Integrated Dell Remote Access Controller 6 (iDRAC6) Version 3.85.03

Release Notes

Release notes

Integrated Dell Remote Access Controller 6 (iDRAC6) iDRAC is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for PowerEdge systems.

Version

iDRAC6 3.85.03

Rev A00

Release date

July 2017

Previous version

iDRAC6 3.80

Importance

RECOMMENDED: Dell recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).

Platform(s) affected

iDRAC6 is supported on the following PowerEdge systems in the PowerEdge M1000e system enclosure:

- PowerEdge M710HD
- PowerEdge M915

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 2008 HPC Edition Server R1/R2 SP1
- Microsoft Windows Server 2012 (Standard, DataCenter, and Essentials Editions) (x86_64)
- 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) 6.0 (x86_64) SP1
- 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) 5.9 (x86, x86_64)
- 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
- ESXi 5.1 U2
- ESXi 5.5
- 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 11.0 (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

The following are the new features in this release:

- OpenSSL upgraded to v1.0.2h
- Dropbear version upgraded to 2016.74
- Updated the signature on the Console Redirection plug-in to SHA2
- Updated ActiveX scauth plugin to SHA2
- Capability to disable TLS1.0 through CLI:
- Use racadm command
- racadm tlsencryptionstrength get/set.
- For usage of the command ,try racadm help tlsEncryptionStrength

Fixes

- CVE-2014-3566 (POODLE) Disable SSLv3 on port 5900.
- CVE-2015-2808 (Bar Mitzvah) Disable SSL RC4 Cipher.
- Fix for remote racadm to allow '&' as part of iDRAC User Password
- SSL certificate expiry date extended to Mar 18, 2027

Important notes

- To use Virtual Console with Java plug-in, the supported JRE version is 1.6.0_20 or higher.
- For Remote Enablement auto-discovery, make sure that the user ID on the provisioning server does not contain any spaces, as iDRAC6 user IDs may not contain spaces. If a user ID containing spaces is configured on the provisioning server, the auto-discovery process may be successful, but the resulting iDRAC6 account is not usable.
- The iDRAC6 can be updated using the DOS utility when DOS is booted using PXE. However, the new firmware image has to be on a local media on the system for this to work properly. Local media can be a RAMDISK, HD, or a USB key on the server. When the image is stored on non-local devices like a network drive, PXE server drive, and so on, the iDRAC6 update on multiple systems must be sequenced that is, it should be done one system after the other. After the first system completes the update, the second system starts the update. After the second system completes the update, the third system starts the update and so on.
- On systems running Windows operating systems, the Explorer window(s) for any media does not close automatically if you remove the media. You must close the window(s) after you remove the media. On systems running Linux operating systems, the file browser window(s) for any media closes automatically if you remove the media.
- iDRAC6 Linux DUPs do not support VMware ESX 4.0 operating systems. If the Linux DUP for iDRAC6 is run on VMware ESX 4.0, the DUP fails. You can update iDRAC6 using one of the following interfaces:
  - Chassis Management Controller Web interface
  - iDRAC6 web interface
  - Remote RACADM
- If the message "A webpage is not responding on the following website" is displayed in Internet Explorer 8.0, see:
  - //blogs.msdn.com/ie/archive/2009/05/04/ie8-in-windows-7-rc-reliabilityand-telemetry.aspx
  - //support.microsoft.com/?kbid=970858
- To execute iDRAC DUPs in XenServer 5.6, you must install the procmail package. You can install the procmail RPM in CentOS 5.4 i386, which can be downloaded from any public site that hosts CentOS packages. However, it is recommended not to install any RPMs manually on XenServer, instead download and install the OpenManage Supplemental Pack from support.dell.com. It contains the procmail package and is the supported method for installing third party packages and applications in XenServer.
- When using the virtual console on RHEL with Firefox browser, if the network connection to the iDRAC is lost a blank message box may be displayed. If the network connection is restored the message box may eventually display the "Virtual Console is restarted" message and then closes. Normally the message is

immediately displayed in the message box but on rare occasions this may not happen. The display of the message is controlled by the JRE and if the blank message box is seen this is not an iDRAC firmware issue.

