

#####

DELL(TM) OPENMANAGE(TM) SERVER ADMINISTRATOR VERSION 6.2
README

#####

Version 6.2

Release Date: December 2009

NOTE: This readme provides information for Dell OpenManage Server Administrator version 6.2

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: See the Dell OpenManage Storage Management readme for detailed information regarding the Storage Management Service.

The 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/manuals".

This file contains the following sections:

- * Criticality
- * Minimum Requirements
- * Release Highlights
- * Installation
- * User Notes
- * Known Issues

#####

CRITICALITY

#####

3 - Optional

Dell recommends that you review specifics about the update to

determine if it applies to your system. The update contains changes that impact only certain configurations and provides new features that may or may not apply to your environment.

MINIMUM REQUIREMENTS
#####

This section provides information about the minimum requirements for installing and using Server Administrator.

- * Please see the latest Dell Systems Software Support Matrix contained on the media for the latest and complete list of supported operating systems and platforms.

=====
SUPPORTED WEB BROWSERS
=====

- * Microsoft(R) Internet Explorer 6.0 (SP2) and 7.0 on Microsoft Windows Server 2003 and Microsoft Windows Server 2008.
- * Firefox 2.0 on SUSE Linux Enterprise Server version 10.
- * Firefox 3.0 on Microsoft Windows Server 2003, Microsoft Windows Server 2008, Red Hat(R) Enterprise Linux(R) (AS, ES, WS) version 4.7 and version 5.2 and SUSE Linux Enterprise Server version 10.

NOTE: The Server Administrator browser attempts to use the available browser in all cases. However, under certain circumstances, using an unsupported (version or unsupported type) browser may not be reported to you. In such cases, you may see unexpected results.

NOTE: The operating system media browser install may not be the version supported by Server Administrator. See the appropriate Red Hat Enterprise Linux operating system documentation to upgrade the base browser install version to the supported version.

NOTE: If you are unable to launch Server Administrator using IPv6 address, check the operating system and browser support for IPv6.

=====
SUPPORTED SSL VERSION
=====

- * Server Administrator supports SSL 3.0 exclusively.

=====
SUPPORTED RAC FIRMWARE
=====

- * iDRAC firmware version 1.1 or greater is required for systems installed with iDRAC.

RELEASE HIGHLIGHTS
#####

* For a detailed table of supported servers and operating systems, see the Dell Systems Software Support Matrix.

INSTALLATION
#####

For complete installation instructions, see the "Dell OpenManage Installation and Security Version 6.2 User's Guide ".

USER NOTES
#####

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

* 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 DSM SA Connection Service will not start after installation. Before you install Server Administrator, ensure that port 1311 is not being used.

* You need to enable 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 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 safely 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 might 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 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. 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.

* Server Administrator security settings are not applicable for Active Directory users. Active Directory users with read-only login can access Server Administrator, even after access is blocked in the preferences page of Server Administrator.

* 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(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 EFS (Encrypting File System)

To improve security, Microsoft provides the capability to encrypt files using EFS (Encrypting File System). Note that Server Administrator will not function if its dependent files are encrypted.

* Server Administrator GUI and CLI Response Time

On Dell PowerEdge x8xx and later systems, the response time for some parts of the Dell OpenManage Server Administrator GUI and CLI have increased to several seconds because some of the iDRAC data is no longer cached by Server Administrator. The data must be retrieved from iDRAC when requested by you.

Some of the Server Administrator GUI pages whose response time may have increased are as follows:

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

Some of the Server Administrator CLI commands whose response time may have increased are as follows:

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

The amount of time varies by hardware system and operating system.
[188345]

=====
NOTES FOR THE INSTRUMENTATION SERVICE
=====

- * 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 Server Administrator, the changed threshold value becomes the default threshold value.

- * When 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 apparent which memory module is the cause. 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 while the system is in "OS Install Mode", memory may be reported incorrectly by Server Administrator. To avoid this issue, you must disable "OS Install Mode" before running Server Administrator.

