Dell OpenManage Server Administrator
Version 7.0

Readme

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

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

NOTE: For detailed information regarding the Storage Management Service, see the Dell OpenManage Storage Management readme.

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 the Dell support website at **support.dell.com**.

What's New

The new features for this release include:

- Added support for the following operating systems:
  - VMware ESXi 5.0 FP1
  - SuSE Enterprise Linux 11 SP2 x86_64

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

- Added support for the following browsers:
  - Internet Explorer 9.0
  - Mozilla Firefox 6.0 and 7.0

- Deprecated support for Mozilla Firefox 3.6
- Added support for 12th (yx2x) systems
- Deprecated support for 8th Generation (xx8x) systems
- Users can configure all BIOS attributes on the new platforms supported
- BIOS settings are grouped under specific categories on the BIOS Settings page.
- Java Runtime Environment upgraded to 1.6 Update 30
- Added more cards to the list of Converged Network Adapters supported
- Users can configure Primary and Failover network access for Remote Access Controller (iDRAC)
- New Platform Events added for Internal SD Module
- System Reset Timer range for Auto recovery of a hung system raised to 720 seconds
- Based on License capability, the Server Administrator dynamically display/hides applicable features
- Provision for reporting power supply firmware version under the Power Supplies Information.
- Use the Server Administrator Web Server installed on a remote system to manage XenServer 6.0, since the local Web Server support has been deprecated as per Citrix's recommendation

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

Installation

For complete installation instructions, see the *Dell OpenManage Server Administrator Installation Guide Version 7.0.*

Installation and Configuration Notes

- The Server Administrator uses port 1311 as the default port. Port 1311 is a registered port number of Dell Inc. If another application is configured to run on port 1311 before Server Administrator is installed, the Dell Systems Management Server Administration (DSM SA) Connection Service will not start after installation. Before you install Server Administrator, ensure that port 1311 is not in use.
- You must enable the client-side scripting in Internet Explorer before starting Server Administrator. To do so, perform the following steps:
  1. Navigate to "Tools" in Internet Explorer.
  2. Under Tools, click "Internet Options".
  3. Under "Internet Options", click the "Security" tab.
  4. Select the security zone that the system running Server Administrator belongs to.

     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. Navigate to "Tools" in Internet Explorer.
  2. Under "Tools", click "Internet Options".
  3. Under "Internet Options", 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. Press '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. Click "Close".
  9. 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 against port 1311 running the Server Administrator Web server may be displayed. 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." Dell has determined that 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." Dell has determined that 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. If you are not, then 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 Simple Network Management Protocol (SNMP) Management Information Base (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 Server Administrator will not function if its dependent files are encrypted.
- Server Administrator Graphical User Interface (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 have increased to several seconds because some of the DRAC/iDRAC data is no longer cached by Server Administrator. The data must be retrieved from the DRAC/iDRAC when users 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 for Instrumentation Service

- On yx1x systems, if conflicting BIOS settings exist when 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 any BIOS configuration to be updated (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.

    OR
  - 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 Dual In-line Memory Module (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 while 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

- While using the Storage Management Service, Stop the DSM SA Data Manager Services before updating the Adaptec(R) Controllers.
- 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

- This service is available on supported systems in this release only. It enables remote access to a server that has lost its network connection or that has become unresponsive. In this 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.

Fixed Issues/Defects

DF289096 ESX4i

Description: DWS does not show connection error after login

DF416987 E-Clarity

Description: The space between two RAID 10 layout span disk in the Advance wizard is more

DF419932 E-Clarity

Description: Improper alignment for "Date" text boxes in asset info page FF3.x

DF419976 E-Clarity

Description: An extra line is displayed in the Destinations Table-Platform Events Page

DF421616 E-Clarity

Description: Page Expired error occurs when the Go Back button is clicked Inband failure page

DF421990 E-clarity

Description: |Om6.4|Improper Alignment

DF423927

Description: Inconsistency seen between DWS and Legacy Login for Interface Names in Brazilian OS

DF445065

Description: Restarting web server from Server Administrator GUI gives fatal JRE error-no functionality loss.

DF449421

Description: Server Administrator GUI: Setting power profile fails when BIOS setup password is enabled.

DF451609

Description: Mail-to Setting should be provided allowing user to set the default mail-address

DF451867

Description: OM6.5.0x136 - ITA omremote.exe does not work against SLES10SP4 targets

DF465223

Description: OM6.5, 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: DF#374857

Description: Connection service needs to be restarted for an Active Directory user login.

Resolution: After adding a VMware ESX 4.1 operating system to the Active Directory domain, an Active Directory user must do the following:

- 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: DF 354388

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

Resolution: If you configure the syslog to store logs on a remote virtual disk, and remove the remote virtual disk 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: DF 516238

Description: Power cycle shuts down server in ESX 4.1 U2 classic .

Resolution: 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.

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

Issue 1: DF 275424, 332775

Description: Domain users unable to login to Windows MN from Linux Web Server.

