Dell EMC iDRAC Service Module 3.4

Release Notes

May 2020
Rev. A02

DELL EMC

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.

1

Dell EMC iDRAC Service Module 3.4 Release Notes

Release type and definition

The Integrated Dell Remote Access Controller (iDRAC) Service Module (iSM) is a lightweight,optional software application that you can install on the Dell EMC PowerEdge yx2x servers or later. The iDRAC Service Module complements iDRAC interfaces—the user interface (UI), 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 you plan to install and the unique integration needs of your environment.

Version

3.4

Release date

March 2019

Previous version

3.3.1

Importance

RECOMMENDED: It is recommended that you apply this update during your next scheduled update cycle. This version contains some new features, feature enhancements, and bug fixes.

What's New

- Removed the support for SUSE Linux Enterprise Server 12.
- TLS protection enabled for securing iSM to iDRAC communication over OS-BMC Passthru.
- Added single sign-on (SSO) to iDRAC UI from the host operating system using the administrator's account.
- Enabled auto dispatch capability for Embedded SupportAssist.
- Added support for IPv6 communication between iSM and iDRAC over OS-BMC Passthru.
- SupportAssist operating system data collection on VMware ESXi now also supports collection in filter mode for privacy.
- Support for Red Hat Enterprise Linux 7.6 operating system.
- Support for ESXi 6.7 U1 operating system. Support for Win10 RS5 client operating system on Precision Rack server R7920.

NOTE: For a complete list of supported platforms and supported operating systems, see the iDRAC Service Module User's Guide version 3.4 at Dell.com/openmanagemanuals.

iDRAC Service Module feature enhancements

- iDRAC Service Module ESXi Live VIB name changed from *iSM* to *dcism*.
- On yx3x PowerEdge servers, Anonymous SupportAssist Collection upload can be performed using the blank username or password in a 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 systems, see your *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 and SUSE Linux Enterprise Server

- To perform an Express Install on 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*.
- You do not have the permissions required to run the script directly on the disk partition. Use the format `sh ISM_Lx.sh` to run the script and initiate iDRAC Service Module installation.

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

- During iDRAC Service Module installation, do not specify your desktop user profile's folder path in the custom installation path. For example, C:\Users\administrator\Desktop must not be used in the custom installation path. 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.

JIT-115250

When iDRAC Service Module is installed on systems running Microsoft Windows operating systems using an `OS DUP`, then the iSM **Modify and Repair** operation from the **Add/Remove** programs will throw an error, *original source path of the file is not found* . You can extract the iSM DUP file, double click the MSI file, and run repair.

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

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-signed certificate. To configure the WinRM listener, 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.

Known issues 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_si.

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

To reload the IPMI driver:

- `modprobe -r ipmi_si`—If the removal fails, then stop any applications using the ipmi_si such as iDRAC Service Module and OpenManage Server Administrator, and retry the operation.
- `modprobe ipmi_si`—Alternatively, the administrator can also restart the host operating system to resolve the issue.

Issue 2

Description: IPv6 support on Linux operating systems is not available for the following features:

- iSM Auto Update
- ismtech
- iDRAC GUI Launcher
- Inband iDRAC Access

Issue 3: JIT-102480

Description: When iDRAC Service Module 3.3.0 or later is installed on a system running the RHEL 6.10 operating system with SELinux enabled in either permissive or enforcing modes, AVC denial logs, noted in iptables, are observed in `/var/log/audit/audit.log` while the following features are enabled or disabled:

1. iDRAC access using the host operating system
2. Host SNMP alerts from the host

Workaround: iDRAC Service Module 3.3.0 and later does not support explicit SELinux policies. No action is expected from the user. iSM functionality is not impacted. Future releases of iSM shall address the AVC denials.

Issue 4: JIT-114656

Description: When iSM with TLS capability, for example: iSM 3.4.0 is installed on Linux operating systems, and the iSM client certificate name is modified and iSM service is restarted, then communication between iSM and iDRAC ends.

Workaround: As a workaround, uninstall and then reinstall iSM 3.4.0.

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 on ESXi 6.5 U2 and ipmi on ESXi 6.7 U1 operating systems may become unresponsive because of an existing issue in the driver. If the IPMI driver becomes unresponsive, reload the IPMI driver.

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

To reload the ipmi_si_drv:

- `esxcli system wbem set -e 0`
- `esxcfg-module -u ipmi_si_drv/ipmi => unload ipmi_si_drv/ipmi`
- `esxcfg-module ipmi_si_drv/ipmi => load ipmi_si_drv/ipmi`
- `esxcli system wbem set -e 1`

Alternatively, the administrator can also restart the host operating system to resolve the issue.

Issue 2: (JIT-118912)

Description: iSM uninstall or wbem stop causes an ungraceful stop of iSM CMPI modules which results in system V semaphore leaks. Recurring system V semaphore leaks will impact iSM functionality. This is a known issue affecting vSphere ESXi 6.7. For more information, see https://kb.vmware.com/s/article/66775.