM is pointing to either online global product listing or online Dell private product listing.

Issue 17: To point to the online global product (GPL) listing to get the latest Symantec solutions and updates:

1. You need a connection to Internet to reach the GPL online.
2. After verifying that you can access the Internet, launch the Symantec Installation Manager through Program Files > Altiris > Symantec Installation Manager.

3. Click Settings in the start-up page of SIM.
4. Click Change product listing and type http://www.solutionsam.com/solutions/pl/symantec.pl.xml.
5. Click OK.
   You can access the latest solutions and updates in the Install New Products page.

Issue 18: To completely remove DMC from your system, use add/remove program instead Of the SIM installer.

Issue 19: Upgrade of Dell Management Console and ITMS to the latest version fails. During the initial installation or upgrade of products/solutions, Symantec Installation Manager (SIM) fails during the stop or restart of services. If you try to restart the service (in this case the service failing was the Altiris Service) manually, the following message is displayed: Failed while starting service: AeXSvc Configuration failed while attempting: Restarting services...

If you try to restart the Altiris Service manually, the following message is displayed:Error 1053: The service did not respond to the start or control request in a timely fashion. Then the Altiris Service stays in 'starting' mode and does not starts (until you reboot the machine or run NET STOP 'service name') Resolution: In the Properties' tab of the service, change the AppID from Local Admin Account to a Domain Admin/LocalSystem account that allows the services to keep running, starting, and stopping properly.

More information is in the Altiris KB:
http://www.symantec.com/business/support/index?page=home

Issue 20: When installing DMC 2.x, Dell branding and customizations are not displayed due to an update to SIM (Symantec Installation Manager). [491982]

Application Launch Solution

Issue 21: Launching Server Administrator for a second time on the same browser results in an error. This is expected behavior. As the part of security fix for XSRF (Cross site request forgery), Server Administrator validates every session against the secret key generated by the server. Close the first instance and re-launch the Server Administrator launch point.

Issue 22: All Dell Management Console launch points are hard coded to default values. If the application is installed in another location, edit the launch point from Settings > Console > right-click Actions. This applies to URL launch points as well.

Issue 23: When creating a right-click action for a particular Resource Type, several unsupported Data Classes are displayed; Choosing an unsupported Data Class results in an error.
To find the Data Classes that is supported for a resource:
1. Go to the Resource Manager for the Resource Type.
2. Go to View> Inventory.

Ensure that you only choose those Data Classes that are listed in the Resource Manager when creating a right-click action for a Resource Type.

Dell OpenManage(TM) Server Administrator Agent Deploy Solution

Issue 24: Server Administrator Agent deploy task wizard displays the status as waiting for Agent to get the status while the agent deploy and remote installation is in progress on the remote target server.

The functionality to update the task status is not enabled by default. This is because the option to have intermediate task status events being reported back to the server results in more bandwidth usage.
To enable this setting:
1. Click Settings > Notification Server > Site Server Settings > Site Management > Settings > Task Service > Settings > Task Service Settings.
2. Select Send detailed task events and click Save Changes. After saving the changes, the agent nodes require an updated configuration to apply the changes so that they can start sending detailed events.
3. Run the Update Client Configuration task to update the changes. The tasks now have this information reported.

Issue 25: OpenManage Server Administrator (OMSA) Deployment task will fail for a managed device that does not have the required disk space to install OMSA on it. Error message would say "The task was killed because it took longer than the allotted time". Ensure that managed device has sufficient disk space in the default drive before you re-run the deployment task.

Issue 26: On few occasions, OpenManage Server Administrator (OMSA) Deployment task wizard throws an error message:
"Failed to create Dell OpenManage Server Administrator Delivery Task"
Restart the following Altiris services and try running the task again:
Altiris Object Host Service
Altiris Service
Altiris Support Service
Altiris Client Task Data Loader
Altiris Client Message Dispatcher

Dell Patch Management Solution

Issue 27: Use update catalog and package repository from the same source. It is recommended that you use the update catalogs and package repository from the same source. Although Patch Management Solution for Dell systems allows you to mix online and offline locations for catalogs and update packages, this may cause problems with the availability of packages described by the catalog.

Issue 28: Identical server names may produce errors in the second-level report results. Drilling down into report results may produce errors if you have two servers with identical names in a production environment.

Issue 29: The Applicable Computers by Individual Update report may display duplicate entries in the first tier report results. The duplicate entries are actually different releases of the update that appear with the same name.

