Dell OpenManage Server Administrator
Version 7.1

Readme

This document contains updated information for the "Dell OpenManage Server Administrator User's Guide" and any other technical documentation included with Server Administrator.

NOTE: Dell OpenManage System Management software, including the Dell OpenManage Server Administrator (Server Administrator), is available only on the "Dell Systems Management Tools and Documentation" DVD.

The Dell OpenManage Server Administrator (Server Administrator) documentation includes the "User's Guide", "Messages Reference Guide", "CIM Reference Guide", "Command Line Interface (CLI) User's Guide", "SNMP Reference Guide", and "Compatibility Guide".

You can access the documentation from the Dell Systems Management Tools and Documentation DVD or from "support.dell.com".

What's New

Added support for the following operating systems:

- VMware ESXi 5.0 U1
- RedHat Enterprise Linux 5 SP8 x86
- RedHat Enterprise Linux 5 SP8 x86_64
- RedHat Enterprise Linux 6 SP2 x86_64

NOTE: Microsoft Windows 2003 is not supported on yx2x systems.

Deprecated the following operating systems:

- RedHat Enterprise Linux 5 SP7 x86
- RedHat Enterprise Linux 5 SP7 x86_64
- RedHat Enterprise Linux 6 SP1 x86_64
- VMware ESXi 5.0

New Platforms supported:

- Dell PowerEdge M820
- Dell PowerEdge T420
- Dell PowerEdge T320

New Features:

Server Administrator:

- Added support for the following Network Interface Cards (NICs), Converged Network Adapters (CNAs), and Fibre Channels (FCs):
  - Broadcom 57810 Dual Port 10GbE KR Blade Converged Mezzanine Card
  - Broadcom 57810 Dual Port 10Gb Base-T -CNA
  - Broadcom 57810 Dual Port 10GbE SFP+ Converged Network Adapter
  - Qlogic QME8252-K Mezz (Ensign Kim)

    - Qlogic P3+ Dual port 10Gb SFP+/DA
    - Brocade 10Gb CNA (BR1741M-k (New)
    - Emulex Single Port FC16 HBA
    - Emulex Dual Port FC16 HBA
    - Qlogic QLE2460 Single port FC4 Adapter
    - Qlogic QLE2462 Dual port FC4 Adapter
    - Brocade BR815- Single Port FC8 Adapter
    - Brocade BR825- Dual Port FC8 Adapter
    - Qlogic QLE2562 Dual Port FC8 Adapter
    - Emulex LPe-12002 Dual Port FC8 Adapter
    - Qlogic QME2572 Dual Port FC8 Mezz
    - Emulex Lpe-1205-M Dual Port FC8 Mezz
    - Qlogic QLE2560 Single Port FC8 Adapter
    - Emulex LPe-12000 Single Port FC8 Adapter
    - Broadcom 57810 Dual Port 10GbE KR Blade Converged Mezzanine Card
    - Broadcom 57810 Dual Port 10Gb Base-T
    - Broadcom 57810 Dual Port 10GbE SFP
    - Qlogic QME8252-K Mezz
    - Qlogic P3+ Dual port 10Gb SFP+/DA
- Added support for PowerEdge “OEM Ready” server models that allow reseller custom branding. For more information, see dell.com/oem.

Storage Management Service:

- The current release supports the Web browsers, Internet Explorer 10.0, and Mozilla Firefox versions 10.0, 11.0, and 12.0.

For a complete list of supported operating systems and platforms, see the latest Dell Systems Software Support Matrix stored on the media.

Hardware and Software Requirements

Hardware Requirements

- Minimum of 2 GB RAM
- Minimum of 512 MB free hard drive space
- Administrator rights
- Monitor with a minimum screen resolution of 800 x 600. The recommended screen resolution is at least 1024 x 768

Software Requirements

- One of the supported operating system and web browsers.
- TCP/IP connection on the managed system and the remote system to facilitate remote system management.

- One of the supported systems management protocol standards. For more information, see "Supported Systems Management Protocol Standards".
- The Server Administrator Remote Access Controller service requires remote access controller (RAC) to be installed on the managed system. See the relevant Dell Remote Access Controller User's Guide for complete software and hardware requirements.

NOTE: The RAC software is installed as part of the Typical Setup installation option, provided the managed system meets all of the RAC installation prerequisites.

- The Server Administrator Storage Management Service requires Dell OpenManage Server Administrator to be installed on the managed system. See the Dell OpenManage Server Administrator Storage Management User's Guide for complete software and hardware requirements.
- Microsoft Software Installer (MSI) version 3.1 or later.

NOTE: Dell OpenManage software detects the MSI version on your system. If the version is lower than 3.1, the prerequisite checker prompts you to upgrade to MSI version 3.1. After upgrading the MSI to version 3.1, you may have to reboot the system to install other software applications such as Microsoft SQL Server.

Installation

For complete installation instructions, see the "Dell OpenManage Server Administrator Installation Guide Version 7.1".

Installation and Configuration Notes

This section provides information to help enhance your experience with Server Administrator in particular, implementations and environments.

- Port 1311 is the default port for Server Administrator. It is a registered port number of Dell Inc. If another application is configured to run on port 1311 before Server Administrator is installed, the DSM SA Connection Service does not start after installation. Before you install Server Administrator, make sure that the port 1311 is not in use.
- Before starting Server Administrator, you must enable the client-side scripting in Internet Explorer. To do so, perform the following steps:
  1. In Internet Explorer, navigate to the "Tools" menu.
  2. Click "Internet Options".
  3. Click the "Security" tab.
  4. Select the security zone to which the system running Server Administrator belongs.

     NOTE: This option should be set to "Trusted sites".

  5. Click the "Custom Level" button.
  6. For Windows 2003, perform the following steps:
     - Under "Miscellaneous", select the "Allow Meta Refresh" radio button.
     - Under "Active Scripting", select the "Enable" radio button.
     - Under "Active scripting", select the "Allow scripting of Internet Explorer web browser controls" radio button.
  7. Click "OK" and restart your browser.

- To allow Single Sign-on for Server Administrator, perform the following steps:
  1. In Internet Explorer, navigate to "Tools".
  2. Click "Internet Options".
  3. Click the "Security" tab.
  4. Select "Trusted sites".
  5. Click the "Custom Level" button.
  6. Under "User Authentication", select the "Automatic Logon with current username and password" radio button. Click 'OK' to exit the "Custom Level" window.
  7. Now select the "Advanced" tab, and under "HTTP 1.1 settings", make sure "Use HTTP 1.1" is checked.
  8. Select "Trusted sites". Click "Sites". Add the server to the website.
  9. Click "Close".
  10. Click "OK" and restart your browser.
- If you run a security scanner tool such as Nessus, against the Server Administrator Web server, certain security warnings may be displayed against port 1311 running the Server Administrator Web server. The following warnings have been investigated by Dell engineering and are determined to be "false positives" (invalid security warnings) that you can ignore:
- "The Web server on 1311 allows scripts to read sensitive configuration and / or XML files." This warning is a false positive.
- "The Web server on 1311 allows to delete "/" which implies that the Web server will allow a remote user to delete the files in root on the server." This warning is a false positive.
- "The web server on 1311 may be susceptible to a 'www Infinite Request' attack." Dell has determined that this warning is a false positive.
- "It is possible to make the remote thttpd server execute arbitrary code by sending a request like: GET If-Modified-Since:AAA[...]AAAA

  Solution: If you are using thttpd, upgrade to version 2.0. Else, contact your vendor and ask for a patch, or change your web server. CVE on this one is CAN-2000-0359". Dell has determined that this warning is a false positive.

- Enabling Integrated Windows Authentication in Internet Explorer is not required to activate the Single Sign-On feature.
- The Server Administrator security settings are not applicable for Active Directory users. Active Directory users with read-only login can access Server Administrator, even after the access is blocked in the Server Administrator Preferences page.
- Dell SNMP MIB Files for Dell Systems Dell SNMP MIB files for Dell systems allows you to obtain and verify information provided by supported software agents. The current MIB files supported by PowerEdge(TM) software agents are located at "\support\mib" on the "Dell Systems Management Tools and Documentation" DVD.

