iDRAC Service Module 2.4 Release Notes

Release Type and Definition

The Integrated Dell Remote Access Controller (iDRAC) Service Module is a lightweight optional software application that can be installed on Dell 12G Servers or later. The iDRAC Service Module complements iDRAC interfaces — Graphical User Interface (GUI), RACADM CLI and Web Service Management (WSMAN) with additional monitoring data. You can configure the features on the supported operating system depending on the features to be installed and the unique integration needs in your environment.

Version

2.4

Release Date

October 10, 2016

Previous Version

2.3

Importance

RECOMMENDED: Dell recommends applying this update during your next scheduled update cycle. This version contains some new features, feature enhancements and bug fix.

Supported Operating Systems

You have to manually configure the OS firewall settings after installing iDRAC Service Module to use the iDRAC Access via Host OS feature. For more information, refer the *iDRAC User's guide*.

- Microsoft Windows 2016
- Microsoft Windows Nano operating system
- Red Hat Enterprise Linux 6.8

NOTE: Limited iDRAC Service Module feature support for Microsoft Windows Nano operating system. For specific support details, refer to the iDRAC Service Module Installation Guide and iDRAC User's Guide.

What's New?

- iDRAC Access via Host OS
  - "OS2iDRAC" firewall rule is enabled when the feature is installed.

Rev. A00
2016 - 10

    * 1266 is the default listen port number.
    * You can check the status and the currently configured port number using the corresponding commands. For more information on the commands to view the port numbers, refer the iDRAC User's Guide.

- In-band SNMP Traps
  - This feature now includes AgentX protocol support on Linux operating Systems.

Known Issues and Resolutions

Issue 1

Description: If DSET 3.4 or later is running, and iDRAC Service Module is shut down or uninstalled; a **Watchdog Timer Expiry** event is observed.

Issue 2

Description: After a successful first time configuration of **iDRAC Access via Host OS** using the iDRAC Service Module webpack; the iDRAC interfaces may not be accessible due to default NetworkSecurity settings in iDRAC; irrespective of whether default NetworkSecurity settings are enabled or disabled.

Reference: **iDRAC GUI → Settings → Network → Advanced → Network Security**. The **IPRange Address** and **IPRange Mask** would be set to default values like 192.168.x.y and 255.255.255.0.

This can be resolved by reconfiguring **iDRAC Access via Host OS** using the PowerShell cmdlet. The IPRange can be set using the **cmdlet** as shown in the example command below:

- For Windows,
  - Enable-iDRACAccessHostRoute -status true -port 12345 -IPRange 10.94.146.5/24.
- On Linux OSes,
  - Enable-iDRACAccessHostRoute 1 12345 10.94.146.5/24.

NOTE: The IP Range value should follow the CIDR format.

Issue 3

Description: On Microsoft Windows 2012 operating systems; if an iDRAC reset operation is performed when any of the iDRAC sessions are opened using **iDRAC access via Host OS** feature, then the connection between iDRAC Service Module and iDRAC may not be re-established. Also, the Microsoft Windows service **IP Helper** might stop running.

In such scenarios, the following steps will resolve the issue.

1. Restart the iDRAC Service Module.
2. Restart the Microsoft Windows **IP Helper** service.
3. If Open Manage Server Administrator is running; restart the **dsm_sa_datamgr**service.

Example:

- Open iDRAC GUI via the **iDRAC access via Host OS** feature.
- Perform an iDRAC firmware update from the GUI. This will reboot iDRAC with the new firmware.
- The **iDRAC Service Module** in the Host does not restart communication with iDRAC.
- IP Helper services stops running.

The issue has been addressed by Microsoft. For more information and the resolution to the issue, visit, https://support.microsoft.com/en-us/kb/3156418

Issue 4

Description: On Microsoft Windows Nano operating system, when iDRAC Service Module 2.4.0 Appx is installed; a critical App-Model-Runtime message is seen. However, there is no change in the functionality.

Issue 5

Description: On Linux Operating system, NVMe Safe removal operation from iDRAC interfaces (GUI/racadm/wsman) may fail on systems having other pci devices along with NVMe. This issue is observed on blade chassis.

Issue 6

Description: "Unknown: " error entries are repeatedly logged in the Syslog folder of the ESXi system. The existing logs overwrite other important events logged previously. This is caused when the virtual switch (vSwitchiDRACvusb) is automatically removed. The issue occasionally occurs during system shutdown or if an administrator disables the OS to iDRAC Pass-through over USB or enables the OS to iDRAC Pass-through over LOM.

