

# **Server Administrator**

**7.3.2**

Release Notes

# Release Type and Definition

## Server Administrator

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

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

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

You can access the documentation from the Systems Management Tools and Documentation DVD or from "[dell.com/support/manuals](http://dell.com/support/manuals)".

### Version

7.3.2

### Release Date

November 2013

### Previous Version

7.3.1

## Important Release Information

The Release Notes is the only document updated for this release. For all other documents, see the 7.3 version of the documents at <http://www.dell.com/support/Manuals/us/en/555/Product/dell-opnmang-srvr-admin-v7.3>

## Importance

RECOMMENDED: It is recommended to apply this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).

## Platform(s) Affected

For a complete list of supported Dell PowerEdge systems and supported Operating systems, see the Dell Systems Software Support Matrix available in the required version of OpenManage Software at [dell.com/openmanagemanuals](http://dell.com/openmanagemanuals).

# What is Supported

## 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

- Supported operating system and web browser.
- TCP/IP connection on the managed system and the remote system to facilitate remote system management.
- Supported systems management protocol standard. 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. For more information on the software and hardware requirements, see the relevant Remote Access Controller User's Guide.
- 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 Server Administrator to be installed on the managed system. For more information on the software and hardware requirements, see the Server Administrator Storage Management User's Guide.
- Microsoft Software Installer (MSI) version 3.1 or later.

NOTE: Server Administrator software detects the MSI version on your system. If the version is earlier 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.

# What's New

Added support for the following operating systems:

- Red Hat Enterprise Linux 5.9 (32-bit and 64-bit)
- Red Hat Enterprise Linux 6.4 (64-bit)
- Microsoft Windows Server 2012 Essentials
- VMware ESXi 5.1 U1
- VMware ESXi 5.0 U2
- Citrix XenServer 6.2

NOTE: Microsoft Windows 2003 is not supported on 12G systems.

Deprecated the following operating systems:

- Red Hat Enterprise Linux 6.3
- Red Hat Enterprise Linux 5.8

New Features:

Server Administrator:

- Security fixes and enhancements
  - Fixed CVE-2012-6272, CSRF, XSS and generic path manipulation
  - Upgraded the JRE to version 1.7 update 21
  - Upgraded the Apache Tomcat to version 7.0.39
- Added support for Google Chrome version 21 and 22
- Added support for Safari 5.1.7 browser on Apple Mac OSX
- Added support for the following Network Interface Cards (NICs):
- Broadcom 57840S Quad Port 10G SFP+ Rack NDC
- Broadcom 57840S-k Quad Port 10GbE Blade KR NDC
- On 12G systems with iDRAC7 1.30.30 and later, you can set Platform Event Destination as IPv4, IPv6, or FQDN

Storage Management Service:

- PCIe SSD support for ESXi 5.1 U1
- Remaining Rated Write Endurance status for SAS and SATA SSD attached to a PERC8
- Fluid Cache for DAS support on Red Hat Enterprise Linux6 .4 and Novell SUSE Linux Enterprise Server 11 SP2 for PERC H810,H710 Adapter,H710P,and H710 Mini on the following systems:
  - R720
  - R820
  - R620
  - T620

For a complete list of supported operating systems and platforms, see the latest Systems Management - Software Support Matrix available on the support site.

## Fixes

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

- BITS040148 Migrated DF418159 Tables have improper formatting in multiple Server Administrator pages.
- BITS040169 Migrated DF504576 OM7.0: Hide toggle buttons when Boot/HDD/UEFI sequence is read only
- BITS040176 Migrated DF523852 Maximum failure threshold value in temperature slot is overlapping in Server Administrator GUI.
- BITS040177 Migrated DF526596 Purchase date should not be greater than till date.
- BITS040218 Migrated DF532466 Index page, Alphabet Links are not working in Mozilla browser
- BITS044716 Search in Online Help is not functioning properly
- BITS044914 key signing algorithm is not saved after upgrade from OM71 to OM7101
- BITS045027 OM72: OMI: Error message while Uninstalling of Server Administrator in W2K8 x86 with FF15.

# Important Notes

## Notes for Server Administrator

On 12G systems with iDRAC7 1.30.30 and later versions, you can set the Platform Event Destination as IPv4, IPv6, or FQDN.

## Notes for Instrumentation Service

- On 11G 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), the conflict prevents the BIOS configuration updates (at system reboot).

