Integrated Dell Remote Access Controller 6 (iDRAC6) Version 1.90

Release Notes

Integrated Dell Remote Access Controller6 (iDRAC6) is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for the Dell PowerEdge systems.

What's New

- Regular Maintenance
- Open source components upgraded(openssl, openldap, libxml)
- Thermal improvement for DR4000 PCI card
- Added New racadm command support for setting ssl Encryption Strength
- Enabled iDRAC support for the Qlogic P3+ Dual port 10Gb SFP+/DA on R715, R815 and R910
- Enabled iDRAC support for the Broadcom 57810 Dual Port 10Gb Base-T-CAN on R715, R815 and R910
- Enabled iDRAC support for the Broadcom 57810 Dual Port 10GbE SFP+
- Converged Network Adapter on R715, R815 and R910
- Enabled iDRAC support for setting Power Supply upper non critical threshold through OMSA and IPMI cmd.
- Enabled iDRAC support for the Emulex LPe16000 Single Port FC16 HBA
- Enabled iDRAC support for the Emulex LPe16002 Dual Port FC16 HBA
- Added the following new racadm commands:
    - racadm sslEncryptionStrength get
      Returns the current encryption strength setting on iDRAC.
      Legal values: 0 or 1 (0= auto negotiate, 1= 128-bit or higher)
    - racadm sslEncryptionStrength [set <value>] [--webserverrestart]
      Sets the encryption strength on iDRAC.
      webserverrestart and set <value > are optional. [--webserverrestart] applies the changes.
      <value>: 0 or 1, (0 = auto negotiate, 1 = 128-bit or higher) None

Hardware and Software Requirements

Supported Systems

iDRAC6 is supported on the following Dell PowerEdge systems:

- DELL PowerEdge R710
- DELL PowerEdge R815
- DELL PowerEdge T410
- DELL PowerEdge R715
- DELL PowerEdge R210
- DELL PowerEdge R510
- DELL PowerEdge T310
- DELL PowerEdge R910
- DELL PowerEdge R310
- DELL PowerEdge R415
- DELL PowerEdge R515
- DELL PowerEdge T610
- DELL PowerEdge R610
- DELL PowerEdge R410
- DELL PowerEdge R810
- DELL PowerEdge T710
- DELL PowerEdge R210 II
- DELL PowerVault DR6000

- DELL PowerVault NX3000
- DELL PowerVault NX3100
- DELL PowerVault NX200
- DELL PowerVault DL2100
- DELL PowerVault NX300
- DELL PowerVault DL2200
- DELL EqualLogic DX6004S
- DELL EqualLogic DX6000
- DELL EqualLogic FS7500
- DELL EqualLogic DX6012S
- DELL EqualLogic DX6000G

Supported Managed Server Operating Systems for iDRAC7

The following operating systems support iDRAC6

- Microsoft(R) Windows Server(R) 2003 family
  The Windows Server 2003 family includes:
  - Windows Server 2003 R2 (Standard, Enterprise, and DataCenter Editions) with SP2 (x86, x86_64)
  - Windows Server 2003 Compute Cluster Edition
- Microsoft Windows Server 2008 SP2 (Standard, Enterprise, and DataCenter Editions) (x86, x86_64)
- Microsoft Windows Server 2008 EBS x64 SP1 (Standard and Premium Editions)
- Microsoft Windows Server 2008 R2 SP1 (Standard, Enterprise, and DataCenter Editions) (x86_64)
- Microsoft Windows Server 2008 HPC Edition Server R1/R2 SP1
- SUSE(R) Linux Enterprise Server (SLES) 10 SP3 (x86_64)
- SUSE(R) Linux Enterprise Server (SLES) 10 SP4 (x86_64)
- SUSE Linux Enterprise Server (SLES) 11 SP1 (x86_64)
- SUSE Linux Enterprise Server (SLES) 11 SP2 (x86_64)
- Red Hat(R) Enterprise Linux (RHEL) 5.5 (x86, x86_64)
- Red Hat(R) Enterprise Linux (RHEL) 6.0 (x86_64) SP1
- Red Hat(R) Enterprise Linux (RHEL) 5.5 (x86, x86_64) SP7
- Red Hat(R) Enterprise Linux (RHEL) 5.8 (x86, x86_64)
- Red Hat(R) Enterprise Linux (RHEL) 6.2 (x86, x86_64)
- Hyper-V(TM) and Hyper-V R2
- VMware(R) ESX 4.0 Update 3
- VMware(R) ESX 4.1 Update 1
- VMware(R) ESX 5.0
- ESXi(TM) 4.0 Update3 Flash and HDD
- ESXi(TM) 4.1 Update 1 Flash and HDD
- ESXi(TM) 5i
- XenServer(TM) 5.6 HDD
- XenServer(TM) 5.6 FP1 HDD

Note: Use the Dell-customized ESXi 4.0 Update 1 Embedded edition. This image is available at **support.dell.com** and **vmware.com**. The remote deployment and local installation of ESXi through Virtual Media is not supported for

standard ESXi Embedded version 4.0, as the installation may fail with the error message, "Installation failed as more than one USB device found."

