##

DELL(TM) OPENMANAGE(TM) SERVER ADMINISTRATOR VERSION 6.0.3 README

##

Version 6.0.3
Release Date: March 2009

NOTE: This readme provides information for Dell OpenManage Server
    Administrator version 6.0.3.

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". You can access the documentation from the
Dell support website at "support.dell.com".

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 OpenManage Server Administrator
  Installation Guide for VMware(R) ESXi 3.5. for the latest and
  complete list of supported operating systems and platforms.

  NOTE: See the "ISSUES FOR DRAC 5" section of this document for the
  supported managed server operating systems by DRAC 5.

===
SUPPORTED WEB BROWSERS
===

* Microsoft Internet Explorer 6.0 (SP2) on Microsoft Windows
  Server 2000.

* Microsoft 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 Enterprise Linux (AS, ES, WS) version 4.7 and
  version 5.2 and SUSE Linux Enterprise Server version 10.

  NOTE: See the "ISSUES FOR DRAC 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 results.

  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 1.0 or greater is required for systems
  installed with iDRAC.

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


```
#######################################################################
RELEASE HIGHLIGHTS
#######################################################################
```

* Added support for the following operating systems:

  - Microsoft(R) Windows(R) XP SP2

  - Microsoft(R) Windows(R) Vista - Business and Enterprise
    editions.

  - VMware(R) ESX Version 3.5i Update 4 or later.

* See the "Dell OpenManage Server Administrator Installation Guide
  for VMware(R) ESXi 3.5." for a complete list of supported Dell
  systems and operating systems.


```
#######################################################################
INSTALLATION
#######################################################################
```