- On certain systems, user-defined thresholds set under Server Administrator become the default thresholds after uninstalling Server Administrator.
- If you change the threshold value of a probe on certain systems, running Server Administrator, and then uninstall Server Administrator, 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: Systems - Management Base Driver (dcdbas) and BIOS Update Driver (dell\_rbu).

- Server Administrator uses these drivers to perform the 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.
- CMC USB ports attached with blade is not enumerated by Server Administrator.

## 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 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.
- On systems prior to 12G, Server Administrator slot page displays iDRAC information, but on 12G systems, the slot page does not display any iDRAC7 information.

## Known Issues

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

### Issues for Server Administrator running on VMware ESX Operating Systems

- DF374857: Connection service has to be restarted for an Active Directory user login. After adding a VMware ESX 4.1 operating system to the Active Directory domain, an Active Directory user must do the following:
  - To log on to Server Administrator using the VMware ESX 4.1 operating system as Server Administrator, restart the DSM SA Connection Service.
  - To log on to the Remote Node using the VMware ESX 4.1 operating system as Remote Enablement Agent, wait for about five minutes for the 'sfcdbd' to add permission for the new user.
- DF354388: Remote Server Administrator Web Server connection to managed node hangs, if a redundant virtual disk containing syslog dumps fails.
  - 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.
- 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>.
- BITS072069: On ESX/ESXi Operating Systems, Server Administrator configuration changes are not persisted after an unclean shutdown.
  - If the server abruptly reboots, configuration changes to Server Administrator Preferences are not retained on VMware ESX or ESXi operating systems. Once an hour, VMware runs a scheduled backup to update any configuration changes to the installed applications (VIBs). For more information, refer to the Knowledge Base article at - <http://Kb.vmware.com/kb/2001780>

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

- DF275424 and DF332775: Domain users unable to login to Windows MN from Linux Web Server.
  - Negotiate authentication is not supported while remotely managing a Windows-based managed node from a Linux-based Server Administrator Web server. 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 is displayed.
  - You can manage a Windows/Linux- based managed system remotely from a Windows-based Server Administrator Web server.

## Issues for Server Administrator Running on All Supported Operating Systems

- On Dell PowerEdge T110 II systems, the following Server Administrator bios settings are not consistent with the F2 bios setup settings:
  - Watchdog timer: Server Administrator displays the option as disabled, but F2 bios allows to change the setting.
  - Embedded Video Controller: Server Administrator provides options to enable or disable, but in F2 bios the option is greyed out.
  - TPM Security: Server Administrator does not allow to change the settings, but F2 bios allows to change the settings.
  - System Profile State: Server Administrator does not allow to make changes, but F2 bios allows to make the changes.
  - Memory Testing: Server Administrator does not support this feature, but F2 bios supports this feature.
  - SRIOV option: Server Administrator does not display this information, but F2 bios displays this feature.
- Due to non-availability of resources, inventory collector 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.
- After installing Server Administrator from the command prompt, typing an "omreport" or "mconfig" command from the same prompt can cause an error. Open a new command prompt window and type commands.
- 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
- After a "Reset to Defaults" operation of the Integrated 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.
- While typing the command "omreport system version -outc <filename>", ensure that you specify an absolute path name for the output file; else, the output file is empty. For example, c:\out.txt.
- Typing "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.
- 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.

- 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" is displayed, modify your command into several simpler commands. Each command should change only one setting.
- 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.
- Log files saved from Server Administrator are saved in zip format. It is recommended that you open this zip file using WinZip. Windows Server 2003 or Windows XP embedded "Compressed (zipped) Folder" utility is not recommended.
- After configuring BIOS settings on certain systems, a second reboot may be required for the Server Administrator to display the updated BIOS settings properly.
- 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 fix 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:

- Type: omconfig system webserver action=stop
  - Locate the "keystore.db.bak" file. The default path is "C:\program files\dell\SysMgt\apache-tomcat\conf".
  - Copy "keystore.db.bak" to "keystore.db".
  - Type: omconfig system webserver action=start
- A temperature drop below a minimum failure threshold does not cause a system reset even if this alert action is set.
- 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.
- 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.
- 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.
- 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.
- 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.
- If Internet Explorer prompts you to "Work Offline", "Connect", or "Try Again", always select "Connect" or "Try Again". Do not select "Work Offline".
- 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.



- On some systems, temperature probe values and settings are only supported for whole degrees, not tenths of a degree. On those systems, setting a fractional value for the minimum warning temperature threshold results in the set value being rounded off to the next whole number value. This behavior may cause the minimum warning threshold to have the same value as the minimum failure threshold.
- 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.
- If you change the operating system Time Zone to a new time zone, 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.
- 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, system reboot) 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.

