##

DELL OPENMANAGE(TM) SERVER ADMINISTRATOR VERSION 5.2 README

##

NOTE: This readme provides information for Dell OpenManage Server Administrator version 5.2.

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

NOTE: See the Dell OpenManage Install 5.2 readme ("readme_ins.txt"), which is located under the "readme" folder on the "Dell(TM) PowerEdge(TM) Installation and Server Management" CD for the latest installation information and issues specifically related to Server Administrator.

NOTE: See the Dell OpenManage Storage Management readme (located in the "srvadmin\docs\readme" directory on the "Dell PowerEdge Installation and Server Management" CD) for supplemental information regarding the Storage Management Service.

NOTE: Server Administrator versioning skipped major versions 3 and 4 so that the Server Administrator and OpenManage versions would match going forward.

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 documentation CD or from the Dell support website at "support.dell.com".

This file contains the following sections:

##
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 impacts only certain configurations, or 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.

==
INSTALLATION AND SERVER MANAGEMENT CD VERSION 5.2 SUPPORTED SYSTEMS
==

Refer to the "Software Support Matrix for Dell PowerEdge Systems" for
a complete list of supported Dell PowerEdge systems.

Server Administrator 5.2 is supported on the "Installation and Server
Management" CD version 5.2.

The following Dell PowerEdge systems are supported for
"Dell PowerEdge Installation and Server Management" CD version 5.2:
600SC, 650, 700, 750, 800, 830, 840, 850, 860, 1435SC, 1600SC, 1650,
1655MC, 1750, 1800, 1850, 1855, 1900, 1950, 1955, 2600, 2650, 2800,
2850, 2900, 2950, 2970, 4600, 6600, 6650, 6800, 6850 and 6950.

The following Dell PowerVault system is supported for
"Dell PowerEdge Installation and Server Management" CD version 5.2:
NX 1950

==
SUPPORTED OPERATING SYSTEMS
==

Refer to the "Software Support Matrix for Dell PowerEdge Systems" for
a complete list of supported Operating systems.

* Microsoft(R) Windows(R) 2000 Server family (32-bit extension)
  (includes Windows 2000 Server SP4 and Windows 2000
  Advanced Server SP4)

* Microsoft Windows Server(TM) 2003 R2 (32-bit and 64-bit
  extensions) (Standard, Enterprise and x64 editions), Microsoft
  Windows Server 2003 SP1 & SP2 (Web Edition), Microsoft Windows
  Storage Server 2003 R2 (includes Express, Standard, Workgroup, and
  Enterprise editions), and Microsoft Windows Server 2003 SBS R2

* Red Hat(R) Enterprise Linux version 4 (AS, WS, and ES) for x86,
  x86_64, and ia64

* Red Hat(R) Enterprise Linux version 5 for x86 and x86_64

* SUSE(R) Linux Enterprise Server version 9 (x86_64) with SP3 and
  SUSE(R) Linux Enterprise Server version 10 (x86_64).
  In XEN mode, support for service console only.

* VMware ESX 3 service console (see www.dell.com/vmware for details)

  NOTE: Refer to the "ISSUES FOR THE DELL REMOTE ACCESS CONTROLLER 5"
  section of this document for the supported managed server operating
  systems by DRAC 5.

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

* Microsoft Internet Explorer 6.0 (SP1) on Microsoft Windows
  Server 2000.

* Microsoft Internet Explorer 6.0 (SP1 and SP2) and 7.0 on Microsoft Windows
  Server 2003.

* Firefox 1.5 on Red Hat Enterprise Linux (AS, ES, WS) version 4 and
  version 5 and SUSE Linux Enterprise Server version 9 SP3 and 10.

* FireFox 2.0 on Microsoft Windows Server 2003, Red Hat Enterprise
  Linux (AS, ES, WS) version 4 and version 5 and SUSE Linux Enterprise
  Server version 9 SP3 and 10.

  NOTE: Refer to the "ISSUES FOR THE DELL REMOTE ACCESS CONTROLLER 5"
  section of this document for the browser supported by DRAC 5.

  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 the user. In such cases, the user
  may see unexpected or incomplete 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.