Issue 30: To update Dell OS Driver pack using Dell Management Console using the Lifecycle Controller on the managed node, download the catalog from ftp.dell.com. Catalog downloaded using the offline option (Server Update Utility catalog) does not contain the windows updates that Dell Management Console requires.

Issue 31: For Symantec Management Agent based updates, Rollout Jobs fail to complete because the final system reboot does not occur.
A server receiving updates from the Dell Management Console may fail to reboot automatically if the Altiris Power Control task fails to execute.

Issue 32: Internet Explorer Memory usage is high when you work with the Dell Patch Management solution. Internet Explorer allocates memory when a new window is opened and does not free the entire memory when that window is closed. Eventually this decreases the system performance.

Resolution: Close all browser windows and reopen Internet Explorer.

Issue 33: SQL memory usage is high when working with Dell Patch Management solution. The Dell Patch Management solution involves high use of SQL memory and affects system performance. Dell recommends a system with minimum 4 GB RAM and the following SQL memory settings:

Total System Memory	Maximum Memory Setting
2 GB	500 MB (minimum SQL Express memory is 256 MB)
4 GB	750 MB (minimum SQL Server memory is 512 MB)
8 GB	3.5 GB
16 GB	8 GB

For more information, see Microsoft KB 321363 and KB 319942.

Issue 34: The Compliance report for a server is displayed only if there are updatable components.

Issue 35: Systems that are rebooted after an update still display a Reboot Required message.
The return code is from the actual update process. You can go to the job and check the status of the task, including the status of the reboot.

Issue 36: The Check applicable updates by Computers report may display multiple entries for the same server name even if the report is grouped by computer name

Issue 37: Patch Rollout Job fails with message Schedule occurs in the past. Scheduling a stage and distribute task does not schedule the Staging and Preparing for Distribution task. It only schedules the Rollout Job.

If the staging and preparing for distribution task takes a longer time and surpasses the scheduled time for rollout job, the rollout job times out and the update task does not run on schedule. In such cases, Dell recommends using the Run now option to apply the patch.

If scheduling is required, then maintain a time delay between Stagings and distribute task and a Rollout job, so that the Rollout Job can start after the staging and distribute task is completed.

Issue 38: A Server Error message is displayed when you launch the Security Permissions page by clicking Settings> Security> Permissions menu on the Web page that is opened from the Getting Started Web part on Dell Patch Management solution portal page.

Resolution: The security permissions page can be launched without errors from the main console window by clicking Settings> Security> Permissions.

Issue 39: For a server that supports updates using Symantec Management Agent and updates using Lifecycle Controller, if an update is applied using one of the methods, that update is still seen as applicable under the Hardware Update Compliance reports.

Resolution: After applying the update to the server using either the Symantec Management Agent or the Lifecycle Controller, the user needs to run the following tasks for the Hardware Update Compliance reports to display the correct info:
1. Compliance Check task on Windows/Linux Servers
2. Dell Management Console Inventory task
3. Compliance task on Lifecycle Controller Enabled Servers

Issue 40: Dell 32 bit Diagnostics do not appear in the hardware compliance reports when updating Lifecycle Controller enabled servers As this update does not report component type currently, it cannot be updated using Patch Management Solution.

Issue 41: Under hardware compliance reports, Lifecycle Controller based updates will show up when the OS Type is selected as Windows or Linux. The Operating System column in the report will either be blank or is displayed as NA for Lifecycle Controller based updates.

Issue 42: When a bundle update is run on multiple LifeCycle Controllers Enabled Servers using WS-MAN (Apply updates using LifeCyle Controller), some of the updates may fail with an error message "A WSMAN connection could not be established". Run the job instance again to perform the update.

Issue 43: When a server and its iDRAC is discovered and inventoried using SNMP + WS-MAN protocol, users may see SNMP inventory information only. Re-run the discovery and inventory to get the WS-MAN inventory. Without WS-MAN inventory, you cannot apply updates using LifeCycle Controllers.

Issue 44: For agent based updates it is possible to have a successful update download task, but then to have the actual update fail to install on the client. In this case the inventory report will correctly show the older version of the update and the update will need to be re-applied.

Issue 45: When using online mode (ftp.dell.com), on few occasions the digital signature check for downloaded updates could fail due to corrupted download. Re-run the stage and distribute task to download the update again.

Event Console

Issue 46: Alert Initiated Discovery will not work for the PowerVault MD storage devices.
MD Array Traps are forwarded from the server where Dell PowerVault Modular Disk Storage Manager application is installed and the Host IP address in the trap is the server's IP address instead of the MD Storage Device. Alert Initiated discovery is run on the Host IP which in this case is the device that is managing the MD Storage device.