- * If you have to uninstall and reinstall the operating system SNMP service, then reinstall Server Administrator as well, so that the Server Administrator SNMP agents are registered with the operating system SNMP agent.

NOTES FOR THE STORAGE MANAGEMENT SERVICE

- * When 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 THE 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.
- * After installing Internet Explorer 5.0 or later, you may notice that the automatic configuration and proxy setting information for each connection is separate from the same information used for the LAN connection. If you have a dial-up and a LAN connection at the same time, Internet Explorer may block your access to the Internet.

This blocking occurs because each connection in Internet Explorer 5.0 uses its own automatic configuration and proxy settings. When you try to establish a PPP connection, Internet Explorer attempts to use the dial-up connection settings to access the Internet.

You can find additional information about this issue in the article Q818060, "Connections No Longer Use Local Area Network Automatic Configuration and proxy settings" in the Microsoft Knowledge Base (KB) at "support.microsoft.com".

To correct this problem, you must apply Microsoft IE HotFix Q818060 or KB839571 to Internet Explorer 6.0 SP1 on Windows 2000 server or Windows 2003 server. HotFix Q818060 and KB839571 are available on the "Server Manage Node" CD in the "\srvadmin\Windows\HotFix" directory. See the following Microsoft support articles for further instructions on applying this HotFix:

- * (Windows 2000 Server) "<http://support.microsoft.com?kbid=818060>"
- * (Windows 2003 Server) "<http://support.microsoft.com/kb/839571>"

As explained in the Microsoft KB article, use the Registry Editor ("regedit.exe") to browse to the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion  
\Internet Settings\
```

If "DialupUseLanSettings" key is not present, create a registry item for "DialupUseLanSettings" and set a value of "1". Make sure the value type is "DWORD".

Note: HotFix Q818060 may still fail to install on Internet Explorer 6.0 SP1. If the error "This update requires Internet Explorer 6.0

SP1 to be installed" occurs, perform these steps:

1. Unzip "Q818060-Eng-IE6.zip".
2. From a Windows command shell, enter "Q818060.exe /C" to extract the HotFix files to a directory.
3. In the command shell, switch to the directory and then enter "ieupdate.exe Q818060".
4. Launch Internet Explorer, open the "Help" menu, and select "About Internet Explorer". Verify that "Q818060" appears in the "Update Versions" field.

KNOWN ISSUES
#####

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

=====
ISSUES FOR SERVER ADMINISTRATOR WEB SERVER RUNNING ON REDHAT LINUX 4 OPERATING SYSTEMS
=====

* Server Administrator Web Server running on RHEL4 Operating system may report an 'out of memory' error while managing a remote system. This error may be reported because of an old curl library present with the Web Server Operating System. Refer to the curl website <http://curl.haxx.se/changes.html> for details. Contact the Operating System vendor for the latest supported library.
[328459]

=====
ISSUES FOR SERVER ADMINISTRATOR WEB SERVER RUNNING ON ALL LINUX OPERATING SYSTEMS
=====

* Negotiate authentication is not supported while remote managing a Windows-based managed node from Linux-based Server Administrator Web Server. If you run 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 will be reported. However, you can remotely manage a Windows/Linux based managed system from a Windows-based Server Administrator Web Server.
[275424,332775]

=====
ISSUES FOR SERVER ADMINISTRATOR RUNNING ON ALL SUPPORTED OPERATING SYSTEMS
=====

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

The presence of this folder does not affect functionality of the inventory collection. The folder can be deleted if required. [138549]

- * After installing Server Administrator from the command prompt, issuing an "omreport" or "omconfig" command from the same prompt can cause an error. Open a new command prompt and issue commands from the new window.
- * 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 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). 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.[136599]
- * 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. To confirm the correct state of the system, use the Server Administrator user interface.
- * 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 to resolve this problem.
- * When issuing the Server Administrator command "omreport system version -outc <filename>", ensure you specify an absolute path name for the output file, for example, "c:\out.txt"; otherwise, the output file will be empty.
- * 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.[124997]
- * For complex "omconfig" CLI commands that contain multiple commands in one command line, the CLI may report a success status for the command even if 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 operations have been modified to avoid the above problem. If, while executing a CLI command you receive the message "Error! Illegal combination of parameters", 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 Server Administrator pages are displayed in Simplified Chinese. To view the Server Administrator 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. For best results, it is recommended to open this zip file using WinZip. Using the 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 updated BIOS settings to be properly displayed by Server Administrator.
- * If you import an invalid root certificate into Server Administrator using "Preferences-> General Settings-> Web Server-> X.509 Certificate" and try to log in to Server Administrator after restarting the Web server, you will see a blank page.

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 webservice 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 webservice action=start
```