Resolution: Negotiate authentication is not supported while managing a Windows-based managed node, from 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 remotely manage a Windows/Linux based Managed System from a Windows-based Server Administrator web server.

Issue 2: DF 533809

Description: 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.

Resolution: 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:

Description: 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.

Resolution: The presence of this folder does not affect the functionality of the inventory collection. You can delete the folder if required.

Issue 2:

Description: After installing Server Administrator from the command prompt, issuing an "omreport" or "omconfig" command from the same prompt can cause an error.

Resolution: Open a new command prompt and issue commands from the new window.

Issue 3:

Description: 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:

Description: After a "Reset to Defaults" operation of the Integrated Dell Remote Access Controller, the first user configuration operation will fail if it is a single-user configuration item (such as enabling or disabling a user or changing user name).

Resolution: 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:

Description: 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 though the system has full redundancy.

Resolution: To confirm the correct state of the system, use the Server Administrator user interface.

Issue 6:

Description: The "Format or Split Mirror" operation may fail on a RAID 1 virtual disk on a CERC SATA 1.5/6ch controller. Dell is working towards resolving this issue.

Issue 7:

Description: While issuing 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**; otherwise, the output file will be empty.

Issue 8:

Description: Issuing 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:

Description: 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.

Resolution: 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:

Description: Some complex "omconfig" CLI commands that contain multiple set operations have been modified to avoid the above problem.

Resolution: While executing a CLI command, if you receive the message "Error! Illegal combination of parameters", modify your command into several simpler commands. Each command should change only one setting.

Issue 11:

Description: When running Server Administrator on a system with a traditional Chinese operating system, the application pages are displayed in simplified Chinese.

Resolution: To view the Server Administrator pages in English, go to your browser language preference page and change the language to English.

Issue 12:

Description: Log files saved from Server Administrator are saved in zip format. For best results, it is recommended that the zip file is opened using WinZip.

Resolution: Using the Windows Server 2003 or Windows XP embedded "Compressed (zipped) Folder" utility is not recommended.

Issue 13:

Description: 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:

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

Resolution: 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 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\iws\config**.
3. Copy **keystore.db.bak** to **keystore.db**.
4. Type: omconfig system webserver action=start

Issue 15:

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

Issue 16:

Description: 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:

Description: 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:

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

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

Issue 19:

Description: All unsecured HTTP requests to Server Administrator receive an invalid response. Server Administrator runs only one instance of the Web server, which is secure.

Resolution: 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:

Description: If the browser used with Server Administrator indicates that it cannot display a page or perform an action, ensure that the browser is in online mode.

Resolution: To go online, perform the following:

1. If you are using Internet Explorer, click "File" on the menu bar and clear the "Work Offline" option. When "Work Offline" is selected, a check is displayed to the left of the option on the "File" menu.

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

Issue 21:

Description: 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 22:

Description: 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 23:

Description: If you close the browser using the "Close" button on the browser or log off from the operating system, the Server Administrator session does not get terminated.

Resolution: This session will be 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. The maximum number of Server Administrator sessions at a time is configured by "connections" entry in \"<OpenManageInstallPath>\iws\config\iws.ini" file.

Issue 24:

Description: If you change the operating system Time Zone to a new timezone, Server Administrator session management will not display the time in the new time zone specified.

Resolution: Restart Server Administrator so that the correct time zone time is displayed in the Session Management page.

Issue 25: DF 78425

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

Resolution: 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 will be 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 26:

Description: Using the Internet Explorer browser, if you install Server Administrator on a system that includes a 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 27: DF 152755

Description: The Server Administrator GUI becomes unresponsive when the alerts log has many events.

Resolution: If the Alert Log contains several entries and if you try to navigate to another page, the Server Administrator GUI may become unresponsive and display the content in about 30 seconds.

Issue 28: DF 172125

Description: Power monitoring probes are shown on certain systems that do not support power monitoring.

Resolution: On certain systems that do not support power monitoring, the 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 will be taken.

Issue 29: DF 185770

Description: Primary User Telephone Number does not accept symbols.

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

Issue 30:

Description: The selection of default option for front panel LCD in Server Administrator will display Model Name whereas the default is Service Tag on the physical LCD.

Issue 31:

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

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

Issue 32:DF 277439

Description: Persistence of Configuration and Log File Changes in VMware(R) ESXi (277439)

Resolution: 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. The changes are lost, if the system is reset without a shutdown before the updates to the designated configuration are made and log files are updated to the disk.

The following is one 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 shutdown before the changes to the configuration file are updated to the disk, the user-defined thresholds become the default thresholds.

Issue 33: DF 315853

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

Resolution: 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 34:

Description: 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 35: DF 489034

Description: Intel(R) TXT configuration fails due to Virtualization technology dependency.

Resolution: 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 (R) 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's configurable.

Issues for Server Administrator Running on all Microsoft Windows Operating Systems

Issue 1:

Description: Execute all Server Administrator CLI commands from a 32-bit Windows command prompt. Acceptable ways to access the 32-bit command prompt are 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:

Description: The DSM SA Connection Service may hang on system startup if both Oracle and VERITAS(R) Backup Exec(TM) are installed on the system.

