Integrated Dell Remote Access Controller 6 Version 2.91.02

Release Notes

Release notes

iDRAC is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge systems.

Version

iDRAC6 2.91.02

Release date

June 2018

Previous version

iDRAC6 2.90

Importance

URGENT: Dell highly recommends applying this update as soon as possible. The update contains changes to improve the reliability and availability of your Dell system.

Platforms affected

iDRAC6 is supported on the following systems:

- PowerEdge R710
- PowerEdge R815
- PowerEdge T410
- PowerEdge R715
- PowerEdge R510
- PowerEdge R410
- PowerEdge R610

What is supported?

Supported Managed Server Operating Systems

The following operating systems support iDRAC6:

- Microsoft Windows Server 2003 family:
  - 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 2012 (Standard, DataCenter, and Essentials Editions) (x86_64)
- Microsoft Windows Server 2008 HPC Edition Server R1/R2 SP1
- SUSE Linux Enterprise Server (SLES) 10 SP3 (x86_64)
- SUSE 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)
- SUSE Linux Enterprise Server (SLES) 11 SP3 (x86_64)
- SUSE Linux Enterprise Server (SLES) 11 SP4 (x86_64)
- Red Hat Enterprise Linux (RHEL) 5.5 (x86, x86_64)

- Red Hat Enterprise Linux (RHEL) 5.5 (x86, x86_64) SP7
- Red Hat Enterprise Linux (RHEL) 5.8 (x86, x86_64)
- Red Hat Enterprise Linux (RHEL) 6.0 (x86_64) SP1
- Red Hat Enterprise Linux (RHEL) 6.2 (x86, x86_64)
- Red Hat Enterprise Linux (RHEL) 6.3 (x86, x86_64)
- Red Hat Enterprise Linux (RHEL) 6.5 (x86, x86_64)
- Red Hat Enterprise Linux (RHEL) 6.7 (x86, x86_64)
- Hyper-V and Hyper-V R2
- VMware ESX 4.0 Update 3
- VMware ESX 4.1 Update 1
- VMware ESX 5.0
- ESXi 4.0 Update3 Flash and HDD
- ESXi 4.1 Update 1 Flash and HDD
- ESXi 5i
- XenServer 5.6 HDD
- XenServer 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

- Microsoft Internet Explorer 7.0 for Windows Server 2003 SP2, Windows Server 2008 SP2, Windows XP 32-bit SP3, and Windows Vista 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 SP2.
- Internet Explorer 8 requires Java 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.
- Microsoft Internet Explorer 10.0 for Windows Vista (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows 7 (32-bit) (64-bit), Windows 8(64-bit) or higher, Windows Server 2008 (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows Server 2008 R2 64-bit, Windows Server 2012 64-bit.
- Microsoft Internet Explorer 11 (only in IE10 Compatibility Mode) for Windows Vista (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows 7 (32-bit) (64-bit), Windows 8 (64-bit) or higher, Windows Server 2008 (32-bit) (64-bit) with Service Pack 2 (SP2) or higher, Windows Server 2008 R2 64-bit, Windows Server 2012 64-bit.
- Mozilla Firefox 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 Firefox 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 Firefox 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 Firefox 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 Firefox on SLES 10 x64 SP3, SLES 11 x64 SP1, RHEL 5.5 and RHEL 6.0 x64 Native version.
- Mozilla Firefox 15 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 Firefox 16 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.

What’s new

N/A

Fixes

- Fixed CVE-2018-1243: Improved encryption strength for remote RACADM to 128 bit.
- Fixed CVE-2018-1212: Command Injection using `Diag` commands. This version prevents web server from allowing command injection using the Troubleshooting-> Diagnostics page.

Important notes

- You must disable the Enhanced Security Mode in Internet Explorer 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.
- To successfully launch Virtual Media, make sure 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, make sure 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.
- When the SSL encryption strength is set to "168-bit or higher" or "256-bit or higher" and a downgrade is performed to firmware version 1.97 or lower, the encryption strength defaults to Auto-negotiate. After this if you upgrade the firmware to version 1.98, the encryption strength is set to the previously set "168-bit or higher" or "256-bit or higher" value.

Known issues

Issue 1

Description

In the iDRAC web interface, sometimes the **Save As** and **Clear Log** buttons on the **Remote Access**-> **Logs**-> **iDRAC Log** page may disappear when you mouse over these buttons.

Resolution

Click Refresh.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

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++ Libraries (VC++ 2008 redistributable package) required to run applications that is 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

Make sure the client system also has this DNS in its DNS list.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 3

Description

When you try to upload files other than the original SSL certificate files in the **Upload Certificate** page, iDRAC Web interface may log out.