  NOTE: A MIB-II-compliant, SNMP-supported network management station is required to compile and browse MIB files.

- OpenManage support for Encrypting File System (EFS)

To improve security, Microsoft provides the capability to encrypt files using EFS. Note that OMSA will not function if its dependent files are encrypted.

- Server Administrator GUI and CLI Response Time

  On Dell PowerEdge x9xx and later systems, the response time for some parts of the Server Administrator GUI and CLI has increased to several seconds as Server Administrator no longer caches some of the DRAC/iDRAC data. The data must be retrieved from the DRAC/iDRAC when you request for it.

Following are the Server Administrator GUI pages whose response time may have increased:

- Server Administrator home page on log in
- Remote Access -> Users
- Alert Management -> Platform Events

Following are the Server Administrator CLI commands whose response time may have increased:

- omreport chassis remoteaccess config=user
- omreport system platformevents
- omreport system pedestinations

The amount of time varies depending on the hardware system and operating system.

Notes

Notes for Instrumentation Service

- On xx1x systems, if conflicting BIOS settings exist while configuring BIOS setup options through Server Administrator, the update attempt may fail at system reboot and none of the BIOS setup options may be updated.

  For example, when you configure Embedded SATA Controller to RAID and Boot Mode to UEFI simultaneously (UEFI does not support RAID option), this conflict prevents updates to any BIOS configuration (at system reboot).

- On certain systems, user-defined thresholds set under Server Administrator become the default thresholds after uninstalling Server Administrator.

  After you change the threshold value of a probe on certain systems, running Server Administrator, and then uninstall the application, the changed threshold value becomes the default threshold value.

- While modifying the warning threshold settings, the values are stored in the firmware as discrete integer values and scaled for display. If the modified value is not a discrete integer, it may change when saved.
- Fan redundancy can have the following states:

  Fully Redundant - The sensors display this status if all the fans in the system are present and are in a non-failure state.

Redundancy Lost - The sensors display this status whenever any system fan fails or is removed from the chassis.

- If a system with memory redundancy enabled enters a "redundancy lost" state, it may not be clear which memory module caused it. If you cannot determine which DIMM to replace, see the "switch to spare memory detected" log entry in the ESM system log to find the memory module that failed.
- If you run Server Administrator when the system is in "OS Install Mode", it may report the memory incorrectly. To avoid this issue, you must disable "OS Install Mode" before running the application.
- If you have to uninstall and reinstall the operating system SNMP service, then reinstall Server Administrator, so that the Server Administrator SNMP agents are registered with the operating system SNMP agent.
- Server Administrator Device Drivers for Linux Server Administrator includes two device drivers for Linux: Dell Systems Management Base Driver (dcdbas) and Dell BIOS Update Driver (dell_rbu).

  Server Administrator uses these drivers to perform its systems management functions. Depending on the system, the application loads one or both of these drivers. These drivers have been released as open source under the GNU General Public License v2.0. They are available in Linux kernels from kernel.org starting with kernel 2.6.14.

Notes for Storage Management Service

- Detailed information on the Storage Management Service is available in the Storage Management Service online help. After installing and launching Server Administrator, you can access the Storage Management Service online help by selecting the Storage or lower-level tree object and clicking the Help button on the global navigation bar.

Notes for Remote Access Service

- The remote access service is available on supported systems only in this release. It enables remote access to a server that has lost its network connection or that has become unresponsive. In the current release of Server Administrator, the Remote Access Service uses Integrated Dell Remote Access Controller (iDRAC).
- iDRAC also has its own CLI that is accessed through the "racadm" command. You can add "racadm" commands to a batch or script file to automate various user tasks. To limit the stress load on the managed system and RAC, add "sleep" or "delay" commands of one or two seconds between the individual "racadm" commands.

Corrected Problems

The following problems were reported in earlier releases of Server Administrator and have been corrected in this release:

- Issue 1 DF289096 ESX4i: DWS does not show connection error after login
- Issue 2 DF416987 E-Clarity: The space between two RAID 10 layout span disk in the Advance wizard is more
- Issue 3 DF419932 E-Clarity: Improper alignment for "Date" text boxes in asset info page FF3.x
- Issue 4 DF419976 E-Clarity: An extra line is displayed in the Destinations Table-Platform Events Page

- Issue 5 DF421616 E-Clarity: Page Expired error occurs when the Go Back button is clicked - Inband failure page
- Issue 6 DF421990 E-clarity: |Om6.4|Improper Alignment
- Issue 7 DF423927: Inconsistency seen between DWS and Legacy Login for Interface Names in Brazilian OS
- Issue 8 DF445065: Restarting web server from Server Administrator GUI gives fatal JRE error-no functionality loss
- Issue 9 DF449421: Server Administrator GUI: Setting power profile fails when BIOS setup password is enabled
- Issue 10 DF451609: Mail-to Setting should be provided allowing user to set the default mail-address
- Issue 11 DF451867: OM6.5.0x136 - ITA omremote.exe does not work against SLES 10 SP4 targets
- Issue 12 DF465223: OM6.5, In IE8 with Enhanced Security, adding trusted site is not fully working

Open Issues and Resolutions

This section provides information on open issues and workarounds with this release of Server Administrator.

Issues for Server Administrator running on VMware ESX Operating Systems

Issue 1 DF374857: Connection service needs to be restarted for an Active Directory user login.

• To log into Server Administrator while using the VMware ESX 4.1 operating system as a server administrator, restart the DSM SA Connection Service.

• To log in to the Remote Node while using the VMware ESX 4.1 operating system as a Remote Enablement Agent, wait for about five minutes for the 'sfcbd' to add the permission for the new user.

Issue 2: DF354388: Remote Server Administrator Web Server connection to managed node hangs, if a redundant virtual disk containing syslog dumps fails due to any reason.

If you configure the syslog to store logs on a remote virtual disc (VD), and remove the remote VD without reconfiguring the syslog to a valid location, the Server Administrator web server screen stops responding.

To continue using the Server Administrator Web server, restart the management services on the managed node.

Issue 3: DF516238: Power cycle shuts down server in ESX 4.1 U2 classic.

On ESX 4.1 U2 classic, when power cycle operation is done from Remote shutdown page using Server administrator, the server shuts down instead of Power cycle or reboot.

Issue 4: DF550588: On ESXi 5.0 U1 operating system, the performance of Server Administrator is slow.

On ESXi 5.0 U1 operating system, the Server Administrator is slow. VMware has reported this as a known issue. For more information, refer to the Knowledge Base article at - http://kb.vmware.com/kb/2016538.

Issues for Server Administrator Web Server running on all Linux Operating Systems

* Issue 1: DF275424, DF332775: Domain users unable to login to Windows MN from Linux Web Server.

Negotiate authentication is not supported while managing a Windows-based managed node from a Linux-based Server Administrator Web server, remotely. If you run the Server Administrator Web server on a Linux based operating system and try to manage a remote Windows managed system as domain user, a "login failed" message appears.

You can manage a Windows/Linux based Managed System remotely from a Windows-based Server Administrator Web server.

Issue 2: DF533809: The "Launch Server Administrator" icon on the X-Windows desktop launches Server Administrator in the default Web browser. The corresponding URL uses the default parameters "localhost" and the port number "1311". Any change in the server IP parameters or a change in the port number for the Server Administrator renders the icon/link useless. To re-activate the functionality, update the icon file with the correct URL parameters.

Issues for Server Administrator Running on All Supported Operating Systems

Issue 1: Due to non-availability of resources, inventory collection may terminate unexpectedly and restart. If this occurs, the folder "C:\Temp\invcol" may be left as an artifact.

The presence of this folder does not affect the functionality of the inventory collection. The folder can be deleted if required.