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

* Server Administrator supports SSL 3.0 exclusively.

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

* DRAC 5 firmware version 1.0 or greater is required for systems

installed with DRAC 5.

* On systems installed with a DRAC 4/I and DRAC 4/P firmware version 1.0 or greater is required.

* RAC firmware version 3.20 or greater is required for DRAC III, DRAC III/XT, ERA, and ERA/O.

RELEASE HIGHLIGHTS

* Added support for the following Dell PowerEdge systems: 2970.

* Added support for Red Hat(R) Enterprise Linux version 5 for x86 and x86_64.

* Added support for NIS, Kerberos, LDAP and Winbind authentication protocols for Linux operating systems.

* Processor capabilities and cache information are moved from processors information page to capabilities and cache information page.

INSTALLATION

For complete installation instructions, see the "Dell OpenManage Installation and Security 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 falls under.
NOTE: This option should be set to "Trusted sites".

5. Click the "Custom Level" button.

6. For Windows 2000, perform the following steps:

- Under "Miscellaneous", select the "Allow Meta Refresh" radio button.

- Under "Active Scripting", select the "Enable" radio button.

7. 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.

- Click "OK" and restart your browser.

* To allow Single Sign-on for Server Administrator, without prompts for user credentials, 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. Click ‘OK' to exit the "Custom Level" window.

7. Select the "Advanced" tab, and under "HTTP 1.1 settings", make sure "Use HTTP 1.1" is checked.

8. Select "Trusted sites". Click on "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 might 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 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.

* 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 PowerEdge Systems

Dell SNMP MIB files for PowerEdge systems allow customers to obtain and verify information provided by supported software agents. The current MIB files supported by PowerEdge software agents are located at "\support\mib" on the "Systems Management Consoles" CD.

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

* OpenManage support for Encrypting File System

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

==========
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.

Additionally, on PowerEdge 6800, the sensors will report a fan redundancy status of "Redundancy Lost" in the following scenarios:

- A power supply is removed and a power supply fan blank is not inserted.
- A power supply fan blank is present but failed.(134157)

* 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 which memory module 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.

* 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, Server Administrator loads one or both of these drivers if required. 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.

Red Hat Enterprise Linux:

Server Administrator provides precompiled dcdbas and dell_rbu modules for Red Hat Enterprise Linux version 3 and 4. These drivers are expected to ship with future Red Hat Enterprise Linux version 3 and 4 Updates.

SUSE Linux Enterprise Server:

These drivers ship with SUSE Linux Enterprise Server version 9 Service Pack 3 (SP3) and version 10. It is expected that future SUSE Linux Enterprise Server version 9 and 10 Service Packs will continue to ship these drivers.

If the drivers are available with the operating system, Server Administrator will use those versions of the drivers. If the drivers are not available with the operating system, Server Administrator will use its precompiled modules on Red Hat Enterprise Linux version 3 and 4. If precompiled drivers are not available with the operating system or Server Administrator, Server Administrator uses its Dynamic Kernel Support (DKS) feature to build the drivers when needed. See the "Dell OpenManage Installation and Security User's Guide" for more information about DKS.

* Setting Alert Actions in Linux

When you set Alert Actions for an event, you can specify the action to "execute an application". Setting an application value with an absolute path will fail if the application does not exist in the local file system or if the application has write file permission for "other users not in the file group (o)" bit. When this failure occur, the action state will stay enabled and the application value will be unchanged.

==========
NOTES FOR THE STORAGE MANAGEMENT SERVICE
==========

* When using the Storage Management Service, the DSM SA Data Manager must first be stopped before Adaptec controllers are updated.

* 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 supported on PowerEdge 650, 700, 750, 800, 830, 840, 850, 860, 1600SC, 1650, 1750, 1800, 1850, 2600, 2650, 2800, 2850, 4600, 6600, 6650, 6800, and 6850 systems 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 the following Remote Access Controllers (RACs): Dell Remote Access Controller (DRAC) 4/I, DRAC 4/P, DRAC III, DRAC III/XT, Embedded Remote Access (ERA), or Embedded Remote Access Option (ERA/O).