Supported Web Browsers for iDRAC7

- Microsoft Internet Explorer(R) 7.0 for Windows Server 2003 SP2, Windows Server 2008 SP2, Windows XP 32-bit SP3, and Windows Vista(R) SP2
- Microsoft Internet Explorer 8.0 for Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2 x64, Windows XP 32-bit SP3, Windows 7,and Windows Vista(R) SP2. Internet Explorer 8 requires Java(TM) Runtime Environment (JRE) version 1.6.14 or later.
- Microsoft Internet Explorer 8.0 (64-bit) for Windows 7 (x86_64), Windows Vista (x86_64) and Windows Server 2008 R2 (x86_64),Windows Server 2008 SP2 (x86_64), Windows Server 2003 SP2 (x86_64)
- Microsoft Internet Explorer 9.0 for Windows Vista (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows 7 (32-bit) (64-bit) or higher, Windows Server 2008 (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows Server 2008 R2 64-bit
- Mozilla(R) Firefox(R) 3.5 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 x64 R2, Windows Vista SP2, Windows 7 x64
- Mozilla(R) Firefox(R) 4.0 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Vista SP2, Windows 7
- Mozilla(R) Firefox(R) 6 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 x64 R2, Windows Vista SP2, Windows 7 x64.
- Mozilla(R) Firefox(R) 7 on Windows XP 32-bit SP3, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 x64 R2, Windows Vista SP2, Windows 7 x64.
- Mozilla(R) Firefox(R) on SLES 10 x64 SP3, SLES 11 x64 SP1, RHEL 5.5 and RHEL 6.0 x64 Native version.

Installation

For more information about iDRAC6, including installation and configuration information, see the "Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise Version 1.70 User Guide" and the "Dell OpenManage(TM) Server Administrator User's Guide." These documents are located on the Dell Support website at "support.dell.com/manuals." On the "Manuals" page, click "Software" > "Systems Management". Click on the appropriate product link on the right-side to access the documents.

Upgrade

Upgrading from iDRAC6 versions 1.85 to 1.90.

Uninstallation

- Use the rollback feature to uninstall version 1.90.
- System purchased with new eMMC cards and 1.80 iDRAC6 firmware version, firmware downgrades are not allowed to lower version.
- On certain hardware configurations, based on the firmware release, firmware downgrades are not allowed.

Open Issues and Resolutions

Issue 1

Description

Sometimes the "Save As" and "Clear Log" buttons on the "Remote Access" > "Logs" > "iDRAC Log" page may disappear when you mouse over these buttons. This is a known limitation with the GUI.

Resolution

To resolve this, click "Refresh".

Issue 2

Description

On some Windows operating systems, under certain conditions, the iDRAC vmcli.exe fails. This is due to the run-time components of Visual C++(R) Libraries (VC++ 2008 redistributable package) required to run applications that are not available.

Resolution

To resolve this, download and install Microsoft Visual C++ 2008 Redistributable Package (x86) from the following location:

microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en.

Issue 3

Description

When you try to upload any files other than the original SSL certificate files in the "Upload Certificate" page, iDRAC GUI may log out.

Resolution

Login to the GUI again and upload the correct SSL certificate.

Issue 4

Description

If you add more than 800 work notes, the GUI page may take additional time to load the page. This is due to huge amount of data that needs to be transacted between the GUI and iDRAC6.The newly added work notes may not be displayed after the page is loaded.

Resolution

To resolve this click "Refresh"

Issue 5

Description

After adding or removing new hardware, system inventory page may not update the changes automatically. This is because, inventory data collected during manufacturing process may not be updated with new changes.

Resolution

Select "Cntl+E" during BIOS POST and enable "Collect System Inventory on reboot". Save and exit from "Cntl+E" option, then reboot the system to collect new system inventory. After the Inventory is collected, the GUI “System Inventory” page displays correct Hardware and software inventory data.

Issue 6

Description

In the “System Details” page, “Virtual MAC” field is not populated if system inventory is not run from iDRAC GUI before accessing this page. This is because the inventory data may not be available for Virtual MAC to display

Resolution

Click “System Inventory” on the iDRAC GUI homepage. Ensure that inventory data is displayed on the “System Inventory” page. After the data is loaded, click the “System Details” tab. The “Virtual MAC” field displays inventory data, if the system supports this feature.

Issue 7

Description

Accessing iDRAC GUI in IPv6 network with Mozilla Firefox 4.0 or later[Mozilla Firefox 5.0], and accepting the CSR certificate displays an error message, "An error has occurred during a connection to <server certificate info>, Peer certificate issuer has been marked as not trusted by the user. (Error code:sec_error_untrusted_issuer)."

Resolution

Create a certificate request and issue it to a trusted domain. Register it to a domain DNS server. Use a trusted domain name, instead of the IPv6 address.

Issue 8

Description

The RACADM Command Line Reference Guide for iDRAC6 1.7, iDRAC6 3.2, and CMC 3.2 defines, RACADM command "ärp" displays interface as "Device". However, for Monolithic servers interface is displayed as "iFace".