For complete installation instructions, see the
"Dell OpenManage Server Administrator Installation Guide
 for VMware ® ESXi 3.5.".

```
#######################################################################
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 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, 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 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 Dell Systems

  Dell SNMP MIB files for Dell systems allow customers 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 Response Time

  On Dell PowerEdge x9xx and later systems, the response times
  for some parts of the OMSA GUI and CLI have increased to several
  seconds because some of the BMC/iDRAC data is no longer cached
  by Server Administrator. The data must be retrieved from the
  BMC/iDRAC when requested by the user.

  The following Server Administrator GUI pages are of note:
  - Server Administrator home page on log in
  - Remote Access -> Users
  - Alert Management -> Platform Events

  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.

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

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

===
NOTES FOR THE REMOTE ACCESS SERVICE
===

* This service is supported on Dell 6950, 2970, R200, M600, M605, R805,
  and R900 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):
  Integrated Dell Remote Access Controller (iDRAC), DRAC5.

* 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, 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, follow 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 RUNNING ON ALL SUPPORTED OPERATING
SYSTEMS
===

* On PowerEdge 1950, 2950 and PowerVault NX 1950 systems with internal
  USB, BIOS setting configuration for Internal USB Port is possible
  only if UA (User Accessible or external) USB ports are set to
  "All Ports On". If UA USB ports are not set to "All Ports On" and
  user tries to configure BIOS setting for Internal USB Port using
  Server Administrator GUI, the configuration will appear to be
  successful but the changes will not take effect on next reboot. If
  UA USB ports settings are changed from "All Ports On" to "All Ports
  Off" or "Only Back Ports On", it will automatically set the Internal
  USB Port to Off on next reboot.

* 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 an 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.

* 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 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.

* 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 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.

* 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 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
  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 log-in session) for
  that user. If a user (or root user) tries to log in to multiple
  Mozilla/Firefox browser instances, then only the last session is
  active and the other older sessions display access forbidden upon
  the next access.

* 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 time zone to a new time zone,
  Server Administrator session management will not display the time in
  the new time zone specified. Server Administrator needs to be
  restarted so that the correct time zone time is displayed in the
  Session Management page.

* Server Administrator Auto Recovery feature may execute the
  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.
  The issue is more prevalent on 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 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.

  For example, if the ip address of the host is 192.168.2.3, and
  Server Administrator listens to port 1311, then use the
  URL 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, the Server Administrator GUI may become
  unresponsive for approximately 30 seconds. [152755]

* If the CPU throttles, the following message in the hardware System
  Event Log (SEL) will be displayed with an unknown severity:
  System Board Power Optimized: Performance status sensor for System
  Board, unknown event.
  [175331]

* 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
  alphanumerics. [185770

* While installing Windows Server 2008 or post installation,if you
  set the Time and Currency formats to any of the newly added
  languages (in comparison with Windows Server 2003), then DSM SA
  Connection service and DSM SA Shared Service of OpenManage Server
  Administrator may fail to start and Command Line Interface options
  may fail to execute. [171026]

* The selection of default option for front panel LCD in Server
  Administrator will display "Model Name" where as the default is
  "Service Tag" on the physical LCD.

* In case server administrator does not respond to your
  selections on the component tree, perform the following steps.

  1. Click on Preferences. This will take you to the preferences page
  2. Click on the Server administrator
  3. Now the items on the front page might respond to your click.

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

  In VMware(R) ESXi, the filesystem is a ramdisk. Modifications made
  to the files within the filesystem are generally not persisted
  across reboots, with the exception of designated configuration files.
  These files are persisted to disk periodically and on ESXi shutdown.
  If the system is reset without a graceful shutdown of ESXi before
  changes to the designated configuration files are persisted to 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
  is reset without a graceful shutdown of ESXi before the changes
  to the configuration file are persisted to disk, the user-defined
  thresholds become the default thresholds. [277439]

* On VMware ESX 3i operating system, Server Administrator supports
  a maximum command log file size of 1 MB. This is configured by
  default.

===
ISSUES FOR SERVER ADMINISTRATOR RUNNING ON ALL MICROSOFT WINDOWS
OPERATING SYSTEMS
===

* 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",
  right-click "DSM SA Connections Services" and select "Start".

* The Server Administrator might show a blank page after the browser
  is refreshed (using <F5> or clicking the browser "Refresh" 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]

* Users may not get appropriate privileges in Server Administrator
  GUI if:
  A) user is part of an Active Directory group which is in turn
     part of another group and

   B) the user launches Server Administrator using desktop icon and
      Single Sign-on is enabled.
   [167801].

* On operating system bootup you may occasionally get an error message
  popup
  – fwInvn32.exe encountered a problem and needed to close. [272344]

* To configure the Active Directory product name for Server Administrator:
  1. Locate the omsaoem.ini file in your installation directory.
  2. Edit the file to add the line "adproductname=text", where text
     is the name of the product object that you created in Active
     Directory. For example, the omsaoem.ini file will contain the
     following syntax if the Active Directory product name is configured
     to 'omsaApp':

     productname=Server Administrator
     startmenu=Dell OpenManage Applications
     autdbid=omsa
     accessmask=3
     adsupport=true
     adproductname=omsaApp

  3. Restart the DSM SA Connection Service after saving the omsaoem.ini
     file to the disk.
  [278267]

* If the system running Server administrator Web server has default proxy
  settings (not the browser proxy settings), the managed system login may
  fail. To fix this problem, the managed system should be accessed directly
  or by bypassing the proxy. You can use the Proxy Configuration Tool to
  configure the direct access or the bypass proxy setting.
  See http://msdn2.microsoft.com/en-us/library/aa384069.aspx for
  details on using the Proxy Configuration Tool.
  [284342]

* Some Internet browsers (e.g. Microsoft Internet Explorer, Mozilla
  Firefox etc) 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 other sessions expire. As a result, a
  "403 forbidden" error message could be displayed in the other
  session windows. Also, if a user has logged in to multiple browser
  instances, the session management window displays only one
  session (the last log-in session) for that user. To avoid these
  issues, access Server Administrator Web Server using a single
  browser instance.[280268]

==
ISSUES FOR SERVER ADMINISTRATOR RUNNING ON MICROSOFT WINDOWS 2003
OPERATING SYSTEMS
==

* The following warning messages that appears after installing Server

Administrator 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"). 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"
   - "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 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

After upgrading Window Server 2003 x64 to Windows Server 2008 x64
with Server Administrator 6.0.3 installed, the Server Administrator
display does not show all of the expected instrumentation pages.
The Server Administartor 6.0.3 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.

===
ISSUES FOR STORAGE MANAGEMENT SERVICE
===

The following are open issues regarding the Storage Management
Service.

STORAGE MANAGEMENT SERVICE ISSUES FOR ALL SUPPORTED OPERATING SYSTEMS
----

* 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.

==
ISSUES FOR REMOTE ACCESS
==

NOTE: The Remote Access Service is supported on PowerEdge 6950, 2970,
   R200, M600, M605, R805, and R900 systems only.

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

ISSUES FOR DRAC 5

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

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

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

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

ISSUES FOR ALL OPERATING SYSTEMS
----

* 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

* 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.

* 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.

##