Dell EMC iDRAC Service Module 3.2

Release Notes

February 2021
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Topics:

- Dell EMC iDRAC Service Module 3.2 Release Notes

Dell EMC iDRAC Service Module 3.2 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

3.2

Release Date

May 2018

Previous Version

3.1

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 7.5 operating system (64-bit)
- Support for VMware ESXi 6.7
- Support for Citrix XenServer 7.1 CU1
- Support for ESXi Live VIB upgrade
- Support for SupportAssist Anonymous upload 12G and 13G
- Support for ESXi package download from iDRAC

NOTE: For a complete list of supported platforms and supported operating systems, see the iDRAC Service Module Guide version 3.2 at **dell.com/openmanagemanuals**.

User Notes for Supported Microsoft Windows Operating Systems

To enable WS-man silently, run 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
```

Known Issues on Microsoft Windows Operating Systems

Issue 1

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, do the following:

1. Restart the iDRAC Service Module.
2. Restart the Microsoft Windows **IP Helper** service.
3. If OpenManage 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-SelfSignedCertificate 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 2: JIT-87075

While uninstalling **iDRAC Service Module**, a popup is displayed if the Firefox browser is opened. The popup prompts that Firefox browser needs to be closed before continuing the uninstallation. Close the Firefox browser and click the **Retry** option to continue the uninstallation.

Limitations on Microsoft Windows Operating Systems

- Do not specify user profile folders like 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.
- You cannot view Lifecycle Controller logs 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.
- 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.

User Notes for Supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server

To perform an **Express Install** on the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems:

Execute `dcism-setup.sh -x` from the **SYSMGMT/iSM/linux** directory.

For more information on the installation instructions, including silent installation, see the "iDRAC Service Module User's Guide".

NOTE: You do not have the permission to run the script directly on the disk partition. Use the format `sh ISM_LX.sh` to run the script and then install iDRAC Service Module.

Known Issues on Linux Operating Systems

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) 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.

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 3: JIT-88625

Description: When iDRAC Service Module 3.2.0 is installed on RHEL 6.9 Operating System with SELinux enabled in Enforcing mode, AVC denial logs (AVC denial is noticed with iptables) are observed in /var/log/audit/audit.log while the following features are enabled or disabled:

1. iDRAC Access via Host OS
2. Host SNMP Alerts

iDRAC Service Module 3.2.0 does not support explicit SELinux policies. No action is expected from the user. There is no functionality impact to iSM features due to this. Future releases of iSM shall address the AVC denials.

Issue 4: JIT-93467

Description: iSM 3.2 OS DUP installation fails on SLES11SP4.

rpm-tool fails to handle OpenPGP subkeys and hence fails in integrity check.

Workaround: Upgrade **rpm4.4.2.337.63.64.1.14842.3.PTF.1081280.x86_64.rpm**. You can download this from https://ptf.suse.com/a4508678dc8ee2c11453898fb347f199/sles11-sp4/14842/x86_64/20180222/.

Issue 5: JIT-96546

Description: To update to iSM 3.2 via idrac, **Repair or Reinstall Service Module** button is disabled if iSM 3.1 is already running on the host OS and if the latest LC DUP is already in iDRAC.

Workaround: Stop iSM service on the host OS. Go to the iDRAC GUI and **Repair or Reinstall Service Module** button will be enabled in the iDRAC GUI. Click on the tab and install ism.

Limitations on Linux Operating Systems

- **BITS088419:** Feature Lifecycle Log Replication on OS Log shows one-hour difference in the "EventTimeStamp" displayed in OS log, when daylight saving is applied.
- **JIT-87572:** When iDRAC Hard Reset is disabled in iDRAC and user performs iDRACHardReset from the Hypervisor operating systems like Citrix Xen, the result indicates success although iDRAC is not reset.

Known Issues on VMware ESXi Operating Systems

Issue 1

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.

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.

Issue 2: JIT-102735

Description: On upgrading iSM 3.1 to iSM 3.2 from VUM, the ESXi OS is rebooting.

Issue 3: JIT-103063

Description: While updating iDRAC Service Module from v3.1 to v3.2 using VUM setup, the ESXi Host OS is going to **maintain** mode automatically.

Issue 4: JIT-103060

Description: iSM cannot be installed through VUM after successful uninstallation.

Workaround for Issue 2, 3 and 4:

The upgrade of iDRAC Service Module Live VIB package for VMware ESXi from iSM 3.1 to iSM 3.2 using DellEMC VUM repository requires a Host OS reboot. Alternatively, you can use the esxcli or PowerCLI interfaces to upgrade iDRAC Service Module without a Host OS reboot.

Limitations and Workarounds on VMware ESXi operating Systems

- The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.
- When **Local Racadm set** is disabled through iDRAC interfaces:
  - 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.
- **JIT-91716, JIT-90475:** WSMan commands for remote iDRAC Hard Reset and remote Enabling or Diabling of InBandSNMPTraps features are not functional on VMware ESXi 6.7.

Workaround: Stop and start WBEM in ESXi 6.7 using the following commands:

1. `esxcli system wbem set -e 0`
2. `esxcli system wbem set -e 1`

- **JIT-82934:** Due to mismatch between package name and VIB name, you may fail to deploy iDRAC Service Module integrated with custom ESXi ISO image using PowerCLI.

Workaround: To integrate iDRAC Service Module VIB into custom ESXi ISO image:

1. Loop Mount the modified ISO image (with iDRAC Service Module integrated) and copy the contents to a temp folder (cp –a <mount dir>/* /tmp/temp_iso; cp <mount dir>/.discinfo /tmp/temp_iso;)
2. `cd /tmp/temp_iso`
3. Rename iDRAC Service Module package by using the command `mv ism.v00 iSM.v00`
4. Add iSM.v00 references in boot.cfg and efi/boot/boot.cfg
5. Recreate the ISO image using `mkisofs -relaxed-filenames -J -R -o /tmp/custom_esxi_ism.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table /tmp/temp_iso`

- **JIT-87572:** When iDRAC Hard Reset is disabled in iDRAC and user performs iDRACHardReset from the Hypervisor operating systems like VMware ESXi, the result indicates success although iDRAC is not reset.