- * A temperature drop to below a minimum failure threshold does not cause a system reset even if this alert action is set.
- * Clicking the browser "Back" and "Refresh" buttons 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 previously disabled in the System Setup Program.
- * The links on the Server Administrator home page may lock up after repeated random clicking. To resolve this situation, 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 indicates that it cannot display a page or perform an action, ensure that the browser is in online mode. To go online, perform the following:
 - If you are using Internet Explorer, click "File" on the menu bar and deselect the "Work Offline" option. When "Work Offline" is selected, a tick mark displays 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".
- * When setting dates in the "Asset Information" section of the Server Administrator home page, the current time is appended to the date. When setting dates with the CLI, the appended time is noon.
- * If Network Adapter Teaming is installed and enabled on your system, Server Administrator does not display the IP address or other connection-related data for the individual network adapters. The connection status and IP address belong to the virtual adapter created by the teaming software.
- * 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.
- * Some Internet browsers (for example, Microsoft Internet Explorer, Mozilla Firefox, and so on) share states, including cookies and browser session information, across multiple instances. If a user tries to log in to multiple browser instances, then only the last session stays active, while the older sessions expire. As a result, the "403 forbidden" error message could be displayed in the older

session windows. Also, if you have logged in to multiple browser instances, the session management window displays only one session (the last log-in session) for you. To avoid these issues, access Server Administrator Web Server using a single browser instance.[280268]

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

* If you change the operating system timezone to a new timezone, Server Administrator session management will not display the time in the new time zone specified. Restart the Server Administrator so that the correct time zone time is displayed in the Session Management page.

* Server Administrator Auto Recovery feature may execute configured action when system is under heavy stress.

The Auto Recovery feature can be set to execute an action (For example, reboot system) to recover a hung system. Since the Auto Recovery timer is now an application level timer instead of a kernel level timer, heavy resource stress on the system makes it more likely that a short keep alive interval (less than 120 seconds) will not be measured accurately, 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. [78425]

* Using Internet Explorer browser, if you install Server Administrator on a system that includes an underscore in its hostname, you must use 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>

* If the Alert Log contains large number of entries and if you try to navigate to another page, Server Administrator GUI may become unresponsive and may take approximately 30 seconds. [152755]

* 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; however no action will be taken. [172125]

* On Server Administrator, Under Asset Information-> System Information-> Primary User Telephone Number configuration allows only alphanumeric characters. [185770]

* 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.

* 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.

Now, the items on the front page may respond to your click.

* Persistence of Configuration and Log File Changes in VMware(R) ESXi

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

The following is 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 graceful shutdown before the changes to the configuration file are updated to the disk, the user-defined thresholds become the default thresholds. [277439]

* On systems running the VMware ESXi operating system, Server Administrator may display the "Measurement Finish Time" in the "Power Tracking Statistics" page as [N/A]. [297532]