Issue 2: After installing Server Administrator from the command prompt, entering an "omreport" or "omconfig" command from the same prompt can cause an error. Open a new command prompt window and enter commands.

Issue 3: If the command log page in the Server Administrator GUI displays an error message indicating that the XML is malformed, you must clear the command log from the CLI using the "omconfig system cmdlog action=clear" command.

Issue 4: After a "Reset to Defaults" operation of the Integrated Dell Remote Access Controller, the first user configuration operation fails if it is a single-user configuration item (such as enabling or disabling a user or changing user name). Always change a combination of two-user configuration items (such as enabling or disabling a user and changing user name) concurrently during your first configuration operation.

Issue 5: While browsing through IT Assistant, if the SNMP protocol is disabled and the CIM protocol is enabled, the redundancy status is shown as "lost" even if the system has full redundancy. To confirm the correct state of the system, use the Server Administrator user-interface.

Issue 6: The "Format or Split Mirror" operation may fail on a RAID 1 virtual disk on a CERC SATA 1.5/6ch controller.

Issue 7: While entering the Server Administrator command line "omreport system version -outc <filename>", ensure that you specify an absolute path name for the output file, for example, "c:\out.txt" else, the output file is empty.

Issue 8: Entering the "omreport system esmlog/alertlog/cmdlog -fmt tbl" command on the CLI can result in XML parsing errors if the size of the log is very large.

Use the GUI or the "omreport system esmlog/alertlog/cmdlog" CLI command to view the contents of the log.

Issue 9: For complex "omconfig" CLI commands that contain multiple set commands in one command line, the CLI may report a success status for the command even if a part of the command failed. To avoid this issue, run only one command per command line. The current settings can be confirmed by performing the corresponding "omreport" command.

Issue 10: Some complex "omconfig" CLI commands that contain multiple set operations have been modified to avoid the above problem. While executing a CLI command if the message, "Error! Illegal combination of parameters" appears, modify your command into several simpler commands. Each command should change only one setting.

Issue 11: When running Server Administrator on a system with a traditional Chinese operating system, the application pages are displayed in simplified Chinese. To view the Server Administrator pages in English, go to your browser language preference page and change the language to English.

Issue 12: Log files saved from Server Administrator are saved in zip format. It is recommended that you open this zip file using WinZip. Using the Windows Server 2003 or Windows XP embedded "Compressed (zipped) Folder" utility is not recommended.

Issue 13: After configuring BIOS settings on certain systems, a second reboot may be required for the Server Administrator to display the updated BIOS settings properly.

Issue 14: If you import an invalid root certificate into Server Administrator, using "Preferences-> General Settings-> Web Server-> X.509 Certificate", and try to log on to the application after restarting the Web server, a blank page is displayed.

To correct this issue, restore your original "keystore.db" file before importing a valid root certificate. To restore the "keystore.db" file, use both the basic operating system commands and the Server Administrator Command Line Instrumentation (CLI).

Perform the following steps from your operating system command line:

1. Type:

   omconfig system webserver action=stop

2. Locate the "keystore.db.bak" file. The default path is

   "C:\program files\dell\SysMgt\apache-tomcat\conf".

3. Copy "keystore.db.bak" to "keystore.db".

4. Type:

omconfig system webserver action=start

Issue 15: A temperature drop below a minimum failure threshold does not cause a system reset even if this alert action is set.

Issue 16: Clicking the "Back" and "Refresh" buttons on the browser may not display the correct page with respect to the Server Administrator component tree, tabs, tab menus, or help, as Server Administrator has been designed with limited functionality to reduce overhead.

Full feature capabilities of the Web browser such as "Back", "Refresh", and "Open in New Window" may not be supported.

Issue 17: Selecting the boot sequence under the BIOS "Setup" tab does not re-enable boot devices that have been disabled in the System Setup Program, earlier.

Issue 18: The links on the Server Administrator home page may not work after repeated random clicking.

To resolve this issue, refresh the browser by pressing <F5> or click the browser "Refresh" button.

Issue 19: All unsecured HTTP requests to Server Administrator receive an invalid response. Server Administrator runs only one instance of the Web server, which is secure. Make all connections through https://<ip address> : <port number>. Any "http://<ip address>: <port number>" request for connection with the server receives an invalid response.

Issue 20: If the browser used with Server Administrator does not display a page or perform an action, make sure that the browser is in online mode. To go online, perform the following:

- In Internet Explorer, on the menu bar, click "File" and clear the "Work Offline" option. When "Work Offline" is selected, a check mark is displayed to the left of the option on the "File" menu.

Issue 21: If Internet Explorer prompts you to "Work Offline", "Connect", or "Try Again", always select "Connect" or "Try Again". Do not select "Work Offline".

Issue 22: While setting dates in the "Asset Information" section of the Server Administrator home page, the current time is appended to the date.

While setting dates with the CLI, the appended time is noon.

Issue 23: On some systems, temperature probe values and settings are only supported for whole degrees, not tenths of a degree. On these systems, setting a fractional value for the minimum warning temperature threshold results in the set value being rounded down to the next whole number value.

This behavior may cause the minimum warning threshold to have the same value as the minimum failure threshold.

Issue 24: If you close the browser using the "Close" button on the browser or log off from the operating system, the Server Administrator session is not terminated. This session is listed in the Session

Management page until the session time out occurs, or DSM SA connection service is restarted, or the operating system is rebooted.

Issue 25: If you change the operating system Time Zone to a new timezone, Server Administrator session management does not display the time in the new time zone specified. Restart Server Administrator to display the accurate time for the time zone in the Session Management page.

Issue 26: DF78425: The Server Administrator Auto Recovery feature may execute the configured action before the time interval when the system is under heavy stress.

The Auto Recovery feature can be set to execute an action (For example, reboot system) to recover a hung system. Since the Auto Recovery timer is now an application-level timer instead of a kernel-level timer, heavy resource stress on the system may result in an inaccurate measurement of a short keep alive interval (less than 120 seconds), and the configured action may be triggered.

The issue is more prevalent in systems that have only one CPU with hyper-threading unsupported/disabled or systems that are subjected to persistent stressful conditions such as, resource depletion and CPU running at 100% usage with significantly more threads than normal usage.

The Auto Recovery feature is not enabled by default. If the Auto Recovery feature has been enabled, increase the System Reset Timer value to at least 120 seconds.

Issue 27: Using the Internet Explorer browser, if you install Server Administrator on a system that includes an underscore in its hostname, you must use the IP address of the target system in the browser URL to launch Server Administrator, as Hostnames with underscores are not supported. For example, (assuming Server Administrator is listening on port 1311):

https://192.168.2.3:1311.

For more information, see the following article on the: Microsoft website - http://support.microsoft.com/kb/312461

Issue 28: DF 152755: The Server Administrator GUI does not respond when the alerts log has many events. If the Alert Log contains several entries and if you try to navigate to another page, the Server Administrator GUI may take about 30 seconds to display the content.

Issue 29: DF 172125: Power monitoring probes are shown on certain systems that do not support power monitoring.

On certain systems that do not support power monitoring, Server Administrator reports the two platform event filters related to power monitoring as "System Power Probe Warning" and "System Power Probe Failure". These two filters are not supported on these systems. That is, you can view and configure these filters, but no action is taken.

Issue 30: DF185770: Primary User Telephone Number does not accept symbols.

On Server Administrator, Under Asset Information->System Information->Primary User Telephone Number configuration allows only alphanumeric characters.

Issue 31: The selection of default option for front panel LCD in Server Administrator displays the Model Name where as the default is Service Tag on the physical LCD.

Issue 32: In case Server Administrator does not respond or is locked to your selections on the component tree, perform the following steps:

1. Click “Preferences”. The Preferences page appears.
2. Click “Server Administrator”. The items on the front page may respond to your click.