- 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>

- 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.
- DF 172125: Power monitoring probes are displayed 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.
- 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.
- The selection of default option for front panel LCD in Server Administrator displays the Model Name whereas the default is Service Tag on the physical LCD.
- 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.

- 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 updated 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.
- DF315853: Some Server Administrator CLI commands functions properly only when run from the elevated console window. It is recommended that you use the elevated console for running the CLI.
- Due to some limitations, you cannot log on simultaneously to multiple browser instances/tabs using SSO login, as only one session remains active while the other sessions expire.
- DF489034: Intel 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 TXT attribute, if it is configurable.
- 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 18 hours after the operating system installation.  
Workaround: To enable editing of the Server Administrator BIOS attributes, launch Lifecycle Controller while booting.
- DF552204: On Mozilla Firefox browsers (versions 10, 11 and 12), Server Administrator fails to launch if IPv6 address is used.  
This is a known issue. For more information, see [https://bugzilla.mozilla.org/show\\_bug.cgi?id=633001](https://bugzilla.mozilla.org/show_bug.cgi?id=633001).
- BITS04016: In case of Boot/HDD/UEFI sequence, if they are read-only, then toggle buttons (+ and -) and submit button are not visible. On BIOS setup page, dependencies may exist between the various attributes for Bios settings. Setting an attribute value may change the state of the dependent attributes to non-editable or editable. For example, changing the Boot Mode to UEFI from the Boot Settings page does not allow you to configure the Boot or Hard-Disk Drive Sequence in the BIOS Boot Settings page. When the page is non-editable, the toggle buttons on the page allows toggling the order of the boot sequence. However, settings cannot be configured since "Apply" button will not available to submit the settings.
- BITS050574: On 11G and 12G systems running the Linux OS, the omreport system summary command displays "RAC Command Interface" as 7.1.0. "RAC Command Interface" is a DRAC4 RPM and its version is 7.1. It is installed as a dependent package for iDRAC6 and iDRAC7 Command Interface packages.

- If a new certificate imported to Server Administrator is not active after restarting the Web server, restore the previous certificate.

To restore the previous certificate, do the following:

1. Stop the Web server.
2. Perform one of the following as applicable:

On systems running Windows:

- Delete the file keystore.db at <installed directory>\Dell\SysMgt\apache-tomcat\conf\
- Rename the file keystore.db.bak at <installed directory>\Dell\SysMgt\apache-tomcat\conf\ to keystore.db

On systems running Linux:

- For 32-bit OS
  - Delete the keystore.db file at /opt/dell/srvadmin/lib/openmanage/apache-tomcat/conf
  - Rename the keystore.db.bak at /opt/dell/srvadmin/lib/openmanage/apache-tomcat/conf to keystore.db
- For 64-bit OS
  - Delete the keystore.db file at /opt/dell/srvadmin/lib64/openmanage/apache-tomcat/conf
  - Rename the keystore.db.bak at /opt/dell/srvadmin/lib64/openmanage/apache-tomcat/conf to keystore.db

3. Start the Web server.

- BITS078118: On 12G systems with specific versions of iDRAC, you cannot set the platform event alert actions (reboot, shut down, and so on) through Server Administrator. Set the alert actions for the events through iDRAC GUI.

### Issues for Server Administrator Running on All Microsoft Windows Operating Systems

- 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.
- 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".
- You may not have appropriate privileges on the Server Administrator GUI if you:
  - Belong to an Active Directory group that is part of another group.
  - Try to launch Server Administrator using the desktop icon when single sign-on is enabled.
- Broadcom architecture has a split driver implementation - evbdx.sys and bxnd60x.sys.
  - evbdx.sys is the Virtual Bus Driver (VBD); also called the Base Driver
  - bxnd60x.sys is the driver for the Broadcom NDIS device.

Microsoft Device Manager reports both the drivers, but Server Administrator displays only the driver details specific to the VBD device.

- BITS080169: Documentation for Power Supply alerts mentions only AC power supply, but the alerts are valid for both AC and DC power supplies.

- BITS054513: On a system running Windows, while running CLI commands using telnet from a system running Linux, the telnet session may terminate if the amount of data being transferred is huge.

Workaround: Redirect the CLI output to a text file and use the "type" command to view the output

- 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.

