iDRAC Service Module 3.0.1 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

3.0.1

Release Date

June 2017

Previous Version

2.5

Importance

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

What's New?

- Support for Redhat Enterprise Linux 6.9 operating system (64-bit)
- Support for Redhat Enterprise Linux 7.3 operating system (64-bit)
- Support for VMware ESXi 6.0 U3 and ESXi 6.5
- Support for Citrix XenServer 7.1
- Support for auto-update of iDRAC Service Module (Microsoft Windows and Linux operating systems)
- Support for "SupportAssist on the Box" features
- Support for FullPowerCycle of the server
- Support for initial installation of iDRAC Service Module from iDRAC GUI (Microsoft Windows and Linux operating systems)
- Support for SupportAssist Collection from Host-OS CLI using Invoke-SupportAssistCollection utility
- Support for OS log collection on VMware ESXi server operating systems
- Support for iDRAC Service Module when iDRAC lockdown mode is enabled

NOTE: For a complete list of supported platforms and supported operating systems, see the Dell EMC Systems Software Support Matrix available in the required version of OpenManage Software at dell.com/openmanagemanuals.

Rev. A00
2017 - 06

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: 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.

You can configure the Windows Remote Management (WinRM) Listener using a server authenticating certificate. If the server authenticating certificate is not available, iDRAC Service Module will force-enable the WinRM listener using a self-sign certificate. To configure the Windows Remote Management (WinRM) listener, you can create a self-signed certificate using the PowerShell cmdlet New-SelfSigned Certificate from Microsoft Windows Server 2012 or later. In operating systems prior to Microsoft Windows Server 2012 you cannot create a self-signed certificate due to the absence of PowerShell cmdlet.

Issue 3

Description: After performing an iDRAC Hard Reset operation on certain Linux operating systems, the IPMI driver (ipmi_si) may become unresponsive because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the IPMI driver (ipmi_si).

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

Steps to reload the IPMI driver:

- `modprobe -r ipmi_si` — If the removal fails, then all applications (such as iDRAC Service Module and OpenManage Server Administrator) using the ipmi_si need to be stopped and retry the operation.
- `modprobe ipmi_si` — Alternatively, the administrator can also restart the Host OS to resolve the issue.

Issue 4

Description: After performing an iDRAC Hard Reset operation on certain VMware ESXi operating systems, the IPMI driver (ipmi_si_drv) may become unresponsive because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the IPMI driver (ipmi_si_drv).

The issue is observed on all iDRAC Service Module v2.3 supported ESXi versions.

Steps to reload the ipmi_si_drv:

- `/etc/init.d/sfcbd-watchdog stop`
- `esxcfg-module -u ipmi_si_drv => unload ipmi_si_drv`

- `esxcfg-module ipmi_si_drv => load ipmi_si_drv`
- `/etc/init.d/sfcbd-watchdog start` — Alternatively, the administrator can also restart the Host OS to resolve the issue.

Installation

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.

NOTE: On Microsoft Windows Operating Systems, to enable WSMAN silently, use the following CLI command:

```
Msiexec.exe /i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2"
CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1" /qn
```

NOTE: On Red Hat Enterprise Linux, SUSE Linux Enterprise Server, and VMware ESX Operating Systems, you will not have the permission to run the script directly on the disk partition. Please use the format "sh ISM_LX.sh" to run the script and initiate iDRAC Service Module installation.

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.
- 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 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).
- Feature Lifecycle Log Replication on OS Log shows one-hour difference in the **EventTimeStamp** displayed in OS log, when daylight saving is applied. (BITS088419)
- 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.
- EventID for Lifecycle Controller Logs replicated to OS log will be 0 for some of the past events.
- TrapID for In-band SNMP Traps will be 0 for some of the past traps.