Issue 33: DF277439: Persistence of Configuration and Log File Changes in VMware ESXi

On systems running the VMware ESXi operating system, the file system is ramdisk. Modifications made to the files within the file system are generally not persistent across reboots, with the exception of designated configuration and log files. These files are updated to the disk periodically and on system shutdown. If the system is reset without a graceful shutdown before the updates to the designated configuration are made and before log files are updated to the disk, the changes are lost.

The following is an example of the effect of this behavior:

On certain systems, the first time that the thresholds for a probe are changed after Server Administrator is installed, the current threshold values for that probe are saved as the default threshold values by writing the values to a configuration file. When "Set to Default" is performed after the first change of the thresholds, Server Administrator sets the threshold values to the values that were saved in the configuration file as the default. If the system running the VMware ESXi operating system is reset without a graceful shutdown before the changes to the configuration file are updated to the disk, the user-defined thresholds become the default thresholds.

Issue 34: DF315853: Some Server Administrator CLI commands functions properly only when run from the elevated console window.

Some Server Administrator CLI commands may function properly only when they are run from the elevated console window. Therefore, it is recommended that you use the elevated console for running the CLI.

Issue 35: Due to some limitations, you cannot login simultaneously to multiple browser instances/tabs using SSO login, as only one session remains active while the other sessions expire.

Issue 36: DF489034: Intel(R) TXT configuration fails due to Virtualization technology dependency

If the current Virtualization Technology attribute setting is "Disabled" (Virtualization Technology is part of the Processor Settings group on the BIOS setup page); the Intel TXT attribute configuration fails on the Server Administrator user interface (System -> Main System Chassis -> BIOS -> Setup ->System Security.) To resolve this issue, configure Virtualization technology setting to "Enabled" and reconfigure the Intel (R) TXT attribute, if it is configurable.

Issue 37: DF549057: When an operating system is installed through USC, the BIOS attributes in Server Administrator are displayed as read-only. You can edit the BIOS attributes after 18 hours of the operating system installation.

Workaround: To enable editing of the Server Administrator BIOS attributes, launch Lifecycle Controller while booting.

Issue 38: DF552204: On Mozilla Firefox browsers (versions 10, 11 and 12), Server Administrator fails to launch if IPv6 address used.

This is a known issue. For more information, see https://bugzilla.mozilla.org/show_bug.cgi?id=633001.

Issues for Server Administrator Running on All Microsoft Windows Operating Systems

Issue 1: Execute all Server Administrator CLI commands from a 32-bit Windows command prompt. You can access the 32-bit command prompt by clicking "Start-> Programs-> Accessories-> Command Prompt" or by clicking "Start-> Run" and then typing "cmd.exe". Attempts to run the CLI commands from the DOS command "command.com" may generate unpredictable results.

Issue 2: The DSM Server Administrator Connection Service may hang on system startup if both Oracle and VERITAS Backup Exec are installed on the system. To manually start the DSM Server Administrator Connection Service on a system running Windows, click "Start-> Programs-> Administrative Tools-> Service", right-click "DSM Server Administrator Connections Services" and select "Start".

Issue 3: You may not have appropriate privileges on the Server Administrator GUI if:

1. You belong to an Active Directory group that is part of another group.
2. You try to launch Server Administrator using the desktop icon when single sign-on is enabled.

Issue 4 DF551365: Server Administrator does not display the IP Address for Network Adapters that are used for virtual machines

Description: In a Microsoft Hyper-V environment, the Server Administrator Network page may indicate network adapters that are connected to a network and display Ethernet statistics but, the IP address is displayed as 'Unknown'. This is because Hyper-V virtualizes adapters that are bonded to its virtual switch. The Server Administrator only discovers physical network adapters and displays their IP addresses that are fully-controlled by the operating system and not by hypervisors.

Issues for Server Administrator Running on Microsoft Windows 2003 Operating Systems

Issue 1: You can ignore the following warning message:

A provider, omprov, has been registered in the WMI namespace, Root\CIMV2\Dell, to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not impersonate user requests correctly.

This can be ignored as the Managed Object Format file used to register the provider ("omprov") states that the provider only reads the inventory data; it does not perform any functions on the server that require user impersonation.

Issue 2: When running Server Administrator, crypt32.dll errors may be written to the operating system Application Event log. This issue occurs due to the "Update Root Certificates" component, which is installed by default as part of Windows Server 2003 installation. For more information on this component and reasons for errors, see the following articles on the Microsoft website:

- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03mngd/04_s3cer.mspx"
- "http://support.microsoft.com/default.aspx?scid=kb;en-us;317541"

There are two options to avoid these errors from being written to the Event log:

- Uninstall the "Update Root certificates" component as described in the first knowledge base article mentioned above.

NOTE: This procedure may affect other programs as discussed in the article.

- Install the Server Administrator certificate as a trusted certificate.

NOTE: This procedure may still prompt you to accept the certificate when you log in to Server Administrator, but will prevent the crypt32 errors from being logged to the Event log.

Issues for Server Administrator running on Microsoft Windows 2008 Operating Systems

Issue 1: DF94201: Single sign-on may not work if Server Administrator is launched using the desktop icon.

If Server Administrator is launched using the desktop icon, Single Sign-on may not work if in the Internet Explorer, under "Tools" -> "Internet Options" -> "Security" -> "Custom Level", the "User Authentication Logon" option is set to "Prompt for user name and password".

To resolve this issue, perform the following steps:

1. Find and select "Tools" from the menu.
2. Select "Internet Options" and click the "Security" tab.
3. Click "Custom level" button and scroll down to "User Authentication".
4. Under "Logon", choose the option "Automatic logon with current user name and password". If Server Administrator is running in the "Local Intranet Zone", you may choose the option "Automatic log on only in Intranet zone" instead.
5. Click "Ok" to open dialog boxes to complete the setting.

Issue 2: DF103661: Microsoft Windows Server 2008 - Alert Action -> Execute Application

For security reasons, Microsoft Windows Server 2008 is configured to not allow interactive services. When a service is installed as an interactive service on Microsoft Windows Server 2008, the operating system logs an error message in the Windows System log about the service being marked as an interactive service.

When you use Server Administrator to configure Alert Actions for an event, you can specify the action to "execute an application". For interactive applications to be executed properly for an Alert Action, the DSM Server Administrator Data Manager Service must be configured as an interactive service. Examples of

interactive applications comprise applications with a Graphical User Interface (GUI) or that prompt users for input in some way such as the "pause" command in a batch file.

When Server Administrator is installed on Microsoft Windows Server 2008, the DSM Server Administrator Data Manager Service is installed as a non-interactive service, which means that it is configured for not interacting with the desktop directly. If an interactive application is executed for an Alert Action in this situation, the application is suspended awaiting input from the user, but the application interface/prompt is not visible to the user. The application interface/prompt is not visible even after the Interactive Services Detection service is started. For each execution of the interactive application, there is an entry for the application process in the "Processes" tab in Task Manager.

If you want to execute an interactive application for an Alert Action on Microsoft Windows Server 2008, you must configure the DSM Server Administrator Data Manager Service to be allowed to interact with the desktop. To allow interaction with the desktop, right-click on the DSM Server Administrator Data Manager Service in the Services control panel and select Properties. In the "Log On" tab, enable "Allow service to interact with desktop" and click OK.

Restart the DSM Server Administrator Data Manager Service for the change to be effective. When the DSM Server Administrator Data Manager Service is restarted with this change, the Service Control Manager logs the following message to the System log: "The DSM Server Administrator Data Manager Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly." This change allows the DSM Server Administrator Data Manager Service to execute interactive applications properly for an Alert Action. Also, make sure the Interactive Services Detection service is running, to see the interface/prompt displayed by the interactive application. Once these changes are made, the operating system displays the "Interactive services dialog detection" dialog box to provide access to the interactive application interface/prompt.

After upgrading Windows Server 2003 x64 to Windows Server 2008 x64 with Server Administrator installed, the application UI does not show all the expected instrumentation pages. The Server Administrator installation must be repaired.