- BITS080696: Windows "No Instance(s) Available" is reported for Dell\_CMApplication class data To get the data for Dell\_CM\* wmi classes query, first query any one of the Dell\_\* classes.

### Issues for Server Administrator Running on Microsoft Windows 2003 Operating Systems

- 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.
- 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://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

- 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:

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

For security reasons, Microsoft Windows Server 2008 is configured to not to 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 or prompt is not visible to the user. The application interface or 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 or 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 or prompt. After upgrading Windows Server 2003 x64 to Windows Server 2008 x64 with Server Administrator installed, the application UI does not display 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.

- 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 Microsoft Windows 2012 Operating Systems**

- BITS068231: On Windows Server 2012 with Server Administrator (32-bit), "Base Memory Address" and IRQ values are not available for any Network Interface Cards.

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

- When starting Server Administrator from the Red Hat Enterprise Linux console, kernel log messages may appear. To avoid these messages, perform the following steps:  
Edit the `/etc/sysconfig/syslog` file and modify `KLOGD_OPTIONS` to `KLOGD_OPTIONS="-c 4"`.  
Restart "syslog" by executing `/etc/init.d/syslog restart`.
- 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.
- 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 11G 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

- 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"
- 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.
- 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.
- The remote access controller uses FTP protocol to perform some of the Server Administrator 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"
- 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.

- 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.
- 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.
- 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.
- RAC firmware 2.0 and later 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.

- 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.

- 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.
- 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.

- DF384362: "Redundancy Status" displays as "Not Applicable" in ESXi even when NICs are teamed. On VMware ESXi systems, NIC teaming status may not display 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.
- 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.
- 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.
- 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.
- DF380725: On Internet Explorer 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.
- On 12G 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 11G servers or below, when the maximum limit is reached, the information logging is stopped.
- 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.
- 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.
- DF520449: On all versions of the ESX, the following USB connection error messages are generated. These messages can be ignored.