* RACs also have their 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, you should add "sleep" or "delay" commands of one or two seconds between the individual racadm commands.

* Unlike DRAC III, configuration of DRAC 4 settings is not supported in Server Administrator. Additionally, Server Administrator performs minimal reporting of DRAC 4 properties. For DRAC 5, a limited amount of NIC and User settings are configurable through Server Administrator to allow the user to connect via Out-Of-Band to the DRAC 5 card. For full configuration and reporting of all DRAC attributes, it is recommended to use the "racadm" command.

* 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 both 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 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 it is not present, create a registry item called "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, follow these instructions:

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 RUNNING ON ALL SUPPORTED OPERATING SYSTEMS

* Due to resource 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 may be deleted if desired. (138549)

* After installing Server Administrator from the command prompt, issuing an "omreport" or "omconfig" command from the same prompt causes an error. You must 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 BMC Management 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)

* On PowerEdge 750 systems, if you disable the Power button in Server Administrator, the system does not power cycle or power down in the event of system instability and/or blue screens. In such cases, you need to physically remove the power cord from the system to power down the unit. As the startup and recovery options in the operating system override those of Server Administrator, you need to configure them in the operating system to restart the system after a crash.

  NOTE: The above situation is applicable only when the "reboot" option in the startup and recovery options is disabled. If the "reboot" option is enabled, the system will automatically reboot and you will not be forced to shut down by removing the power cord. (126837)

* 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.

* If you have a RAID 1 virtual disk on a CERC SATA 1.5/6ch controller, performing a Format or Split Mirror operation may fail. Dell is working to resolve this problem.

* When issuing the Server Administrator command line "omreport system version -outc <filename>", be sure to 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 set 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 Server Administrator in English, go to your browser language preference page and change the language to English.

* When a log file is saved from Server Administrator, it is 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 get a blank page.

  To correct this issue, you must restore your original "keystore.db" file before importing a valid root certificate. To restore the "keystore.db" file, you must 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

* A temperature that drops below a minimum failure threshold does not cause a system reset even if this alert action is set.

* A reporting error, for the amount of memory enabled, may exist for the Level 2 (L2) cache memory when you view "Processor interface" for PowerEdge 6600 and 6650 systems. It may be incorrectly displayed as 256 K.

  If you purchased more than 256 K of L2 cache with your system, all of the L2 cache you have installed is fully enabled. The reporting error will be corrected in a future BIOS release for PowerEdge 6600 and 6650 systems.

* 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.

  Example:

1. Click "Main System Chassis" under "System Component Tree".

2. Click "Fans" under "Main System Chassis".

3. Click "Alert Actions" on the tab menu bar.

4. Click the "Back" button on the browser.

This action takes you to the "Fan Probes" page, leaving the tab menu bar unchanged. This action places the "Fan Probes" page under "Alert Actions" on the tab menu bar instead of under "Fan Probes".

* 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 might lock up after repeated random clicking. To resolve this situation, refresh the browser by pressing <F5> or by clicking 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 check 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.

* Mozilla-based browsers (including Firefox) share states, including cookies and browser session information, across multiple instances of running browsers under the same login session. If a user (or root user) has logged in to multiple Mozilla/Firefox browser instances, then the session management shows only one session (the last session logged in) of that user. If a user initially logs in to OMSA with certain privileges, and then starts another instance of the browser and logs into that instance with higher privileges, the initial OMSA session with the lower privileges will be elevated to the higher privileges of the second OMSA session automatically and vice versa.

* If a user closes the browser using browser close button or logs off from the OS,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 OS 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 a user changes the operating system timezone to a new timezone, Server Administrator session management will not display the time in the new timezone specified. Server Administrator needs to be restarted so that the correct timezone 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 (e.g. 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. In particular, the issue will be more prevalent in a system which has only one CPU, Hyper-Threading is not supported or is disabled, and the system is 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)

* If you install Server Administrator on a system that includes a underscore in its hostname, you must use the target system's IP address in the browser's URL to launch Server Administrator as

hostnames with underscores are not supported and can lead to unexpected behavior. For example (assuming Server Administrator is listening on port 1311): https://192.168.2.3:1311.