Go to Start->Settings->Control panel->Add Remove Programs->Select "Change" on the Server Administrator installation and select the "Repair" option to correct the issue.

Issue 3: DF330800: Server Administrator Web server local user login fails on the Windows 2008 R2 Managed Node.

When a Windows 2008 R2 Managed Node is added to a domain, logging in from any Server Administrator Web Server to that Windows 2008 R2 Managed Node will fail with local user or local power-user credentials. Only the credentials of a local Administrator or Domain user will work, with a prerequisite that all required winrm configurations have been applied.

Issues for Server Administrator running on Red Hat Enterprise Linux Operating Systems

Issue 1: When starting Server Administrator from the Red Hat Enterprise Linux console, kernel log messages may appear. To avoid these messages, perform the following steps:

1. Edit the "/etc/sysconfig/syslog" file and modify KLOGD_OPTIONS to KLOGD_OPTIONS="-c 4".
2. Restart "syslog" by executing "/etc/init.d/syslog restart".

Issue 2: When using the Mozilla browser on Red Hat Enterprise Linux operating systems, the font and type size on the Server Administrator global navigation bar appear different from the default font and type size that application uses.

Issue 3: For systems running a supported Red Hat Enterprise Linux operating system, kernel driver messages such as "AAC_ChardevOpen" may be displayed in the console at the login prompt. These messages are displayed in the console when the driver initialization is delayed by the installation of Server Administrator services and can be ignored.

Issues for Remote Access

NOTE: The Remote Access Service is supported on xx1x systems only.

The following subsections list the currently known issues regarding implementation and operation of your RAC and the Remote Access Service in Server Administrator.

Issues for all Operating Systems

Issue 1: Server Administrator user interface and commands related to "local authentication enable" are not applicable for RAC firmware 3.20.

The Active Directory authentication feature replaces the "local operating system authentication" feature in this version of firmware. Due to this change, the following commands return errors:

- "racadm localauthenable"

- "omconfig rac authentication"

Issue 2: Due to fluctuations in the watchdog timer, the "Last Crash Screen" may not be captured when the Automatic System Recovery is set to a value of less than 30 seconds. To ensure correct functioning of the "Last Crash Screen" feature, set the System Reset Timer to at least 30 seconds.

Issue 3: DF132894: The cfgDNSServer1 and cfgDNSServer2 properties of group cfgLanNetworking may be set to identical values while swapping addresses. Some performance may be lost temporarily during the swapping. The cfgLanNetworking group is configured using the "racadm config" command.

Issue 4: The remote access controller uses FTP protocol to perform some of the Dell OpenManage commands. If a firewall is installed in the system, it may cause these commands to fail.

The following Server Administrator CLI commands use FTP protocol to communicate with the RAC:

"omconfig rac uploadcert"

"omconfig rac generatecert"

The following racadm commands use FTP protocol to communicate with the RAC:

"racadm sslcertupload"

"racadm sslcsrgen"

"racadm fwupdate"

Issue 5: If the RAC configuration is reset to factory defaults using the "racadm racresetcfg" command, the RAC configuration tab in Server Administrator does not reflect the reset configuration settings until the system reboots. Also, the RAC configuration page in Server Administrator cannot be used to make any configuration changes until the system reboots.

Issue 6: The RAC does not support local RAC user IDs with special characters. When adding a local RAC user, use only alphanumeric characters for the user name.

Issue 7: While the RAC is being reset, the Instrumentation Service cannot read sensor data for certain systems. As a result, the voltage, temperature, and other probes may not be visible on the Server Administrator home page until the RAC has completed resetting.

Issue 8: The RAC may not send traps when your system is locked up. To enable traps to be sent when the system is locked, configure the watchdog timer using the Server Administrator GUI. On the GUI, click the "Properties" tab and ensure that "Auto Recovery" is selected. The default value of the "Action On Hung Operating System Detection" setting is "None". "None" indicates that detection will not be performed.

Issue 9: RAC firmware 2.0 and higher does not support passwords with special characters (non-alphanumeric) only for RAC user IDs logging in using the Web-based interface (with Local RAC Authentication). You cannot log on to RAC, if you created RAC user IDs using previous versions of the firmware or using Server Administrator that is running version 2.0 firmware on the managed system.

Use one of these methods to correct this issue:

- Change your passwords before updating the firmware.
- Use the following CLI command to change the password:

"omconfig rac users username=xx userpassword=yy"

where "xx" is the original user ID and "yy" is the new password.

- Change the password through Server Administrator using the "User" tab. Make sure that the check box to change the password is checked. Enter a new password, and then enter it again to validate the change.
    - Use the racadm utility to change the password:

    "racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <usr_index> <new_pwd>"

    where <usr_index> is the index of the user database entry to be modified and <new_pwd> is the new password.

Issue 10: Depending on your network and proxy configurations and whether you are using Mozilla browser, you may need to enter the exact IP address of the RAC controller you are trying to access in the "No Proxy for" field of your browser.

Perform the following steps:

1. Open your Mozilla browser.
2. Click "Edit".
3. Click "Preferences".
4. Click "Advanced" in the left sidebar.
5. Click "Proxies" in the left sidebar.
6. Enter the RAC IP address in the "No Proxy for:" field.
7. Click "OK" and then close the browser.

Issue 11: If the out-of-band RAC user interface is spawned off from the Server Administrator home page with a Mozilla browser, strings with extended ASCII characters may not display correctly in certain languages. This issue occurs because the Server Administrator sets the browser UTF-8 character. To correct this issue, change the browser character coding to ISO-8859-1. For Japanese and Chinese, UTF-8 is the correct encoding for RAC pages.

Issue 12: To view the RAC Web-based interface when using Mozilla 1.6, you must configure your cookie settings to "Enable all cookies".

To enable all cookies, go to the menu options and click "Edit -> Preferences -> Privacy & Security -> Cookies", and then select "Enable all cookies". If you do not perform these steps, you cannot log on to the Web interface and a message appears indicating that your username and password are incorrect.

Issue 13: DF384362: "Redundancy Status" shows as "Not Applicable" in ESXi even when NICs are teamed.

On VMware ESXi systems, NIC teaming status may not show up in the Server Administrator network section. This is an expected behavior due to operating system limitation and has no functional impact to the system.

Issue 14: DF384061: Self-signed certificate does not enable the compatibility listener in Windows 2008 R2 managed node.

On a Windows 2008 R2 managed node, a valid CA signed certificate is required to create compatibility mode WinRM Listener. You cannot create a compatibility mode listener with a self-signed certificate.

Issue 15: DF165588: Blank page is displayed after the browser is refreshed using <F5> or by clicking the browser "Refresh" button.

Server Administrator UI may display a blank page after the browser is refreshed, using <F5> or by clicking the browser "Refresh" button in Internet Explorer Version 7.0. This is a known issue and Microsoft has provided an article and fix. The Knowledge Base article number is KB933006 and the fix is provided as security update 933566 (MS07-033):Cumulative Security Update for Internet Explorer.

Issue 16: DF319132: Set operation in Server Administrator is blocked if a single sign-on is used to log on

Internet Explorer 8 has a new security feature called "Loopback security check" which prevents NTLM-based authentication from the local machine. This feature blocks users from performing any set operation in Server Administrator if they are logged in using single sign-on (SSO), (clicking the Server Administrator desktop icon) on Internet Explorer 8.

Issue 17: DF380725: On IE or Firefox Web browsers, you cannot attach files to an e-mail if the filename contains non-ASCII letters.

To attach files to an e-mail, rename files to contain ASCII characters.

Issue 18: On Yx2x servers, Server Administrator displays the Embedded Systems Management (ESM) or hardware logs. However, when the maximum limit for number of logs that can be recorded is reached, the existing oldest logs are overwritten. But for Yx1x servers or below, when the maximum limit is reached, the information logging is stopped.

Issue 19: DF523827: On Citrix XenServer 6.0, if the Alert on Console alert action is configured from the Server Administrator CLI or GUI, the alert message may not be displayed in a readable format.