Resolution: To manually start the DSM SA Connection Service on a system running Windows, click **Start-> Programs-> Administrative Tools-> Service**, right-click **DSM SA Connections Services** and select **Start**.

Issue 3:

Description: 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.

Issues for Server Administrator Running on Microsoft Windows 2003 Operating Systems

Issue 1:

Description: The following warning message can be ignored:

"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.
0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789"

Issue 2:

Description: 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

Resolution: 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: DF 94201

Description: 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**.

Resolution: 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: DF 103661

Description: 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 to 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 SA 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 SA Data Manager service is installed as a non-interactive service, which means that it is configured for not allowed to interact with the desktop directly. If an interactive application is executed for an Alert Action in this situation, the application will be suspended waiting for input from the user, but the application interface/prompt will not be visible to the user.

The application interface/prompt will not be visible even after the Interactive Services Detection service is started. For each execution of the interactive application, there will be 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 SA Data Manager service to be allowed to interact with the desktop. To allow interaction with the desktop, right-click on the DSM SA 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 SA Data Manager service for the change to take effect. When the DSM SA Data Manager service is restarted with this change, the Service Control Manager logs the following message to the System log: "The DSM SA 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 SA 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 "Interactive services dialog detection"

dialog box will be displayed by the operating system 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 of 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: DF 330800

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

Resolution: 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:

Description: When starting Server Administrator from the Red Hat Enterprise Linux console, kernel log messages may appear.

Resolution: To avoid these messages:

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:

Description: 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:

Description: For systems running a supported Red Hat Enterprise Linux operating system, kernel driver messages such as "AAC_ChardevOpen" may be displayedvin 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 Storage Management Service

The following are open issues regarding the Storage Management Service.

Storage Management Service Issues for all Supported Operating Systems

Issue 1:

Description: When issuing certain "omconfig storage" CLI commands with "Power User" privileges, the following message may be displayed: "Error! User has insufficient privileges to run command: omconfig"

Resolution: You must be logged in as an Administrator to perform these actions.

Issue 2:

Description: On a Windows Server 2003 system, it is recommended that you update to Service Pack 1 or later. Service Pack 1 is required to support SAS technology.

Issue 3:

Description: 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. Dell is working to resolve this problem.

Issue 4:

Description: 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. Dell is working towards resolving this issue.

Issue 5:

Description: 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 6:

Description: 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 7:

Description: 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 Swindow, rather than launching the selected option.

Storage Management Service Issues for Red Hat Enterprise Linux Operating Systems

Issue 1:

Description: 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. Dell is working for this issue is being worked out.

Issue 2:

Description: Using the Storage Management Service Advanced Create VDisk WizardWith Chinese or Japanese language browser settings, may occasionally result in text overflowing to the bottom of the side-by-side blue text boxes.

Issues for Remote Access

Note: The Remote Access Service is supported on yx1x 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:

Description: The 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 will return errors:

```
"racadm localauthenable"
"omconfig rac authentication"
```

Issue 2:

Description: 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: DF 132894

Description: 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:

Description: 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:

Description: 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:

Description: 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:

Description: 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:

Description: The RAC may not send traps when your system is locked up.

Resolution: 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:

Description: 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). If you created RAC user IDs using previous versions of the firmware or if you created user IDs using Server Administrator that is running version 2.0 firmware on the managed system, you cannot log in to the RAC.

Resolution: Use one of these methods to correct this issue:

- Change your passwords before updating the firmware.

  OR

- 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.`

  OR

- Change the password through Server Administrator using the "User" tab.

- Ensure that the check box to change the password is checked. Enter a new password, and then enter it again to validate the change.

OR

- 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:

Description: 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.

Resolution: 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:

Description: If the out-of-band RAC user interface was 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 browser is set to the UTF-8 character set by Server Administrator.

Resolution: 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:

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

Resolution: 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 will not be able to log in to the Web interface and you will receive a message that your username and password is incorrect.

Known Limitations and Workarounds

Limitation 1: DF 384362

Description: "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.

Limitation 2: DF 384061

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

Workaround: 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.

Limitation 3: DF 165588

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

Workaround: Server Administrator UI may show 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 there is an article and fix provided by Microsoft. The Knowledge Base article number is KB933006 and a fix has been provided as security update 933566 (MS07-033):Cumulative Security Update for Internet Explorer.

Limitation 4: DF 319132

Set operation in Server Administrator is blocked if a single sign-on is used to log in.

Workaround: 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 Server Administrator desktop icon) on Internet Explorer 8.

Limitation 5: DF 380725

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

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

Limitation 6:

Description: 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.

Limitation 7: DF 523827

Description: 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. (523827)

Limitation 8: DF 530134

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

Workaround: 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.

Limitation 9: DF 520449

Description: 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
```

Limitation 10: DF 531509

Description: 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.

Limitation 11: DF 532055

Description: 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
   ```

Documentation Errata

None

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 - 03 Rev. A00