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 produce unpredictable results.

* The DSM SA Connection Service might 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", and, then right-click "Secure Port Server" and select "Start".

ISSUES FOR SERVER ADMINISTRATOR RUNNING ON MICROSOFT WINDOWS 2003 OPERATING SYSTEMS

* Warning messages ("A provider, omprov, has been registered in the WMI namespace, Root\CIMV2\Dell, to use the Local System account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests") may be displayed after installing Server Administrator. These messages 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. (139526)

* When running Server Administrator on Windows 2003 Small Business Server Edition, the "Export" function will display the export file in the browser window, instead of prompting the user to "open" or "save" the export file.

* 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 OS Application Event log. This issue occurs due to the "Update Root Certificates" component, which is installed by default as part of Windows Server 2003 installation. For more information on this component and reasons for errors, see the following articles on the Microsoft website:

"http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03mngd/04_s3cer.mspx"

"http://support.microsoft.com/default.aspx?scid=kb;en-us;317541"

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

- Uninstall the "Update Root certificates" component as detailed 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 RED HAT ENTERPRISE LINUX OPERATING SYSTEMS
==========

* When starting Server Administrator from the Red Hat Enterprise Linux console, kernel log messages may appear. To suppress 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.

* On systems running Red Hat Enterprise Linux 4 Gold (x86 and x86_64 architectures) with DRAC 4 installed, the CD device will be listed under a Tertiary Channel instead of the Primary Channel. This issue has been resolved in Red Hat Enterprise Linux 4 Update 2.

* In the initial release of Red Hat Enterprise Linux 4, the SNMP daemon will time-out when walking the network configuration section of the MIB II tree on systems running the x86_64 operating system. This results in missing data while trying to manage this server using Dell IT Assistant. This issue can be fixed by updating net-snmp-libs-5.1.2-11.EL4.6 found in Red Hat Enterprise Linux 4 Update 3.

* For systems running a supported Red Hat Enterprise Linux operating system, kernel driver messages such as "AAC_ChardevOpen" are sometimes 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.

==========

ISSUES FOR SERVER ADMINISTRATOR RUNNING ON SUSE LINUX ENTERPRISE SERVER OPERATING SYSTEMS

==========

* On systems running SUSE Linux Enterprise Server 9 SP3, an incorrect IP address for the system may be displayed in SNMP applications. There is a bug in net-snmp 5.1.3.1-0.6 RPM and earlier versions where the SNMP daemon provides an incorrect SNMP response to a request for a network interface address. For example, if a network interface has an IP address of 192.168.1.1, the SNMP daemon will provide an IP address of 192.168.1.1.0.0.0.0. This may have adverse affects when trying to manage the system and may affect Dell IT Assistant operations.

  To avoid this issue, update the net-snmp RPM to version 5.1.3.1-0.13 or later via YaST Online Update.

* On systems running SUSE Linux Enterprise Server 9 SP3, Server Administrator Web interface may freeze when clicking on components in the tree view (left pane of the interface).

  To correct this issue, restart the connection service by running

  "srvadmin-services.sh restart" or
  "omconfig system webserver action=restart"

  from the command line. You must refresh the web interface and log back into Server Administrator to continue.

==========
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 message "Error! User has insufficient privileges to run command: omconfig" 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.

* On a Windows 2000 system, it is strongly recommended that you update to Service Pack 4 or later. Service Pack 4 is required to fully support SAS technology.

* On a Red Hat Enterprise Linux 3.x system, Update 3 or later is required for Storage Management and Update 7 or later is required to fully support SAS technology. Dell strongly recommends that you use the Red Hat Network (RHN) service to update your system software with the latest update package before deploying your system. Go to www.redhat.com to access the RHN service and download updates.

* 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" might 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.

* If a virtual disk, using the GUI, is renamed with 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 after 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 the bottom of the side-by-side blue text boxes.

