Rev. A02
October 2018

Dell EMC iDRAC Service Module 3.4 Release Notes

Topics:

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

3.3

Release Date

October 2018

Previous Version

3.2

Importance

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

What's New

- Support for Redhat Enterprise Linux 6.10 operating system (64-bit)
- Support for Ubuntu Server 18.04.1 LTS
- Support for SUSE Linux Enterprise Server 15

- Support for VMware ESXi 6.5U2

NOTE: For a complete list of supported platforms and supported operating systems, see the iDRAC Service Module User's Guide version 3.3 at **dell.com/openmanagemanuals**.

iDRAC Service Module Feature Enhancements

- iDRAC Service Module ESXi Live VIB name changed from **iSM** to **dcism**.
- On 13G servers, Anonymous Support Assist Collection upload can be performed using the blank username or password in proxy environment.

The user notes, known issues and workaround are mentioned separately in each operating system section in this document.

For more details on limitations and supported operating system, see **iDRAC Service Module User's Guide.**

User notes for supported Microsoft Windows operating systems

To enable WSMAN 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
```

.

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

- To perform an **Express Install** on the Red Hat Enterprise Linux, SUSE Linux Enterprise Server and Ubuntu 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**.
- You do not have the permission to run the `ISM_Lx.sh` script directly on the **SMINST** disk partition. Please use the format `sh ISM_Lx.sh` to run the script and initiate iDRAC Service Module installation.
- Starting iSM version 3.3, iSM confi,gures the Host OS USBNIC interface only once. Subsequently, if you bring down the USBNIC interface on the Host OS by deleting the IP address, making the interface link down or disabling the IPV4 or IPV6 address on this interface, then iSM will retain the user con,guration and does not override the interface settings. To restore the communication between iSM and iDRAC, please restart the iSM service on the Host OS.

Limitations

- The Full PowerCycle feature is not supported on FC640, M640, and M640-VRTX platforms.

Limitations on Microsoft Windows and Linux operating systems

JIT-133026

Description: To use the single sign-on feature in iSM, you must upgrade to iSM 3.5.0, and your iDRAC firmware must be version 4.00.00.00 or later.

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.

Limitations on Linux operating systems

BITS088419

Description: Lifecycle Log Replication feature in operating system log shows one-hour difference in the EventTimeStamp displayed in operating system log when daylight saving time is in effect.

JIT-87572

Description: When the iDRAC HardReset option is disabled in iDRAC and you can perform a iDRACHardReset operation from the hypervisor operating systems such as Citrix Xen , the result indicates success although iDRAC is not reset.

JIT-117904

Description: In GNOME-enabled Linux variants, if the auto-suspend feature is enabled, the operating system gets into suspended state after a certain idle time. This logs a message, *Watchdog Timer Expired*, in the Lifecycle Log, if the operating system is not awake before the watchdog expiry time is reached.

JIT-117517

Description: iSM start communications with iDRAC using IPv4 stack by default. If you bring down the OS-BMC Passthrough, host side interface using `ifconfig <interface-name> down`, the communication will switch to IPv6 once the interface is brought up.

Limitations and workarounds on VMware ESXi operating systems

iDRAC access through the host operating system feature is not supported on VMware ESXi operating systems.

When `local racadm set` is disabled through iDRAC interfaces:

- iDRAC Service Module fails to configure the OS-to-iDRAC Passthrough in USB NIC mode.
- iDRAC Service Module functionality is restored when `local racadm set` is enabled.

EventID for Lifecycle Controller logs replicated into the operating system log is 0 for some past events.

TrapID for in-band SNMP traps is 0 for some past traps.

JIT-91716 and JIT-90475

Description: WSMan commands for remote iDRAC hard reset and remote enabling or disabling of `InBandSNMPTraps` features are not functional on VMware ESXi 6.7 or later.

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

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

JIT-87572

Description: When iDRAC hard reset is disabled in iDRAC and you perform `iDRACHardReset` from hypervisor operating systems such as VMware ESXi, the result indicates success although iDRAC is not reset.

Known issues

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.

Known Issues and Limitations on Linux Operating Systems

Issue 1

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 2: BITS088419

Description: Feature Lifecycle Log Replication on OS Log shows one-hour difference in the **EventTimeStamp** displayed in the OS log, when daylight saving is applied.

Issue 3: JIT-102480

Description: When iDRAC Service Module 3.3.0 is installed on RHEL 6.10 operating system with SELinux enabled in either of Permissive or Enforcing modes, 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.

Workaround: iDRAC Service Module 3.3.0 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-106937

Description: If dependent packages for iSM are not present on Ubuntu OS, then installation through OS DUP installs iSM in install+unpacked state. You can verify this using the below command:

```
#dpkg -s dcism
        Package: dcism
        Status: install ok unpacked
```

Workaround: To ,fix this issue, run the command `apt-get install -f`. This will install dependent packages.

Known Issues, Limitations, and Workaround 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 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

Description: The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.

Issue 3

Description: When **Local Racadm set** is disabled through iDRAC interfaces:

— The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.

— 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.

Issue 4

Description: EventID for Lifecycle Controller Logs replicated to OS log will be 0 for some of the past events.

Issue 5

Description: TrapID for In-band SNMP Traps will be 0 for some of the past traps.

Issue 6 (JIT-91716, JIT-90475)

Description: WSMan commands for remote iDRAC Hard Reset and remote Enabling or Disabling 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`

Issue 7 (JIT-87572)

Description: 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.

Issue 8 (JIT-101652, JIT-102735, JIT-103063)

Description: While upgrading iDRAC Service Module ESXi Live VIB package through VMware Update Manager (VUM), the host OS enters maintenance mode and then reboots..

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.