Issue 47: Traps from some Dell printers such as model number 2330dn and 2145cn may not be categorized properly in the Event Console. These models may not support the standard printer MIB (RFC 3805) for trap classification. Such traps will be received by the Event Console but displayed as Unknown Event Name, Unknown Event Category and Undetermined severity.

Resolution: You can perform all actions, such as Resolve, Acknowledge, and View Details that can be performed on other recognized alerts. The difference between recognized and unrecognized traps is that Name, Category, and Severity do not display the proper values.

Issue 48: Traps may not be received when both IT Assistant and Dell Management Console are installed on the same management station. To correct this behavior, restart the Altiris Event Engine and Altiris Event Receiver services.

Issue 49: Traps received from a managed node server having Red Hat Enterprise Linux 4 (Update:7) (x86 or 64) installed on it, will show 0 as Trap Description in Event Console. This issue is caused by a net-snmp bug introduced in Red Hat Enterprise Linux 4 (Update:7) operating system and not specific to Dell Management Console. Install the below mentioned rpms on the managed node to fix this issue:

net-snmp-utils-5.1.2-13.el4_7.3.x86_64.rpm
net-snmp-libs-5.1.2-13.el4_7.3.x86_64.rpm and
net-snmp-5.1.2-13.el4_7.3.x86_64.rpm

Issue 50: Purge policy will not purge events required for maintaining the device state. If you have large number of alerts it could cause latency in the Console.

Resolution: You can clear out the alerts manually in SQL Management Studio by deleting the alert entries in EC_Alerts table and delete the rulestate file located under [DMC_INSTALL_DIR]\Altiris Agent\Monitor Agent. However this will clear all device health until the next device health poll (default: every 1 hour).

Monitoring

Issue 51: Alerts sent from some versions of the PowerVault MD Storage Management Software for the MD3000 family of devices will not be associated with the MD device in Dell Management Console.

As a result, OnDemand polling for the MD Array will not be triggered. An alert will be generated on the next scheduled health polling cycle if the device state has changed. Reduce the polling interval for the primary health metric if you require more timely updates. Changing the interval will also affect other devices.

Issue 52: To create Customer filter for the Monitoring policies & metrics, it is required that you create the filter from the Dell Management Console Portal -> "Group View - Aggregate Health by Dell Resource" web part by launching the "Configure" dialog box. Save this newly defined custom filter and select the same in the "Monitor Target" web part for the monitor policies and metrics. Ensure that you run automation policy or reset the Monitoring Agent to pick up the latest changes.

Issue 53: If Performance monitoring is not working, it may be due to:

- The performance polices are not enabled by default. See the Dell Management Console User's Guide or the tutorial video for details on how to enable these policies.
- Performance policies for Windows require Windows 2003 or greater.
- The server you are attempting to monitor must be classified as a Dell Computer. This is a licensing restriction of the limited license.
- For WMI support, the credentials defined in the connection profile at the time the device was discovered must be valid credentials for that device. If the credentials are no longer valid for the device, the device must be re-discovered with the proper credentials.
- The last discovery for the device must have included the WMI protocol. When a device is discovered, it will only use the latest connection information to communicate with the device.

Issue 54: If any Group Metric target is changed from the default value to a custom target, this custom target must also be added to the policy. Changing this target will also force the group metric report to use this same target. Data from the old target will no longer be visible in the report. The new target must not be created from the monitor UI as this applies additional filters on the target and it will not work.

Issue 55: Under certain circumstances, the custom target may not display properly in the Monitor Resources by Status Web part.

Issue 56: If Performance Viewer is launched in 64 bit Internet Explorer instance on Microsoft Windows 2008, you will get errors like "An error has occurred during initialization of performance viewer. Re-installing performance viewer ActiveX controls may resolve the problem". In this release DMC supports 32 bit internet explorer, which is default browser on Microsoft Windows 2008.

Issue 57: In a maximum configuration environment consisting of 1000 devices or more, where health and power monitoring are enabled, it is not recommended to run Health Monitor Email task as it may result in SQL deadlocks and performance degradation.

Issue 58: After upgrading to DMC 2.x, all the devices health state will be displayed as Critical or Undetermined. It is recommended to reboot the system after an upgrade is performed to retrieve the health state of all the devices accurately. [490603]

Network Discovery and Inventory

Issue 59: SNMP Discovery of Windows Server 2008 Devices An SNMP-only network discovery task will fail to discover a system if that system is running Windows Server 2008 with its Network discovery feature disabled.