==========
ISSUES FOR REMOTE ACCESS
==========

NOTE: The Remote Access Service is supported on PowerEdge 650, 700, 750, 800, 830, 840, 850, 860, 1600SC, 1650, 1750, 1800, 1850, 2600, 2650, 2800, 2850, 4600, 6600, 6650, 6800, and 6850 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 THE DELL REMOTE ACCESS CONTROLLER 5

Download the DRAC 5 readme from support.dell.com for the latest information about all known issues.

Download the DRAC 5 readme from support.dell.com for the latest information about all supported web browsers and managed server operating systems.

* DRAC 5 support on SUSE Linux Enterprise Server (version 10) is limited to the Manage Node and to the CLI only. DRAC 5 does not support the Out of Band GUI on the Management station.

* DRAC 5 GUI supports Mozilla Firefox 1.0.7 only (32-bit)

* DRAC 5 GUI supports only 32-bit browser editions.

ISSUES FOR THE DELL REMOTE ACCESS CONTROLLER 4

Download the DRAC 4 readme from support.dell.com for the latest information about all known issues.

* Perform the following steps if you do not see the "Remote Access Controller" properties tab in the Server Administrator user interface, after installing it on a system with DRAC 4:

  1. Make sure that the "Remote Access" service is running.

  2. Refresh the Server Administrator user interface.

     If the "Remote Access Controller" properties tab still does not appear:

     - Close the Server Administrator user interface.

     - Restart the "DSM SA Data Manager" service.

     - Restart the "Secure Port Server" service.

     - Open the Server Administrator user interface and log in.

* When connecting to a remote DRAC 4 using a Mozilla Web browser from a Linux client, the Virtual Media feature may not be available. The browser displays the error: "Virtual Media Plug-in is not installed or running". This issue is caused by new Java applet security features of Mozilla 1.7.3 and newer. Perform the following steps to manually install the plug-in for that specific browser:

  1. Log in to DRAC 4 and navigate to the "Properties" page.

  2. Change the Web address in the browser window from "https://<DRAC4-IP-address>/cgi/main" to "https://<DRAC4-IP-address>/rac4vm.xpi", and press Enter.

     Mozilla prompts you with an "Opening rac4vm.xpi" dialog, allowing you to save the file to your local file system.

  3. Click "OK" and save the file to a temporary location (should be your home directory, by default).

  4. After saving the file, close the browser.

  5. Restart the browser, and specify the Web address of the "rac4vm.xpi" file (for example: file:///root/rac4vm.xpi).

6. Mozilla presents you with the "Software Installation" dialog:
   Click the "Install" button to continue.

7. After installation completes, close and restart the browser.

8. Now, log in to DRAC 4, and navigate to the Virtual Media link.
   The plug-in is installed and ready to use.

9. At this point, delete the "~/rac4vm.xpi" file.

* 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)

ISSUES FOR DELL REMOTE ACCESS CONTROLLER III, DELL REMOTE ACCESS CONTROLLER III/XT, ERA, AND ERA/O

Download the readme for your RAC type from support.dell.com for
the latest information about all known issues.

* Remote Access Dial-Up Settings: If you change a DRAC III modem
  "Dial Mode" setting to "Tone" or "Pulse" using Server Administrator,
  IT Assistant displays the opposite setting.

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 "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 the fluctuations in the watchdog timer, the "Last Crash
  Screen" may not be captured when the Automatic System Recovery is
  set to a value 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 up, you must configure the watchdog timer using the Server Administrator GUI. In the Server Administrator GUI, click the "Properties" tab and ensure that "Auto Recovery" is selected. The default value of the "Action On Hung Operating System Detection" setting is "None". "None" indicates that detection will not be performed.

* RAC firmware 2.0 and 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 the following four 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 userid 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.

DRAC III ISSUES FOR WINDOWS OPERATING SYSTEMS

---

* A dial-up network connection to the remote access controller is established by the RAC managed system software installer. The RAC software will not work properly if this dial-up connection is deleted or if a proxy is set up in the Internet settings. An InstallPPP utility is provided with the RAC software to restore the RAC PPP connection. This utility can also correct Internet connection problems with proxy server settings, when using the Windows 2003 operating system. You can run the utility from the Windows command prompt with the argument "CreateRACConnection" as shown below:

  c:\>installPPP CreateRACConnection

* Applications that use InstallShield 3.x to install software may take longer to install if RAC Services are running. To reduce the software installation time, stop RAC Services before performing the installation. You must restart RAC Services after the installation is complete.