- * Due to the limitation of VMware ESX 3i/4i, the “About” tab in the Server Administrator Preferences page will display 'Preferences Preferences' instead of 'Server Administrator Preferences.'
[276236]
- * While trying to manage a system running the VMware ESXi version 4 operating system from Server Administrator Web Server, an “Internal Error” message may be displayed if the management agent stops responding.
[289096]
- * 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.
[315853]
- * The Remote Management feature is not supported on the system running VMWare ESX 3.5 operating system, either as a Server Administrator Web server or a Remote Enablement Agent. If you use systems running VMWare ESX 3.5 operating system as a Server Administrator Web server or as a Remote Enablement Agent, a "login failed" message will be displayed while managing it as a remote node (s). On VMWare ESX 3.5 based managed systems, even though the remote enablement option is available, it is not supported when actually installed. You can manage VMWare ESX 3.5 based system as a local node.
[280822,330584,330615]
- * Time zone changes which are applied manually or through the network time server will not take effect in Server Administrator unless you restart Server Administrator services.

In addition you will need to restart the following services if Remote Enablement is installed.
For Windows Operating Systems:
 - Windows Management Instrumentation Service
 - Windows Remote Management (WS-Management)For Linux Operating Systems:
 - SFCB daemon (/etc/init.d/sfcbd)
 - Open-WSMan daemon (/etc/init.d/openwsmand)[329124]
- * In case of Power Monitoring statistics, reset the values after restart of Server Administrator services for time zone changes to take effect.
[329124]
- * If the IDSDM (Internal Dual SD Module) Redundancy is disabled through the (F2) BIOS Setup and the system is rebooted with IDSDM card installed, then the Internal Dual SD Module Redundancy section will not be reported on the Removable flash media information page or the corresponding CLI command i.e. omreport chassis removableflashmedia.
[349628]

ISSUES FOR SERVER ADMINISTRATOR RUNNING ON ALL MICROSOFT WINDOWS OPERATING SYSTEMS

* 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.

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

* The Server Administrator 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 from 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. [165588]

* You may not have appropriate privileges on Server Administrator GUI if :

1. You are part of 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.

* Some Internet Explorer versions like IE8 share session cookies across multiple session instances. If you are logged in to a remote node and open another instance locally, then the session cookies of the first instance will be shared with the second session. As a result, few fields will not be visible and your data gets shared. To avoid this, open a New Session item on the File menu or run iexplore.exe with the -nomerge parameter. This will open a new browser window, and this new browser instance will not share session cookies with the original browser window. [320433]

* Internet Explorer 8 has a new security feature called "Loopback security check" which prevents NTLM-based authentication from the local machine. This feature blocks you from performing any operation in Server Administrator if logged in using single sign-on (clicking Server Administrator desktop icon) on Internet Explorer 8. [319132]

=====

ISSUES FOR SERVER ADMINISTRATOR RUNNING ON MICROSOFT WINDOWS 2003 OPERATING SYSTEMS

=====

* 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 correctly impersonate user requests

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 system that require user impersonation.

* An error message ("The compressed (zipped) folder is invalid or corrupted") will be displayed when you perform the following actions in Server Administrator on Windows 2003 for x64 systems with Internet Explorer 6 Service Pack 1:

1. Go to System -> Logs
2. Select "Command," "Alert," or "Hardware."
3. Click "Save As"
4. Click "Open" in "File Download" message box.

Additionally, the "Export" function in the Server Administrator GUI may not work. The root cause of both problems is the same. To resolve the issue, uncheck "Do not save encrypted pages to disk" under Tools-> Internet Options-> Advanced tab. For more information, see the following article on the Microsoft website:

-> "<http://support.microsoft.com/default.aspx?scid=kb;en-us;812935>",
-> "<http://support.microsoft.com/default.aspx?scid=kb;en-us;141582>"
and
-> "<http://support.microsoft.com/default.aspx?scid=kb;en-us;144876>".

* 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.msp"
-> "<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 on 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

=====

* 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". [94201]

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 logon only in Intranet zone" instead.
5. Click "Ok" to open dialog boxes to complete the setting.