Perform the following steps to enable Network discovery on the target server:
1. Navigate to the target system's Control Panel.
2. Select Network and Sharing Center.
3. In the Sharing and Discovery section, set Network discovery to On.

Issue 59: IPMI Discovery: For proper classification of the IPMI device, the Channel Privilege Level Limit on the IPMI device and the IPMI Privilege level of the connection profile must match. If these levels do not match, the device will be classified as a Network Resource.

The following table lists the appropriate level relationships:

IPMI Device Channel Privilege Level Limit	Connection Profile IPMI Privilege level
Administrator	admin
Operator	operator
User	user

Issue 60: Discovery of Microsoft High Availability (HA) Clusters HA Clusters can be discovered using SNMP only. The discovery task that is intended to discover HA Clusters must have SNMP enabled in its Connection Profile and the associated credentials must be correct for the target devices.

In order for the members to be discovered, the IP address of each cluster member must be included in the list of addresses to be discovered by the discovery task.

When discovering HA Clusters, the cluster name may replace the name of the active cluster node. To avoid this, do not include the cluster IP address in the discovery range.

If the cluster IP address is the only IP address in the discovery task that is related to the HA Cluster, the currently active cluster node will be discovered and its name will be the same as that of the cluster itself. This results in the cluster name appearing in several places under the All Devices organizational view.

For example:
- Under HA Clusters as the HA Cluster
- In the resource pane as the discovered system when the cluster's organizational group is selected
- In the resource pane as the discovered system when the Servers organizational group is selected

Issue 61: Duplicate entries of a server found after running a discovery task

If a server and its associated Dell Remote Access Card (DRAC) are discovered using SNMP (with or without also using IPMI), two entries for that server are displayed under the All Devices organizational view: one entry for the server and one for the DRAC.

Issue 62: Dell Servers are classified as Computer even if IPMI is enabled in the connection profile.

When discovering Dell servers using only SNMP or WMI, Server Administrator must be installed and running on the managed system in order for the system to be classified as a Dell Computer.

Consider this situation:
- If IPMI is used in combination with SNMP or WMI,
- You specify both, the server IP address and baseboard management controller (BMC) IP address in the discovery task, and
- Target server is not running Server Administrator

Two devices will be discovered: a Computer and a Dell Computer.

In this case, the Dell Computer is associated with the BMC IP address and the Computer is associated with the target server.

Issue 63: Symantec Management Agent push fails in certain cases when using SNMP+IPMI or SNMP+WS-MAN to discover a server and its associated iDRAC.

If a server and its DRAC or BMC are discovered using SNMP and IPMI, or SNMP and WS-MAN the IP address of the DRAC/BMC may be associated as the primary IP address of the server.

To avoid this situation, it is recommended you discover the DRAC/BMC in its own discovery task before discovering the server in a separate discovery task.

Issue 64: With latest firmware version 3.1, Dell PowerConnect switch M6348 will not be discovered as Dell device. As a result, PowerConnect M6348 Switch is not shown in Dell reports.

Issue 65: DMC uses the industry standard Printer MIB version 2 to discover and classify printers. Since this is an industry wide standard, many non-Dell printers will respond to SNMP queries based on this MIB. In addition, the MIB does not supply a way to distinguish the manufacturer of the printer. As a result, many non-Dell printers will be classified as Dell Printers when discovered by DMC.

Issue 66: Linux Symantec Management Agent entry is not correlated with Dell Computer entry

When the Symantec Management Agent is installed on a Dell server running a supported Linux distribution and resource entry for that system is automatically created by the Symantec Notification Server.

After a Network Discovery task is run in which the system described above is targeted, a second resource entry is created for that system.

Ideally, there should only be one resource for this system. However, the Symantec Management Agentdoes not provide enough information about the system for DMC to detect the duplicate devices thus creating the situation described above.

Issue 67: Inventory for Brocade Switches shows incorrect details.

When devices are discovered on subnets different from that of the DMC console, the MAC address of the router is returned as the MAC address of the devices.

DMC uses ARP to gather the MAC addresses during Network Discovery and the router returns its own MAC address to the ARP request when the device is on a different subnet.

Issue 68: The Contact Information table in Resource Manager -> Hardware Summary is not displayed for ESXi machines.

Reports

Issue 69: PowerConnect M6220, M6348, M8024 and 8024F may not show up in the Ethernet switch report.

At the time of this Dell Management Console release, the shipping version of the firmware for these switches was not providing the information needed to display them in this report. This is being addressed in newer firmware releases for the individual switches.

Issue 70: Removed Symantec Management Agent Version report under Dell Reports folder. Use reports located under Notification Server>Agent reports folder.