Issue 20: DF530134: On VMware ESX 4.1 managed node, while USB arbitration service is running, Inventory Collector does not respond while stopping the Server Administrator services.

To resolve this issue, stop the USB arbitration service and run the Inventory Collector.

To stop the USB arbitration service:

1. Run the “ps aux|grep usb” command to check if the USB arbitration service is running.
2. Run the “chkconfig usbarbitrator off” command to prevent the USB arbitration service from starting during boot.
3. After the USB arbitrator service is stopped, reboot the server to allow the Inventory collector to run.

Issue 21: DF520449: On all versions of the ESX, the following USB connection error messages are generated. These messages can be ignored.

The following shows a typical message:

Vendor: iDRAC Model: MAS022 Rev: 1.00

Type: Direct-Access ANSI SCSI revision: 02

Vendor: iDRAC Model: SECUPD Rev: 0329

Type: Direct-Access ANSI SCSI revision: 02

(520449)

Issue 22: DF531509: The setup and/or system password configuration from Server Administrator GUI or CLI is successful, but the password is displayed as blank instead of asterisk (*) on the F2 BIOS page.

Issue 23: DF532055: From Windows Server 2008 R2 SP1, when an administrator manages Red Hat Enterprise Linux 6.1 (64-bit) or 5.7 (32 and 64-bit) operating systems, Server Administrator reports connection error intermittently.

Workaround: Perform the following settings and manage the remote system from webserver.

1. Configure TCP Chimney offload to disable state by running following command:

   netsh int tcp set global chimney=disabled

2. Configure RSS (Receive Side Scaling) to disable state by running following command:

   netsh int tcp set global rss=disabled

3. Configure NetDMA to disable state by running following command:

   netsh int tcp set global NetDMA=disabled

Known Limitations and Workarounds for Storage Management Service

Issue 1: DF529750: Inconsistent reporting between iDRAC7 and Storage Management regarding HBA adapter batteries.

Description: “Battery Status reported by Storage Management is inconsistent with the one reported by iDRAC7 interfaces (for example: iDRAC7 Web interface, RACADM and so on) for PERC 8 controllers when a Learn Cycle is in progress.

Storage Management reports the Battery status as Warning while iDRAC7 interfaces report the Battery status as ‘ok’.”

Workaround: Warning status is transient and does not warrant any action by the user. Battery status changes to ‘ok’ once the Learn cycle is complete

Recommendation: Ignore the warning

Issue 2: View slot occupancy report shows 4 HDD slots on backplanes with just two HDD slots for any server.

Issue 3: Physical disk clear operation is not available on PERC 8 family of controllers.

Issue 4: DF489665: Max Config: OM on ESXi 4.1 U2 Experiences Timeouts and very poor performance.

Description: When using ESXi with a large number of directly attached disk drives, delays or timeouts in OpenManage Storage Manager may be encountered during VD creation. PowerEdge servers support up to two RAID controllers. Each array controller supports up to eight MD1200/1220 enclosures. In the case of Server Administrator 7.0 and earlier versions with ESXi, max direct attach storage configs will timeout during VD creation. To create a VD using ESXi it could take up to 12 minutes to successfully build the XML output for up to 200 drives. If more than 200 drives exist in the direct attach enclosures you may encounter a timeout error during VD creation. "The action performed has failed."

Solution: Improvements are being investigated for the OM7.1 timeframe in Q1 of 2012. Until then the number of direct attached drives must be reduced to below 200 if the timeout is encountered. Please allow sufficient time for the VD to be created.

Issue 5: Physical disk properties such as Manufacture day, Manufacture week, and Manufacture year are available for SAS drives only.

Issue 6: Dell OpenManage Server Administrator Storage Management 7.0 does not support PERC 4 controllers and earlier versions on ESXi 4.x, ESXi 5.x, ESX 4.x, and all 64-bit Linux Operating System.

Issue 7: Hot removal of enclosure is not supported in Storage Management. It may result in unpredictable errors, such as stopping Storage Management service.

Issue 8: Creating many sliced span virtual disks using the spun-down drives through the command line or GUI result may be delayed.

Workaround: After creating one sliced span virtual disk, wait for some time to create the next sliced span virtual disk.

Issue 9: In ESX4 Classic, 'deprecated SCSI ioctl' message is displayed on the console.

Description: In VMware ESX 4.0 Classic system, the following warning message(s) is displayed on the console: “Program dsm_sa_datamgrd is using the deprecated SCSI ioctl, Please convert it to SG_IO.” This is a kernel warning message displayed when storage operations are in progress. This is only a deprecation warning and not an indication of a failing operation.

Workaround: Reduce the kernel logging level. By default, VMware ESX kernel logging level is set to ‘6’ to print all the kernel messages with severity higher than ‘information.’ Reduce it to ‘4’, so that messages with severity, ‘error,’ and above get printed to the console.

To do this, execute the following command as a ‘root’ user:

/proc/sys/kernel/printk.

Issue 10: A Security Key Identifier can contain numerals, lowercase alphabets, uppercase alphabets, non-alphanumeric characters (except space), or a combination of any of these.

NOTE: If you have used the special characters ”/” (forward slash) or “ ‘ ” (single quote) in the Security Key Identifier, they are displayed as “_” (underscore) on the Change Security Key page and Import Secured Foreign Configurations page. This is applicable only to the Security Key Identifier and not to the Passphrase.

Issue 11: If Storage Management displays a path failure message for a Logical Connector after a reboot, use the "Clear Redundant Path View", provided in the "Change Controller Properties" controller task, and restart the system.

NOTE: Use this command only if you have intentionally removed the multipath connection while rebooting the system.

Issue 12: In the VMware ESX 4.x and ESX 5.x environment, when you create a virtual disk using Storage Management, you may see an error message "The task failed to complete: The create virtual disk task was

successful but the operating system may not be aware of the new virtual disk." However, the virtual disk is available for all operations on rebooting the system.

Issue 13: Patrol Read is not supported on SSD media. The Patrol Read feature fails for any controller that has SSD media on a virtual disk.

Issue 14: Hot plug of enclosures takes time to enumerate the enclosure and its components. During this time, there will be a delay in the response time of tasks, such as displaying the physical disks on the physical disk page and in the virtual disk selection page.

Issue 15: All virtual disks from the SAS/iR controller display the name "IR Virtual Disk" on the "Preview" page. On successful import, another name is assigned to these virtual disks and the "IR Virtual Disk" name is not displayed on the "Preview" page.

Issue 16: Storage Management supports assignment of only one dedicated hot spare for a virtual disk on SCSI Controllers.

Issue 17: Storage Management does not permit connecting the first enclosure in single path and attaching the subsequent enclosures in multipath. All enclosures must be connected in multipath to enable the multipath view.

Issue 18: An error message may not appear when "Import Foreign Configuration" task is not successful.

Description: The "Import Foreign Configuration" task can only import virtual disks that have consistent data. A virtual disk with inconsistent data cannot be imported. When importing multiple virtual disks in a single operation, however, the "Import Foreign Configuration" task may report successful completion even when inconsistent virtual disks are present and have not been imported successfully.

Solution: If the "Import Foreign Configuration" task is unable to import an inconsistent virtual disk, then the physical disks that belong to the virtual disk continue to display a "Foreign" state after the "Import Foreign Configuration" task completes. In this case, repeat the "Import Foreign Configuration" task until one of the following occurs:

- There are no longer any physical disks in "Foreign" state after the "Import Foreign Configuration" task completes.
- You receive an error stating that the "Import Foreign Configuration" task has not completed successfully. This error indicates that there are no longer any consistent virtual disks available to be imported. Therefore, all virtual disks that are not imported are inconsistent and you can either perform a "Clear Foreign Configuration" to remove the virtual disks or remove the physical disks from the controller.

Issue 19: DF60696: Storage Management responds slowly when using Internet Explorer 7.x, 8.x on a system with mixed SAS and SATA physical disks.

