

# iDRAC Service Module 2.3

## 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

2.3

### Release Date

March 29, 2016

### Previous Version

2.2

### 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

- Red Hat Enterprise Linux 6.7
- Red Hat Enterprise Linux 7.1
- SUSE Linux Enterprise Server 11 SP4
- VMware ESXi 6.0 U1
- Citrix XenServer 6.5 SP1

### What's New?

- Remote iDRAC Hard Reset



- iDRAC Access via Host OS
- In-band SNMP Traps
- Additional network interface monitoring through Redfish client interface
- Support for Redhat Enterprise Linux 7.2 operating system (64-bit), SUSE Enterprise Linux 12 SP1 operating system (64-bit)

## 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 performing an iDRAC Hard Reset operation on certain Linux operating systems, the IPMI driver (**ipmi\_si** for Linux operating systems, **ipmi\_si\_drv** for VMware ESXi operating systems) may become unresponsive because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the IPMI driver (**ipmi\_si** for Linux operating systems, **ipmi\_si\_drv** for VMware ESXi operating systems).

The issue is observed on Linux kernel version prior to 3.15. An update is available in the following operating systems with Linux kernel version 3.15 or later:

- RedHat Enterprise Linux 6.6
- RedHat Enterprise Linux 7.1
- SUSE Enterprise Linux 11 SP4
- SUSE Enterprise Linux 12 SP1

The issue is observed in the following VMware ESXi operating systems:

- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0

Steps to reload the IPMI driver in Linux operating systems is as follows:

- **modprobe -r ipmi\_si**, if the removal fails, then all applications (such as, iDRAC Service Module and OpenManage Server Administrator use ipmi\_si) should be stopped using the **modprobe ipmi\_si** command and retry the operation.
- Alternatively, you can also restart the Host OS in order to resolve the issue.

Steps to reload the IPMI driver in VMware ESXi operating systems is as follows:

1. `/etc/init.d/sfcbd-watchdog stop`
2. `esxcfg-module -u ipmi_si_drv => unload ipmi_si`
3. `esxcfg-module ipmi_si_drv => load ipmi_si_d`
4. `/etc/init.d/sfcbd-watchdog start`

Alternatively, you can also restart the Host OS in order to resolve the issue.

## 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.
- 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).
- Feature Lifecycle Log Replication on OS Log shows one-hour difference in the **EventTimeStamp** displayed in OS log, when daylight saving is applied.
- The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.
- The In-band SNMP Traps feature on Linux does not support AgentX protocol.
- 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 will not work resulting in ASR000 event. iDRAC Service Module functionality is restored when "Local racadm set" is enabled.

© 2016 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.