* Due to functional details that are specific to Windows Dynamic DNS servers, the RAC internal PPP IP address is broadcast to the Dynamic DNS service on servers running Windows. The Dynamic DNS service stores that particular IP address in its DNS look-up table and associates it with the name of the system that hosts the RAC. This action causes problems with Active Directory under Windows. The default value for a RAC's internal PPP IP address is 192.168.234.235, but the address can be changed by the user. This issue is a known problem, and there is an article and a hot fix available from Microsoft. The Knowledge Base article number is Q292822. Downloading the hot fix and implementing the steps in the article solve the problem.

* If you have used the "Systems Management Consoles" CD version 3.1, or earlier, to install RAC management station software on any system running a Windows operating system, you must remove any previous versions of the RAC management station software before installing a later version of the RAC management station software.

  To remove the RAC management station software on Windows, perform the following steps:

  1. Insert the "Systems Management" CD into the CD drive.

2. When the installation application starts, click "Exit".

3. Open a command shell window:

a. Click the "Start" button, and then click "Run".

b. In the "Run" dialog box, type the following command and then press <Enter>:

cmd

4. Start the Install Shield uninstallation program to remove software:

a. In the command shell window, type the following line (replacing x: with the actual drive letter of your CD drive, such as d:):

x:\rac20\mtpkg\setup.exe

b. Select "Remove", and then click "Next".

c. Click "OK".

d. Click "Finish".

5. Close the command shell window.

* On systems running Windows, the RAC installation process requires a virtual modem connection named RACPORT to communicate between the operating system and the RAC. When any modem is added to the system, the operating system automatically creates a virtual fax device icon in the printers folder. The fax icon is not used by the RAC and can be deleted or ignored.

* The mouse movement on a local Windows system may appear jerky and erratic during DRAC III console redirection. This behavior is evident especially when using menus or opening windows.

* Resizing the Windows desktop to a resolution of 640 x 480 causes some information to not be visible in the browser window when using the RAC Web-based interface. This issue occurs in Internet Explorer. To view a screen in its entirety when using a resolution of 640 x 480, you must enlarge the browser window.

* While installing applications such as SQL Server 2000,if the RAC device (PCI Function 0, PCI Function 2 and RAC Virtual UART Port) is disabled and the RAC service is running, you may experience problems such as an application hang. To successfully install these applications you can either re-enable the driver else you can stop the service.(129915)

DRAC III ISSUES FOR RED HAT ENTERPRISE LINUX OPERATING SYSTEMS

---

* While installing the Dell OpenManage systems management applications through the Nautilus File Manager, you must use the "Run" button and not the "Run In Terminal" button after choosing the "start.sh" script from the File Manager's file list. Use the "Run In Terminal" button for applications that do not open a window of their own (the "start.sh" script opens its own window). If you choose "Run In Terminal", you must restart the racvnc service after installing Dell OpenManage systems management applications by typing the following command:

  "service racvnc restart"

* When using Console Redirection on a managed system running Red Hat Enterprise Linux, the focus (cursor moved back over an object) follows the cursor. Occasionally, the text windows in Console Redirection lose focus. Before attempting to type in a text window in a Console Redirection window, click the mouse in the text window's spacebar or top menu bar to ensure that your target text window has the focus on the correct window or application that you are attempting to use.

##

Trademarks used in this text: "Dell", "PowerEdge", "PowerVault", and "OpenManage" are trademarks of Dell Inc.; "Intel" is a registered trademark of Intel Corporation; "Microsoft", and "Windows Server" are registered trademarks of Microsoft Corporation; "Red Hat" is a registered trademark of Red Hat, Inc.; "SUSE" is a registered trademark of Novell Inc.; "EMC" and "Navisphere" are registered trademarks of EMC Corporation; "VERITAS" is a registered trademark and "Backup Exec" is a trademark of VERITAS Software Corporation.

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.

February 2007