To stop the repetitive "Unknown:" error entries in the syslog without rebooting the virtual machines or the ESXi hypervisor, perform the following steps:

1. ps | grep vmsyslogd (and note the CID number)
2. kill -15 <CID number>
3. /etc/init.d/sfcbd-watchdog restart

Installation

- To install iDRAC Service Module on Windows Server 2008 R2 SP1 Core, Microsoft Windows Server 2012 Core and Microsoft Windows Server 2012 R2 Core, Windows-on-Windows (WOW) mode must be enabled.
- You must login to the system as an administrator or choose the **Run as administrator** option to install iDRAC Service Module.
- On the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, to perform an **Express Install** execute **dcism-setup.sh -x** from the **SYSMGMT/iSM/linux** directory.

For more information on installation instructions, including silent installation options, see the *iDRAC Service Module Installation Guide*.

Limitation

- Do not specify user profile folders such as a desktop folder (**C:\Users\administrator\Desktop**) as custom installation paths for installing iDRAC Service Module. This is because services running on the system account cannot access such folders.
- On systems running Microsoft Windows Server 2008 Service Pack 2 operating system, a warning message about the Dell Self-Signed Certificate for registering the Dell iDRAC Virtual USBNIC Device is displayed during iDRAC Service Module installation. Click **Install** to proceed with the installation (BITS113354).
- When OS to iDRAC Pass-through in the USB NIC mode is enabled with USB 3.0 enabled in BIOS, iDRAC Virtual USB NIC driver does not load automatically on Microsoft Windows 2008 R2 SP1. The Intel USB 3.0 xHCI driver on Microsoft Windows 2008 R2 SP1 Host OS is not recognizing the RNDIS configuration during enumeration. This issue is specific to USB 3.0 and Microsoft Windows 2008 R2 SP1. To resolve the issue, manually load the Microsoft RNDIS driver on the Host OS (BITS239254).
- Lifecycle Controller logs are not seen in the new folder in the Event Viewer (169898) if you have recently changed the folder name of the Lifecycle Controller logs in the Event Viewer, Microsoft recommends that you reboot the operating system to be able to view the Lifecycle Controller logs under the new view name (BITS113354).
- On Dell's 12th generation of PowerEdge servers with iDRAC firmware version 1.57.57 or earlier, Windows Management Instrumentation (WMI) feature is not active by default. The WMI feature is automatically activated when iDRAC firmware version 2.10.10.10 or later is installed (BITS113354).
- On Windows operating system, a feature that is enabled using the installer and disabled using any interface other than the installer, can only be enabled using the same interface or the installer in GUI mode (BITS180635).
- If iDRAC Service Module 2.0 or later is used with an iDRAC firmware version prior to 2.10.10.10, the WMI interface may stop responding. It is recommended to upgrade to the latest iDRAC firmware or reset the iDRAC (BITS178203).

- When iDRAC Service Module 2.3 is used for WMI queries through WinRM, additional properties with null value may be observed. This can be ignored.
- Feature Lifecycle Log Replication on OS Log shows one-hour difference in the **EventTimeStamp** displayed in OS log, when daylight saving is applied.
- On Linux Operating Systems, when iDRAC Service Module 2.3.0 and iDRAC Service Module 2.3.0.1 patch are installed, then to uninstall iDRAC Service Module completely, the iDRAC Service Module 2.3.0.1 patch has to be uninstalled before uninstalling iDRAC Service Module 2.3.0.
- The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.
- When Local RACADM set is disabled through iDRAC interfaces,
  - The iDRAC Service Module will fail to configure the OS to iDRAC Pass-through in the USB NIC mode.
  - If OS to iDRAC Pass-through in the USB NIC mode is already configured, Watchdog feature does not work resulting in ASR000 event.

  iDRAC Service Module functionality is restored when "Local racadm set" is enabled.
- When you use iDRAC Service Module 2.3 for WMI queries over winrm, additional properties with null value is observed. This does not affect the functionality and it can be ignored.
- If iDRAC Service Module 2.3.0 is installed on a Linux OS with the iDRAC Access via Host OS feature enabled, you have to to remove the rules of the previous port when upgrading from 2.3.0 to 2.4.0.
- When the iDRAC's USB NIC is not functioning, the iDrac Service Module installer is completing the installation and starting the iDRAC Service Module process without any notification about the failure to start the communication with the iDRAC. This issue is observed during iDRAC Service Module is installed using setup.sh command the iDRAC.