- To launch iDRAC6 Virtual Console using Internet Explorer 7.0 32-bit with Java plug-in from Windows 2003 32-bit SP2 or R2 Enterprise Management Station:
  1. Open IE 7.0 browser window.
  2. Click Tools-> Internet Options-> Security tab.
  3. In the Select a zone to view or change security setting section, select Trusted Sites.
  4. Click Custom level.
  5. Under Downloads, enable Automatic prompting for the file downloads.
  6. Click OK and again click OK. The changes are applied.
- The WS-MAN CQL filtering implementation in this release is experimental, and it is recommended not to use this currently.
- The embedded NIC MAC addresses displayed under System-> Properties-> System Details are the server-assigned MAC addresses. If the MAC addresses are remotely managed or chassis-assigned, the active MAC addresses are available under System-> Properties-> WWN/MAC.
- When launching the iDRAC web interface and iDRAC virtual console from the Chassis Management Controller Web interface within a few seconds of each other, the iDRAC web interface may have a session timeout. This can also happen any time the virtual console is launched from the Chassis Management Controller after the iDRAC web interface has been launched from the Chassis Management Controller. This is expected behavior because of browser session management.
- Remotely managed MAC addresses require appropriate hardware and firmware. To fully enable remote management of MAC addresses, CMC 3.20 (or later) must be installed.
- In the iDRAC web interface, System-> Logs-> Work Notes page, the note about the length of a new work note indicates that the maximum number of characters supported is 50.
- When using the WS-MAN DCIM_RAIDService GetAvailableDisks method to retrieve specific RAID devices, the XML file passed to the command contains a “RaidLevel” value for the selection. No error checking is done on the RaidLevel Value. Therefore, if an incorrect or invalid value is specified, incorrect results may be returned (for example, “abcd” becomes “0”; “64.999” becomes “64”). The RaidLevel specified must be an appropriate integer RAID level value (“1”, “2”, “4”, “64”, “128”, “2048”, “8192”, “16384”, per DCIM_VirtualDiskView.mof).
- RACADM sslkeyupload command is not supported on the 11th generation of PowerEdge blade servers.

Known issues

Issue 1

Description

When the JRE is configured to verify the certificate against a Certificate Revocation List (CRL) and/or online certificate validation the certificate validation may sometimes fail. This is because the Certificate Authority (CA) that issued the certificate is not accessible due to connectivity problems or is not responding in a timely manner.

Resolution

Wait and retry at a later time.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 2

Description

Remote Services: When using TFTP to download an ISO image to the vFlash, if the image exceeds the free space on vFlash, an error message is not generated. However, subsequent operations on the ISO fails.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 3

Description

If you run Dell Update Packages (DUPs) when vFlash is in-use, the vFlash is disconnected and reconnected. If a write operation is in-progress, this action can corrupt the vFlash contents.

Resolution

Re-initialize the vFlash SD card.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 4

Description

In Internet Explorer 7.0, if you launch the iDRAC6 Virtual Console when several tabs are open, all the tabs are hidden while only the Virtual Console opens. If the tab warning is turned off and you close the Virtual Console, all the tabs and the browser close without warning.

Resolution

To prevent this, go to Internet Properties- > Tabs-> Settings and select the Warn me when closing multiple tabs option.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 5

Description

If a Virtual Media drive is disconnected using the OS eject option, then the drive may not be available until the operating system re-enumerates the USB devices.

Resolution

For the operating system to auto-detect the Virtual Media drive, the iDRAC6 Virtual Media device can be reattached.

To do this:

1. Go to System-> Virtual Console/Media-> Configuration.
2. Set the Attach Virtual Media option to Detach and click Apply.
3. Set the Attach Virtual Media option to Attach and click Apply.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 6

Description

The racresetcfg command in RACADM restores all properties to their default values except cfgDNSRacName in the cfgLanNetworking group.

Resolution

Not applicable.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 7

Description

When using a configuration file with RACADM to configure iDRAC6, changing objects that affect the network connection stops the rest of the configuration file from taking effect.

Resolution

Not applicable.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 8

Description

Using the iDRAC web interface to shut down the XenServer operating system by selecting Graceful Shutdown does not shut down the server.

Resolution

It is recommended that you use the shutdown menu option in the XenServer console or in the XenCenter management GUI.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 9

Description

TFTP firmware update from local RACADM does not work after a racresetcfg or if IPv6 addresses are used.

Resolution

Use the firmware RACADM for TFTP firmware update.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 10

Description

When using the Virtual Console that uses the Java plug-in with attached Virtual Media, occasionally when disconnecting the Virtual Media, the console also closes unexpectedly.

Resolution

Restart the Virtual Console to regain access.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 11

Description

During the SLES 11 installation through the *Dell Systems Management Tools and Documentation* DVD, if the DVD is connected through Virtual Media, the image installation may not proceed after the system configuration step. It displays a warning dialog message similar to the following:

"Empty destination in URL: hd:///install/?device=/dev/sdc1".

Resolution

To continue the installation, delete the question mark '?', refresh the URL and the installation will proceed. This issue is not seen when using the managed system's local CD/DVD or using the operating system DVD directly instead of the *Dell Systems Management Tools and Documentation* DVD.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 12

Description

Sometimes the Virtual Console feature of iDRAC becomes unavailable.