Issue 9

Description

When a storage enclosure is disconnected or accidentally removed, the corresponding status of its components (that is, EMM, PSU, fan, and temperature sensors) are reported as critical. IDRAC browse a page that uses JavaScript functions to retrieve page data, the progress bar in Internet Explorer may not always be accurate.

Issue 10

Description

The iDRAC User Guide 1.7 defines, disabling Smart Card Logon sets the CLI out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM to their default state. This should be read as "On disabling Smart Card Logon, CLI out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM retain their state".

Issue 11

Description

To successfully launch Virtual Media, ensure that you have installed a 64-bit JRE version on a 64-bit operating system with 64-bit browser or a 32-bit JRE version on a 32-bit operating system with 32-bit browser. iDRAC6 does not support 64-bit ActiveX versions. Also, ensure that for Linux, the "compat-libstdc++-33-3.2.3-61" related package is installed for launching Virtual Media. On Windows, the package may be included in the .NET framework package.

Issue 12

Description

The RACADM Command Line Reference Guide for iDRAC6 1.7, iDRAC6 3.2, and CMC 3.2 defines that the RACADM command "racdump" displays Trace log information, RAC event log, and System event log. There is a separate command available to display Trace logs, RAC logs, and SEL logs.

Note: You must disable the Internet Explorer "Enhanced Security Mode" for the Java-based virtual console and virtual media plug-in to function properly. Else, specify the ActiveX plug-in in the iDRAC6 configuration instead of Java. In addition, you must add the iDRAC6 web URL to the Intranet security zone only. Also, this zone settings must be "Medium-Low" or lesser, for the control to function properly.

Issue 13

Description

Integrated Dell Remote Access Controller 6 (iDRAC6) Version 1.7 User Guide defines the GUI interface link as "Remote Access" instead of "iDRAC Settings".

Issue 14

Description

The expiry date for iDRAC default certificate is 2023. To get this updated Certificate, clear the "Preserve Configuration flag" option while updating iDRAC firmware through GUI. Make sure to delete cache from the GUI (IE as well as Firefox).

Firefox web browser might encounter an error if the certificate contains the same serial number as another certificate. Use the following link or procedure to resolve the same.

(support.mozilla.com/en-US/kb/Certificate%20contains%20the%20same%20serial%20number%20as%20another%20certificate)

Resolution

Delete your old exception and use temporary exceptions for subsequent visits to the iDRAC page.

To delete your old exception:

1. On the Firefox window, click "Firefox" and then click "Options."
    - For Windows XP, click “Tools” and then "Options."
    - For Linux OS, click "Edit" and then "Preferences."
2. Select the "Advanced" panel, and then click the Encryption tab.
3. Click "View Certificates" to open the Certificate Manager window.
4. In the Certificate Manager window click the "Servers" tab.
5. Identify the item that corresponds to the site that generates the error.

   Note: The Certificate Authority (CA) for that server - the CA name appears above the site name.
6. Click on the server certificate that corresponds to the site that generates the error and press "Delete."
7. Click OK when you are prompted to delete the exception.
8. Click the "Authorities" tab and select the item that corresponds to the CA that you noted earlier and then press "Delete."
9. Click OK when you are prompted to delete the exception.

To add a temporary exception to allow access to the page:

When you access the iDRAC page, an “Untrusted” error message is displayed.

1. Click on the "I Understand the Risks" link at the bottom of the error.
2. Click on “Add Exception…” to open the Add Security Exception window.
3. Click “Get Certificate” to fill in the Certificate Status section of the Add Security Exception window.
4. Click to un-check the “Permanently store this exception” option.
5. Click “Confirm Security Exception” to close the Add Security Exception window.

   The iDRAC page gets loaded.

Issue 15

Description

When the Certificate Authority(CA) is enabled, if we specify Domain Controller(DC) as FQDN and Global Catalog(GC) as IP address, Test settings “Authentication” fails and normal login succeeds

Expected Behavior : Test settings “Authentication” should be succeeded by using DC FQDN.

Resolution

User should specify the FQDN for GC, then test settings Authentication will be succeeded.

Issue 16

Description

SSH server takes more time to establish connection from putty client.

Resolution

For improving the performance, change the order of Key exchange algorithm in Putty ssh configuration:

1. Open Putty
2. Expand SSH tab
3. Click on "Kex"
4. Change order in Algorithm selection policy window
5. Connect to the SSH server

   The connection will be established quickly

Issue 16

Description

The following commands or command options are not supported for iDRAC6 1.90, though there are reference to these commands or options in RACADM Guide and iDRAC6 User’s Guide.

Resolution

For improving the performance, change the order of Key exchange algorithm in Putty ssh configuration:

- testkmsconnectivity
- sslcsrgen (type 2)
- sslcertupload (type 3 and type 4)
- sslcertdownload (type 3 and type 4)

Global Support

For information on technical support, visit **www.dell.com/contactus**.

For information on documentation support, visit **support.dell.com/manuals.** On the **Manuals** page, click **Software** ->**Systems Management.** Click on the specific product on the right -side to access the documents.

2012 – 6 **Rev. A00**