Resolution

Log in to the Web interface again and upload the correct SSL certificate.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 4

Description

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

Resolution

Click **Refresh**.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

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

During BIOS POST, select <Ctrl+E> and enable Collect System Inventory on reboot. Save and exit from <Ctrl+E> option and then reboot the system to collect new system inventory. After the inventory is collected, the System Inventory page displays the correct Hardware and software inventory data.

Issue 6

Description

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

Resolution

In the iDRAC web interface, click **System Inventory** tab. Make sure 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 the inventory data, if the system supports this feature.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 7

Description

When you access the iDRAC web interface in IPv6 network with Mozilla Firefox 4.0 or later and accept the CSR certificate, it 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.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 8

Description

iDRAC browse a page that uses JavaScript functions to retrieve page data, the progress bar in Internet Explorer may not always be accurate.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 9

Description

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

Firefox web browser may display 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 the old exception and use temporary exceptions for subsequent visits to the iDRAC page.

To delete the 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.
3. Click the **Encryption** tab.
4. Click View Certificates to open the Certificate Manager window.
5. In the **Certificate Manager** window click the **Servers** tab.
6. 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.

7. Click on the server certificate that corresponds to the site that generates the error and click **Delete**.
8. Click **OK** when you are prompted to delete the exception.
9. Click the **Authorities** tab and select the item that corresponds to the CA that you noted earlier and then click **Delete**.
10. 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 I Understand the Risks.
2. Click **Add Exception**.... The **Add Security Exception** window is displayed.
3. Click **Get Certificate** to display the certificate in the **Certificate Status** section.
4. Clear the Permanently store this exception option.
5. Click **Confirm Security Exception**. The **Add Security Exception** window is closed. The **iDRAC** page is displayed.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 10

Description

When the Certificate Authority (CA) is enabled, the Domain Controller (DC) is specified as FQDN and Global Catalog (GC) as IP address, the authentication using Test Settings fails and normal login succeeds. The expected behavior is the authentication using Test Settings must succeed by using DC FQDN.

Resolution

Specify the FQDN for GC.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 11

Description

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

Resolution

For improving the performance, change the order of the key exchange algorithm in Putty SSH configuration:

1. Open **Putty**.
2. Expand **SSH** tab.
3. Click **Kex**.
4. Change the order in the **Algorithm selection policy** window.
5. Connect to the SSH server. The connection is established.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 12

Description

In a system with Microsoft Windows Server 2012 R2 and Dell OpenManage 7.4, the operating system name may not appear on the iDRAC6 web interface and RACADM. This is an intermittent issue.

Resolution

View the operating system name from the Dell OpenManage Server Administrator installed on the host system.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 13

Description

After updating Lifecycle Controller using the Remote Enablement (RE) Services, the Lifecycle Controller version is not updated in the System Summary page in the iDRAC web interface.

Resolution

Reboot iDRAC to view the updated Lifecycle Controller version.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 14

Description

The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC.

Resolution

There is no patch for this vulnerability it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include:

- Disabling IPMI over LAN if it is not needed.
- Using strong passwords to limit the successfulness of off-line dictionary attacks.
- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 15

Description

Telnet session is not getting cleared from ssninfo even after closing the session

Resolution

Manually delete the telnet session from GUI Session management

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Issue 16

Description

Health status is reported as critical when OS is shutdown

Resolution

If there are any critical events in SEL logs, SEL logs needs to be cleared. If SEL logs are cleared, health status is reported as expected.

Versions/Systems affected

All iDRAC6 supported Dell PowerEdge systems.

Limitations

None for this release.

Installation

Installation and Configuration Notes

For more information about iDRAC6, including installation and configuration information, see the Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise Version 1.95 User Guide and the Dell OpenManage Server Administrator User's Guide. These documents are located on the Dell Support website at dell.com/support/manuals.

Upgrade

N/A

Uninstallation

- Use the rollback feature to uninstall iDRAC6 version 2.80.
- 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.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area.

To contact Dell for sales, technical support, or customer service issues, go to dell.com/contactdell.

Accessing documents from Dell Support website

To access the documents from Dell Support website:

1. Go to dell.com/support.
2. Under Browse for a product, click View products.
3. Click Software and Security and then click the required link.
4. To view the document, click the required product version.

You can also directly access the documents using the following links:

iDRAC and LC documents	dell.com/idracmanuals
Enterprise System Management	dell.com/openmanagemanuals
Serviceability tools	dell.com/serviceabilitytools
OpenManage Connections Enterprise Systems Management	dell.com/OMConnectionsEnterpriseSystemsManagement
OpenManage Connections Client Systems Management	dell.com/OMConnectionsClient

Rev: A00