Tasks

Issue 71: To run IPMI-related tasks against IPMI-capable devices, such as Dell servers, you must enable the IPMI protocol to discover these devices. The discovery task for IPMI devices should include the IP Addresses that support the IPMI protocol. For Dell servers, these are the IP Addresses by which the DRAC and/or BMC communicate.

Issue 72: On managed systems running Windows, if you want to set the front panel LCD text to a multi-word text that contains spaces, use the Command Line Builder task or the BIOS Configuration task. Also enclose the text in quotes. For example: PowerEdge 2950.

Issue 73: On managed systems running Linux, you cannot set the front panel LCD text to a string with embedded spaces using the Command Line Builder or BIOS configuration tasks. PowerEdge 2950 is not a valid setting for LCD text on Linux systems.

Managed systems running Linux have additional restrictions on custom text: some special characters like "&" and "(" cannot be used in the custom text for the above tasks.

Issue 74: In the Associate Dell Devices task, in Target Selection, (Apply to> Computers,) if you choose the filter (Add Rule): exclude computers not in> Group> Computers, then it only displays (managed) systems that have the Symantec Management Agent installed on them.

To select unmanaged computers, choose the following filter: exclude computers not in> Computer list> Computers.

Issue 75: Exporting a task or policy to an external USB device does not release the device handle.

To work around this issue, export the task or policy to a local drive and copy the exported files to the external USB device.

Issue 76: Dell Web Server (DWS) Configuration is not supported for Linux targets in OMSA 6.1. As a consequence configuring DWS using either the DWS Configuration Task or the OpenManage Command Line Interface (OMCLI) task on Linux targets will cause the task to fail. Due to an issue in the task framework with Linux targets, these tasks when executed against Linux targets take a long time (~1 hour) to show the failure.

Issue 77: If you click on the "Warranty Report" link from the "Warranty Extractor Task" UI on an SSL enabled DMC, you are required to enter Administrator credentials to access the page. This is due to an issue in the framework API used to retrieve the URL prefix. If you provide the correct credentials, you can view the report from the Task UI page. Alternately, you can choose to view the report from the "Reports"-> "Dell Reports" page, where you are not required to supply credentials.

Issue 78: Remote Server Administrator command line task may fail for Server Administrator running on Microsoft Windows 2008 and Microsoft Windows 2008 R2. To enable the successful functioning of remote Server Administrator CLI, the managed system and the management station must be on the same domain or there should be a trust relationship between the two domains.

If you have a Windows firewall configured on either the management station or the managed system, change these settings:

On the management station:
1. Open TCP port 135.
2. Add the "omremote.exe" application
   (located in \dmc\DMCTasksSolution\ToolsBin) to the firewall exception list.

On the managed system:
On the command prompt, type:
"netsh firewall set service RemoteAdmin"

For more information on connecting through the Windows firewall, see Microsoft's MSDN website for Platform SDK: Windows Management Instrumentation (Connecting through Windows Firewall) at:
- http://support.microsoft.com/kb/875605
- http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx

Ensure the following settings are applied for users with non-administrator privileges:
1. Grant DCOM remote launch and activation permissions for a user or group.
2. Grant DCOM remote access permissions.
3. Allow users access to a specific WMI namespace.

For more information see:
http://msdn.microsoft.com/en-us/library/aa393266(VS.85).aspx

Issue 79: When a task is running, the task status may be incorrectly shown as Pending. Double click on the task run instance to view the correct status.

Issue 80: Warranty task may fail due to internet connectivity issue with the web service; in such cases please make sure you have internet connectivity and retry after some time, the task should work.

Issue 81: When using Update CMC Firmware task, make sure the firmware image path specified does not exceed 65 characters. Otherwise the task fails with an error message: "ERROR: Specified path is too long."

ESX Support

Issue 81: The Symantec Management Agent is not supported on ESXi 4.0. As a result, Dell Patch Management and Performance monitoring are not supported.

Resource Links

1. The Dell TechCenter
   http://www.delltechcenter.com/page/Dell+Management+Console
2. Altiris Knowledge Base Articles
   http://www.symantec.com/business/support/index?page=home
3. Juice User Community: A Community for Symantec Customers and End Users
   http://www.symantec.com/community/
4. Video Tutorials: DMC 2.0.2 installer has references to a bunch of video tutorials.
   http://en.community.dell.com/

Global Support

For information on technical support, visit www.dell.com/contactus.

See the Dell Management Console FAQs on the Dell TechCenter website.

July 2011 **Rev. A00**