Description: When using the "Create Virtual Disk" wizard from the Storage Management graphical user interface (GUI), you may notice decreased performance when using Internet Explorer 7.x, 8.x on a system with multiple Dell PowerVault(TM) MD1000 storage enclosures that are heavily populated with mixed SAS and SATA physical disks.

Solution: Use a supported browser other than Internet Explorer 7.x, 8.x or use the Storage Management command line interface (CLI) to create the virtual disk.

See the Server Administrator readme for information on supported browsers. See the Storage Management online help or the "Server Administrator Command Line Interface User's Guide" for information on using the Storage Management CLI.

Issue 20: DF152362: Storage Management may not display controllers installed with the Service and Diagnostics utility.

Description: Storage Management may not recognize devices that are installed after Storage Management is already running.

Solution: If Storage Management does not recognize a newly-added device and this problem has not been corrected with a Global Rescan, then reboot the system.

Issue 21: DF120475: Storage Management SNMP traps are not filtered by Server Administrator.

Description: Server Administrator allows you to filter SNMP traps that you do not want to receive. To implement SNMP trap filtering, select the "System" tree-> "Alert Management" tab-> "SNMP Traps" subtab. The "SNMP Traps" subtab has options for enabling and disabling SNMP traps based on severity or the component that generates the trap. Even when the SNMP traps are disabled, Storage Management generates SNMP traps.

Solution: SNMP trap filtering will be provided in a future release of Storage Management.

Issue 22: When issuing certain "omconfig storage" CLI commands with "Power User" privileges, the "Error! User has insufficient privileges to run command: omconfig" message may be displayed. You must be logged on as an Administrator to perform these actions.

Issue 23: Invalid "Format and Check Consistency" options are displayed for regenerating a virtual disk.

When a physical disk in a virtual disk is rebuilding, the virtual disk changes to a "Regenerating" state. The Format and Check Consistency operations should not be performed on a virtual disk that is in a Regenerating" state. However, the task drop-down menu for a "Regenerating" RAID 1-concatenated virtual disk may display the "Format and Check Consistency" options.

Issue 24: If a physical disk in a RAID 1-concatenated virtual disk fails, the virtual disk is in a "Degraded" state.

Rebooting the system may cause the virtual disk to change to a "Failed" state, but the virtual disk is still fully-operational and can be restored to "OK" status once a functional physical disk is added back to the RAID-1 set.

Issue 25: Using the Storage Management Service "Advanced Create VDisk Wizard" may occasionally result in a vertical scrollbar of less than normal width. If this occurs, resizing the Server Administrator window causes the vertical scrollbar to be redrawn correctly.

Issue 26: Using the GUI, if a virtual disk is renamed to a name containing multiple blank and consecutive spaces, the name is truncated to a single space after "Apply" is clicked.

Issue 27: When the "Open in a New Window" option is selected in the Storage Management Service Advanced Create VDisk Wizard, the current page is opened in a new window, rather than launching the selected option.

Issue 28: If a physical disk in a RAID 1-concatenated virtual disk fails, the virtual disk is in a "Degraded" state. The Check Consistency operation should not be performed on a virtual disk while it is in a degraded state. However, the task drop-down menu for a degraded RAID 1-concatenated virtual disk may display the "Check Consistency" option. Do not perform a consistency check until appropriate actions are performed to restore the virtual disk.

Issue 29: With Chinese or Japanese language browser settings, using the Storage Management Service Advanced Create VDisk Wizard may occasionally result in text overflowing to the bottom of the side-by-side blue text boxes.

Firmware for PERC controllers

Firmware for PERC 4e/DC,PERC 5/E, PERC 5/i Integrated, PERC 5/i Adapter, SAS 5/iR Integrated, SAS 5/iR Adapter, SAS 5/i Integrated, SAS 5/E Adapter, PERC 6/E Adapter, PERC 6/i Integrated, PERC 6/i Adapter, SAS 6/iR Integrated, SAS 6/iR Adapter,SAS 6/int. Modular, LSI 1020, LSI 1030, PERC H800 Adapter, PERC H700 Integrated, PERC H700 Adapter, PERC H700 Modular, PERC H200 Adapter, PERC H200 Integrated,PERC H200 Modular, 6Gbps SAS HBA Controllers, PERC H310 Adapter, PERC H310 Mini Blades, PERC H310 Mini Monolithic, PERC H710 Adapter, PERC H710 Mini Blades, PERC H710 Mini Monolithic, PERC H710P Adapter, PERC H710P Mini Blades, PERC H710P Mini Monolithic, and PERC H810 Adapter Controllers.

Controller	Firmware/BIOS
PERC 4e/DC	5B2D
PERC 5/E	5.2.2-0076
PERC 5/i Integrated	5.2.3-0074
PERC 5/i Adapter	5.2.3-0074
SAS 5/iR Integrated	00.10.51.00/06.12.05.00
SAS 5/iR Adapter	00.10.51.00/06.12.05.00
SAS 5/i Integrated	00.10.51.00/06.12.05.00
SAS 5/E Adapter	00.10.51.00/ 06.12.05.00
PERC 6/E Adapter	6.3.0-0001
PERC 6/i Integrated	6.3.0-0001
PERC 6/i Adapter	6.3.0-0001
SAS 6/iR Integrated	00.25.47.00/06.22.03.00

SAS 6/iR Adapter	00.25.47.00/06.22.03.00
SAS 6/int. Modular	00.25.47.00/ 06.22.03.00
PERC H800 Adapter	12.10.2-0004
PERC H700 Integrated	12.10.2-0004
PERC H700 Adapter	12.10.2-0004
PERC H700 Modular	12.10.2-0004
PERC H200 Adapter	07.03.05.00
PERC H200 Integrated	07.03.05.00
PERC H200 Modular	07.03.05.00
PERC H200 Embedded	07.03.05.00
6Gbps SAS HBA	07.03.05.00
PERC H310 Adapter	20.10.1-0084
PERC H310 Mini Monolithic	20.10.1-0084
PERC H310 Mini Blades	20.10.1-0084
PERC H710 Adapter	21.0.1-0131
PERC H710 Mini Blades	21.0.1-0132
PERC H710 Mini Monolithic	21.0.1-0132
PERC H710P Adapter	21.0.1-0132
PERC H710P Mini Blades	21.0.1-0132
PERC H710P Mini Monolithic	21.0.1-0132
PERC H810 Adapter	21.0.1-0132
PERC S110	3.0.0.0139
PERC S100	2.0.0-0162
PERC S300	2.0.0-0162

Windows Drivers for PERC Controllers

Windows Drivers for PERC 4e/DC, PERC 5/E, PERC 5/i Integrated, PERC 5/i Adapter, SAS 5/iR Integrated, SAS 5/iR Adapter, SAS 5/i Integrated, SAS 5/E Adapter, PERC 6/E Adapter, PERC 6/i Integrated, PERC 6/i Adapter, SAS 6/iR Integrated, SAS 6/iR Adapter, SAS 6/int. Modular, LSI 1020, LSI 1030, PERC H800 Adapter, PERC H700 Integrated, PERC H700 Adapter, PERC H700 Modular, PERC H200 Adapter, PERC H200 Integrated, PERC H200 Modular, 6Gbps SAS HBA, PERC H310 Adapter, PERC H310 Mini Blades, PERC H310 Mini Monolithic, PERC H710 Adapter, PERC H710 Mini Blades, PERC H710 Mini Monolithic, PERC H710P Adapter,PERC H710P Mini Blades, PERC H710P Mini Monolithic, and PERC H810 Adapter Controllers