The following is 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)
```



- 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.
- 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 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`
- BITS086423: After an upgrade to the current version, Server Administrator does not retain the support link information on the Preferences page.
- BITS083068: IE8 Issues: In OMSA GUI, under System >Logs >Hardware/Alert/Command, while saving the logs in IE8 using "Save As" option, a twice zipped file is created. On extracting the contents of the zip file, an extension less file is obtained. To get the html and auxiliary folder, you must extract the extension less file.
- BITS091830: Distributed Web Server (DWS) connection does not work if you have installed the sblim-sfcb rpm from SLES11 SP3 OS DVD. To make the connection work, install sblim-sfcb rpm either from SLES11 SP2 or from OM DVD.

## Limitations

### Known Limitations and Workarounds for Storage Management Service

- 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.
- View slot occupancy report shows 4 HDD slots on backplanes with just two HDD slots for any server.
- Physical disk clear operation is not available on PERC 8 family of controllers.
- 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 as part of the upcoming OM releases. 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.

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

- 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.

- 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.

- 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.

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

- o There are no longer any physical disks in "Foreign" state after the "Import Foreign Configuration" task completes.
- o 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.

- 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 PowerVault 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.

- 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.

- 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.

- 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.
- 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.
- 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.
- Fluid Cache Details are not automatically enumerated on SUSE Linux 11 SP2 x86\_64 operating system after system reboot.

Description: Fluid Cache details are not enumerated in CLI or GUI after system reboot. Issue is applicable only to SUSE Linux 11 SP2 x86\_64 operating system.

Solution: To see the Fluid Cache details through CLI or GUI, connect to Fluid cache through CLI or GUI.

- CLI Command to connect to Fluid Cache: `omconfig storage fluid cache action=connect`
- GUI Command to connect to Fluid Cache: Although Fluid Cache details are not enumerated in GUI after system reboot, Fluid Cache component is enumerated in Storage component tree.

Steps to connect:

1. Click Fluid Cache component listed under storage tree.
  2. Click "Connect Fluid Cache" option to connect to Fluid Cache.
- DAS Fluid Cache License cannot be applied through DWS Client.
  - After hot removing the PCIe SSD which is part of Fluid Cache Pool, Fluid Cache Pool does not show the updated value of Cache Count.

## Installation Prerequisites

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.

## Installation Procedure

For complete installation instructions, see the "Server Administrator Installation Guide Version 7.3".

This section provides information to enhance your experience with Server Administrator implementations and environments.

- To install Server Administrator on Windows Server 2008 R2 SP1 Core and Windows Server 2012 Core, Windows-on-Windows (WOW) mode must be enabled.
- Port 1311 is the default port for Server Administrator. It is a registered port number of Server Administrator. 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:
  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:
    - In "Miscellaneous", select the "Allow META REFRESH" radio button.
    - In "Active Scripting", select the "Enable" radio button.
    - Under "Active scripting", select the "Allow scripting of Microsoft 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. Select the "Advanced" tab and in "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, security warnings may be displayed against port 1311, the port running the Server Administrator Web server. The warnings have been investigated by engineering and are determined to be "false positives" (invalid security warnings) that you can ignore. The following are the warnings:

- "The Web server on 1311 allows scripts to read sensitive configuration and / or XML files."
- "The Web server on 1311 allows to delete "/" which implies that the Webserver will allow a remote user to delete the files in root on the server."
- "The web server on 1311 may be susceptible to a 'www Infinite Request' attack."
- "It is possible to make the remote tthttpd server execute arbitrary code by sending a request like: GET If-Modified-Since:AAA[...]AAAA

Solution: If you are using tthttpd, upgrade to version 2.0. Else, contact the vendor for a patch or change the web server. CVE on this one is CAN-2000-0359".

- 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 if the access is blocked in the Server Administrator Preferences page.
- Dell SNMP MIB Files for Dell Systems:
- Dell SNMP MIB files for Dell systems allow you to obtain and verify information provided by supported software agents. The current MIB files supported by PowerEdge software agents are located at "\support\mib" on the "Systems Management Tools and Documentation" DVD.

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

- Server Administrator support for Encrypting File System (EFS)
- To improve security, Microsoft allows encrypting files using EFS. Note that SERVER ADMINISTRATOR will not function if its dependent files are encrypted.
- Server Administrator GUI and CLI Response Time