Resolution

Run the racadm racreset command to access the Virtual Console again.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 13

Description

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

Resolution

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

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 14

Description

When using the Virtual Media with recent Windows releases on the management station, the CD/DVD redirection may not work properly and may cause continuous USB bus resets if you have logged in using non-administrator account.

Resolution

Set the Attach Virtual Media option to Detach to stop the USB bus resets and allow CD/DVD redirection to work properly when you log in again with an Administrator's account.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 15

Description

When remote management is enabled, the WWN/MAC page may not immediately display the remotely enabled MACs and instead may display N/A under the remotely assigned column. This may happen when you navigate to the to the WWN/MAC page for the first time.

Resolution

If this happens, navigate to a different page in the iDRAC6 web interface and then return to the WWN/MAC page to see the remotely assigned MACs. Ensure the host system has booted before navigating to the WWN/MAC page when remote management is enabled.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 16

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 PowerEdge systems.

Issue 17

Description

Accessing the iDRAC virtual console displays UNKNOWN publisher name message during certificate download.

Resolution

Add the iDRAC certificate. To do so, right-click on the right corner of iDRAC web Interface URL and import the certificate.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 18

Description

Power monitoring graph is not visible in iDRAC web interface with Internet Explorer 9 and 10 browsers.

Resolution:

Use compatibility mode in browser settings.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 19

Description

The SD sensor states remain unchanged when the "Internal SD Card Port" BIOS option is toggled

Resolution

Upgrade to the latest supported BIOS for PowerEdge M910.

Versions/Systems affected

All iDRAC6 supported PowerEdge M910 systems.

Issue 20

Description

On the 11th generation of PowerEdge blade servers running Microsoft Windows Server 2012 R2 and Dell OpenManage 7.4, the operating system name may not appear on the iDRAC6 GUI or the RACADM CLI interface. This is an intermittent issue.

Resolution

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

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 21

Description

On PowerEdge modular servers with iDRAC6 version 3.75, the web GUI is inaccessible when the SSL encryption strength is set to 168-bit or higher or 256-bit or higher and firmware is downgraded to iDRAC6 version 3.65 or lower. However, the other interfaces are functional.

Resolution

Perform the following steps:

1. Launch the iDRAC GUI.
2. Navigate to iDRAC Settings-> Network/Security-> Services page.

3. Set SSL Encryption to Auto-Negotiate or 128-bit or higher.

   The browser session is terminated.

4. Launch a new browser session and perform the downgrade.

You can also run the following RACADM command and perform the downgrade:

```
racadm sslencryptionstrength set 0 (or 1)
```

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 22

Description

Incorrect values listed as Legal Values and Default value for the cfgLdapRoleGroupPRivelege command in the *iDRAC6 Enterprise for Blade Servers Version 3.5 RACADM Reference Guide*.

Resolution

The LDAP Role Group Privilege value may vary between 0x00000000 and 0x000001ff. The default value is 0x00.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 23

Description

After configuring the extended schema login, there is a possibility that the login through the extended schema may fail. This issue may occur if the Active Directory user does not have Administrator privileges.

Resolution

On Kerberos, add “Domain controllers” and “Domain admins”.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 24

Description

Virtual console fails to launch with JAVA plugin jre8u131

Resolution

Use lower version of Java plugins,

Recommend to use Java7u80 or Java8u121

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 25

Description

Racadm config –g cfgRacTuning command through local racadm does not enumerate the attributes of webserver configurations.

Resolution

Use cfgRacTuning command through Firmware racadm or remote racadm to enumerate the attributes of webserver configurations.

Versions/Systems affected

All iDRAC6 supported PowerEdge systems.

Issue 26

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 PowerEdge systems.

Limitations

When connecting to the iDRAC web interface using browsers supporting localized languages, some popups may have generic messages that are not localized in the title such as: "The page at //10.35.155.207 says:". This is a browser limitation and cannot be changed in the iDRAC.

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 for Blade Servers Version 3.50 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

If you are upgrading from iDRAC6 versions 2.1 or 2.2, you must first install iDRAC6 version 2.30 or 2.31 before installing the 3.30 version. If you are upgrading from the iDRAC6 versions older than 3.40, there can be a firmware update issue with Microsoft Internet Explorer.

Note: This issue started with Microsoft security update KB2618444 and fixed in iDRAC 3.40 release.

Resolution:

Upgrade 3.40 or higher firmware version using browsers other than IE or update firmware using other interfaces.

After updating 3.40 or higher firmware version using workaround methods, the subsequent firmware updates is successful with all supported methods.

Uninstallation

- Use the rollback feature to uninstall iDRAC6 version 3.85.
- System purchased with new eMMC cards and 3.30 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