* 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". In order for interactive applications to execute properly for an Alert Action, the DSM SA Data Manager service must be configured as an interactive service. Examples of interactive applications are applications with a Graphical User Interface (GUI) or that prompt

you 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 to not be 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 need 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 in order 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. [103661]

After upgrading Windows Server 2003 x64 to Windows Server 2008 x64 with Dell OpenManage Server Administrator installed, the Dell OpenManage Server Administrator display does not show all of the expected instrumentation pages. The Dell OpenManage Server Administrator installation must be repaired.
Go to Start-> Settings-> Control panel-> Add Remove Programs-> Select "Change" on the DELL OpenManage Server Administrator installation and select the "Repair" option to correct the issue.

* When a managed node based on Windows 2008 R2 is added to a domain, Logging in from any Server Administrator Web Server to that managed node will fail with local user or local power-user credentials. Only local Administrator or Domain user credentials works, with a prerequisite that all required winrm configurations have been applied.
[330800]

ISSUES FOR SERVER ADMINISTRATOR WEB SERVER RUNNING ON MICROSOFT WINDOWS XP OPERATING SYSTEM

* If you are running Server Administrator Web Server on a Microsoft Windows XP SP2 operating system and trying to manage a system with VMware ESXi version 4 operating system remotely, a login failure message is displayed. To resolve this issue, apply Microsoft KB909425. The KB is available at

<http://support.microsoft.com/kb/909425/>
[275271]

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 display. To avoid these messages, perform the following steps:

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

* 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 Server Administrator 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 safely ignored.

* When SELinux is enabled, Server Administrator may log the following message in the system log, without any impact to functionality. The following message can be ignored:

```
setroubleshoot: SELinux is preventing pam_console_app (pam_console_t)
"read write" to /opt/dell/srvadmin/var/lib/openmanage/.omaipc (var_lib_t).
[333642]
```

ISSUES FOR STORAGE MANAGEMENT SERVICE

The following are open issues regarding the Storage Management Service.

STORAGE MANAGEMENT SERVICE ISSUES FOR ALL SUPPORTED OPERATING SYSTEMS

- * 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 in as an Administrator to perform these actions.
- * On a Windows Server 2003 system, it is strongly recommended that you update to Service Pack 1 or later. Service Pack 1 is required to fully support SAS technology.
- * Invalid "Format and Check Consistency" options are displayed for a regenerating 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.
- * 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 yet 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 to resolve this problem.
- * 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.
- * When the "Open in a New Window" option is selected in the Storage Management Service Advanced Create VDisk Wizard, the current page is opened in a new window, rather than launching the selected option.

STORAGE MANAGEMENT SERVICE ISSUES FOR RED HAT ENTERPRISE LINUX OPERATING SYSTEMS

- * 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 to resolve this problem.

- * 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.

ISSUES FOR REMOTE ACCESS

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

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

ISSUES FOR ALL OPERATING SYSTEMS

- * 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"

- * 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.
- * 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.[132894]
- * 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"
```

- * 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. In the Server Administrator GUI, click the "Properties" tab and ensure that the "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 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.

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.

- * 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 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. 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 will not be able to log in to the Web interface and you will receive a message that your username and password are incorrect.

#####

Information in this document is subject to change without notice.
(C) 2009 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: "Dell", "PowerEdge", "PowerVault", and "Dell OpenManage" are trademarks of Dell Inc.; Intel is a registered trademark of Intel Corporation in the United States and other countries; "Microsoft", and "Windows Server", are registered trademarks of Microsoft Corporation in the United States and/or other countries; "Red Hat" is a registered trademark of Red Hat Inc. in the United States and/or other countries; "SUSE" is a registered trademark of Novell Inc. in the United States and/or other countries; "VERITAS" is a registered trademark and "Backup Exec" is a trademark of VERITAS Software Corporation; Adaptec is a registered trademark of Adaptec, Inc.

Server Administrator uses the OverLIB JavaScript library. This library can be obtained from "<http://www.bosrup.com/web/overlib/>".

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2009