- On 9G and later systems, the response time for some components of the Server Administrator GUI and CLI has increased to several seconds as Server Administrator does not cache some of the DRAC/iDRAC data. The data is retrieved from the DRAC/iDRAC when you request for it.
- Following are the Server Administrator GUI pages for which the 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 for which the 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 and operating system

### Firmware for PERC controllers

Firmware for 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 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	6.3.1-0003
PERC 6/i Integrated	6.3.1-0003
PERC 6/i Adapter	6.3.1-0003
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	12.10.5-0001
PERC H700 Integrated	12.10.5-0001
PERC H700 Adapter	12.10.5-0001
PERC H700 Modular	12.10.5-0001
PERC H200 Adapter	07.03.06.00
PERC H200 Integrated	07.03.06.00
PERC H200 Modular	07.03.06.00
PERC H200 Embedded	07.03.06.00
6Gbps SAS HBA	07.03.06.00
Internal Tape Adapter	07.03.06.00
PERC H310 Adapter	20.12.0-0004
PERC H310 Mini Monolithic	20.12.0-0004

PERC H310 Mini Blades	20.12.0-0004
PERC H710 Adapter	21.2.0-0007
PERC H710 Mini Blades	21.2.0-0007
PERC H710 Mini Monolithic	21.2.0-0007
PERC H710P Adapter	21.2.0-0007
PERC H710P Mini Blades	21.2.0-0007
PERC H710P Mini Monolithic	21.2.0-0007
PERC H810 Adapter	21.2.0-0007
PERC S110	3.0.0.0139
PERC S100	2.0.0-0162
PERC S300	2.0.0-0166+00193000

### Windows Drivers for PERC Controllers

Windows Drivers for 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.

<b>Controller</b>	<b>Windows Server 2008 32-bit Driver</b>	<b>Windows Server 2008 64-bit Driver</b>	<b>Windows Server 2008 R2 Driver</b>	<b>Windows Server 2012 Driver</b>
PERC 5/E	2.24.0.32	2.24.0.64	4.5.0.64	Native
PERC 5/i Integrated	2.24.0.32	2.24.0.64	4.5.0.64	Native
PERC 5/i Adapter	2.24.0.32	2.24.0.64	4.5.0.64	Native
SAS 5/iR Integrated	1.28.03.01	1.28.03.01	1.28.03. 52	Native
SAS 5/iR Adapter	1.28.03.01	1.28.03.01	1.28.03. 52	Native
SAS 5/i Integrated	1.28.03.01	1.28.03.01	1.28.03. 52	Native
SAS 5/E Adapter	1.28.03.01	1.28.03.01	1.28.03. 52	Native
PERC 6/E Adapter	2.24.0.32	2.24.0.64	4.5.0.64	Native
PERC 6/i Integrated	2.24.0.32	2.24.0.64	4.5.0.64	Native
PERC 6/i Adapter	2.24.0.32	2.24.0.64	4.5.0.64	Native
SAS 6/iR Integrated	1.28.03.01	1.28.03.01	1.28.03. 52	Native
SAS 6/iR Adapter	1.28.03.01	1.28.03.01	1.28.03. 52	Native
SAS 6/iR Modular	1.28.03.01	1.28.03.01	1.28.03. 52	Native

LSI 1020 on a PowerEdge 1600SC	Not Applicable	Not Applicable	Not Applicable	Not Applicable
LSI 1030 on a PowerEdge 1750	Not Applicable	Not Applicable	Not Applicable	Not Applicable
PERC H800 Adapter	4.31.1.32	4.31.1.64	4.31.1.64	Native
PERC H700 Integrated	4.31.1.32	4.31.1.64	4.31.1.64	Native
PERC H700 Adapter	4.31.1.32	4.31.1.64	4.31.1.64	Native
PERC H700 Modular	4.31.1.32	4.31.1.64	4.31.1.64	Native
PERC H200 Adapter	2.0.35.10	2.0.35.10	2.0.35.10	Native
PERC H200 Integrated	2.0.35.10	2.0.35.10	2.0.35.10	Native
PERC H200 Modular	2.0.35.10	2.0.35.10	2.0.35.10	Native
6Gbps SAS HBA	2.0.35.10	2.0.35.10	2.0.35.10	Native
PERC H310 Adapter	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H310 Mini Monolithic	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H310 Mini Blades	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710 Adapter	5.1.90.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710 Mini Blades	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710 Mini Monolithic	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710P Adapter	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710P Mini Blades	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H710P Mini Monolithic	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
PERC H810 Adapter	5.1.118.32	5.1.118.64	5.1.118.64	5.1.118.64
Internal Tape Adapter	2.0.35.10	2.0.35.10	2.0.35.10	Native
PERC S100	2.0.0-0162	2.0.0-0162	2.0.0-0162	Not Applicable
PERC S300	2.0.0-0162	2.0.0-0162	2.0.0-0162	Not Applicable
PERC S110	3.0.0.0134	3.0.0.0134	3.0.0.0134	Not Applicable

## Linux Drivers for PERC Controllers

Linux Drivers for 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

<b>Controller</b>	<b>Red Hat Linux Driver 6.4</b>	<b>Red Hat Linux Driver 5.9</b>	<b>SUSE Linux 11 SP2 64-bit Driver</b>	<b>SUSE Linux 10 SP4 64-bit Driver</b>
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	Native	Native	Native
SAS 5/iR Adapter	Native	Native	Native	Native
SAS 5/i Integrated	Native	Native	Native	Native
SAS 5/E Adapter	Native	Native	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	Native	Native	Native
SAS 6/iR Adapter	Native	Native	Native	Native
SAS 6/int. Modular	Native	Native	Native	Native
LSI 1020 on 1600SC	Native	Native	Native	Not applicable
LSI 1030 on Power Edge 1750	Native	Native	Native	Not applicable
PERC H800 Adapter	Native	Native	Native	Native
PERC H700 Integrated	Native	Native	Native	Native
PERC H700 Adapter	Native	Native	Native	Native
PERC H700 Modular	Native	Native	Native	Native
PERC H200 Adapter	Native	Native	Native	Native

PERC H200 Integrated	Native	Native	Native	Native
PERC H200 Modular	Native	Native	Native	Native
6Gbps SAS HBA	Native	5.2.220.64	Native	Native
PERC H310 Adapter	Native	Native	Native	Native
PERC H310 Mini Monolithic	Native	Native	Native	Native
PERC H310 Mini Blades	Native	Native	Native	Native
PERC H710 Adapter	Native	Native	Native	Native
PERC H710 Mini Blades	Native	Native	Native	Native
PERC H710 Mini Monolithic	Native	Native	Native	Native
PERC H710P Adapter	Native	Native	Native	Native
PERC H710P Mini Blades	Native	Native	Native	Native
PERC H710P Mini Monolithic	Native	00.00.05.38	Native	Native
PERC H810 Adapter	Native	Native	Native	Native
Internal type Adapter	Native	5.2.220.64	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

## Installation and Configuration Notes

N/A

© 2013 Dell Inc.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™, Venue™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, vMotion®, vCenter®, vCenter SRM™ and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.