Controller	Windows Server 2008 32-bit Driver	Windows Server 2008 64-bit Driver	Windows Server 2008 R2 Driver
PERC 4e/DC	Native	Native	Native
PERC 5/E	2.24.0.32	2.24.0.64	2.24.0.64
PERC 5/i Integrated	2.24.0.32	2.24.0.64	2.24.0.64
PERC 5/i Adapter	2.24.0.32	2.24.0.64	2.24.0.64
SAS 5/iR Integrated	1.28.03.01	1.28.03.01	1.28.03.01
SAS 5/iR Adapter	1.28.03.01	1.28.03.01	1.28.03.01
SAS 5/i Integrated	1.28.03.01	1.28.03.01	1.28.03.01
SAS 5/E Adapter	1.28.03.01	1.28.03.01	1.28.03.01
PERC 6/E Adapter	2.24.0.32	2.24.0.64	2.24.0.64
PERC 6/i Integrated	2.24.0.32	2.24.0.64	2.24.0.64
PERC 6/i Adapter	2.24.0.32	2.24.0.64	2.24.0.64
SAS 6/iR Integrated	1.28.03.01	1.28.03.01	1.28.03.01
SAS 6/iR Adapter	1.28.03.01	1.28.03.01	1.28.03.01

SAS 6/iR Modular	1.28.03.01	1.28.03.01	1.28.03.01
LSI 1020 on a PowerEdge 1600SC	Not Applicable	Not Applicable	Not Applicable
LSI 1030 on a PowerEdge 1750	Not Applicable	Not Applicable	Not Applicable
PERC H800 Adapter	4.31.1.32	4.31.1.64	4.31.1.64
PERC H700 Integrated	4.31.1.32	4.31.1.64	4.31.1.64
PERC H700 Adapter	4.31.1.32	4.31.1.64	4.31.1.64
PERC H700 Modular	4.31.1.32	4.31.1.64	4.31.1.64
PERC H200 Adapter	2.0.12.10	2.0.12.10	2.0.12.10
PERC H200 Integrated	2.0.12.10	2.0.12.10	2.0.12.10
PERC H200 Modular	2.0.12.10	2.0.12.10	2.0.12.10
6Gbps HBA	2.0.12.10	2.0.12.10	2.0.12.10
PERC H310 Adapter	5.1.90.32	5.1.90.64	5.1.90.64
PERC H310 Mini Monolithic	5.1.90.32	5.1.90.64	5.1.90.64
PERC H310 Mini Blades	5.1.90.32	5.1.90.64	5.1.90.64
PERC H710 Adapter	5.1.90.32	5.1.90.64	5.1.90.64
PERC H710 Mini Blades	5.1.90.32	5.1.90.64	5.1.90.64

PERC H710 Mini Monolithic	5.1.90.32	5.1.90.64	5.1.90.64
PERC H710P Adapter	5.1.90.32	5.1.90.64	5.1.90.64
PERC H710P Mini Blades	5.1.90.32	5.1.90.64	5.1.90.64
PERC H710P Mini Monolithic	5.1.90.32	5.1.90.64	5.1.90.64
PERC H810 Adapter	5.1.90.32	5.1.90.64	5.1.90.64
PERC S100	2.0.0-0162	2.0.0-0162	2.0.0-0162
PERC S300	2.0.0-0162	2.0.0-0162	2.0.0-0162
PERC S110	3.0.0.0134	3.0.0.0134	3.0.0.0134

Linux Drivers for PERC Controllers

Linux Drivers for PERC 4e/DC,PERC 5/E, PERC 5/i Integrated, PERC 5/i Adapter, SAS 5/iR Integrated, SAS 5/iR Adapter, SAS 5/i Integrated, SAS 5/E Adapter, PERC 6/E Adapter, PERC 6/i Integrated, PERC 6/i Adapter, SAS 6/iR Integrated, SAS 6/iR Adapter, SAS 6/int. Modular, LSI 1020, LSI 1030, PERC H800 Adapter, PERC H700 Integrated, PERC H700 Adapter, PERC H700 Modular, PERC H200 Adapter,PERC H200 Integrated, PERC H200 Modular, 6Gbps SAS HBA Controllers, PERC H310 Adapter, PERC H310 Mini Blades, PERC H310 Mini Monolithic, PERC H710 Adapter, PERC H710 Mini Blades, PERC H710 Mini Monolithic, PERC H710P Adapter, PERC H710P Mini Blades, PERC H710P Mini Monolithic, and PERC H810 Adapter Controllers

Controller	Red Hat Linux Driver 6.1	Red Hat Linux Driver 5.7	SUSE Linux 11 SP2 64-bit Driver	SUSE Linux 10 64-bit Driver
PERC 4e/DC	Not Applicable	Native	Native	Native
PERC 5/E	Native	Native	Native	Native
PERC 5/i Integrated	Native	Native	Native	Native
PERC 5/i Adapter	Native	Native	Native	Native
SAS 5/iR Integrated	Native	4.00.38.02-3	Native	Native
SAS 5/iR Adapter	Native	4.00.38.02-3	Native	Native
SAS 5/i Integrated	Native	4.00.38.02-3	Native	Native

SAS 5/E Adapter	Native	4.00.38.02-3	Native	Native
PERC 6/E Adapter	Native	Native	Native	Native
PERC 6/i Integrated	Native	Native	Native	Native
PERC 6/i Adapter	Native	Native	Native	Native
SAS 6/iR Integrated	Native	4.00.38.02-3	Native	Native
SAS 6/iR Adapter	Native	4.00.38.02-3	Native	Native
SAS 6/int. Modular	Native	4.00.38.02-3	Native	Native
LSI 1020 on a PowerEdge 1600SC	Native	Native	Native	Not Applicable
LSI 1030 on a PowerEdge 1750	Native	Native	Native	Not Applicable
PERC H800 Adapter	Native	00.00.04.27	Native	Native
PERC H700 Integrated	Native	00.00.04.27	Native	Native
PERC H700 Adapter	Native	00.00.04.27	Native	Native
PERC H700 Modular	Native	00.00.04.27	Native	Native
PERC H200 Adapter	Native	02.00.00.00	Native	Native
PERC H200 Integrated	Native	02.00.00.00	Native	Native
PERC H200 Modular	Native	02.00.00.00	Native	Native
6Gbps SAS HBA	Native	02.00.00.00	Native	Native
PERC H310 Adapter	Native	00.00.05.38	Native	Native
PERC H310 Mini Monolithic	Native	00.00.05.38	Native	Native

PERC H310 Mini Blades	Native	00.00.05.38	Native	Native
PERC H710 Adapter	Native	00.00.05.38	Native	Native
PERC H710 Mini Blades	Native	00.00.05.38	Native	Native
PERC H710 Mini Monolithic	Native	00.00.05.38	Native	Native
PERC H710P Adapter	Native	00.00.05.38	Native	Native
PERC H710P Blades	Native	00.00.05.38	Native	Native
PERC H710P Mini Monolithic	Native	00.00.05.38	Native	Native
PERC H810 Adapter	Native	00.00.05.38	Native	Native
PERC S100	Not Supported	Not Supported	Not Supported	Not Supported
PERC S300	Not Supported	Not Supported	Not Supported	Not Supported
PERC S110	Not Supported	Not Supported	Not Supported	Not Supported

PREREQUISITE DRIVERS AND FIRMWARE

Storage Management does not display controllers and their features on systems that do not meet the driver and firmware requirements. At Storage Management runtime, you can determine whether the system meets the firmware requirement or not, by checking the application log files for notifications on outdated firmware. At runtime, On SCSI controllers, Storage Management displays the firmware version at runtime while on SAS controllers it displays the firmware and driver versions.

Documentation Errata

DF551575: Online Help needs to be updated for Shutdown Feature

Description: In the Power Cycle section of online help, the note states that “Power cycle feature is not available for ESX 4.1 Classic”. But Power Cycle feature is not supported for ESXi5.x as well.

Resolution: The note needs to be modified as “ Power cycle feature is not available for ESX 4.1 Classic and ESXi 5.x.”

Versions Affected: 7.1

Global Support

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

For information on documentation support, visit **support.dell.com/manuals.** On the **Manuals** page, click **Software** ->**Systems Management.** Click on the specific product on the right -side to access the documents.

2012 – 06 **Rev. A00**