Dell EMC iDRAC Service Module

Version 3.4.1

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.

2019 - 09

Rev. A00

Contents

1

Release Summary

The Integrated Dell Remote Access Controller (iDRAC) Service Module (iSM) is a lightweight optional software application that can be installed on the yx3x generation of PowerEdge servers or later. This release of iDRAC Service Module adds support to yx5x generation of PowerEdge servers and support for RedHat Enterprise Linux 8.0 and ESXi operating system.

Topics:

Version

iDRAC Service Module version 3.4.1

Release Date

September 2019

Priority and recommendations

Recommended: Dell recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that help keep your system software current and compatible with other system modules (Firmware, BIOS, drivers, and software).

2

Compatibility

License Requirements

For information regarding license agreements, go to iDRAC Service Module 3.4.1 User's Guide available at **www.dell.com/ismmanuals**

Supported Platforms

iDRAC Service Module 3.4.1 supports yx3x to yx5x generation of PowerEdge servers.

Supported Systems

The table lists the platforms that are supported by iDRAC Service Module 3.4.1.

yx5x servers	yx4x servers	yx3x servers
R6515	T140	C4130
R7515	T340	C6320
	R240	FC430
	R340	FC630
	R740xd2	FC830
	MX740c	M630 VRTX
	MX840c	M630
	R840	M830
	R940xa	R230
	R7425	R330
	R7415	R430
	R6415	R530
	C6420	R630
	FC640	R730
	FD332	R730xd
	M640	R830
	M640-VRTX	R930
	R440	T130
	R540	T330
	R640	T430
	R740	T630
	R740xd	
	R940	
	T440	
	T640	

C4140

Previous Versions

- iDRAC Service Module 1.0
- iDRAC Service Module 2.0
- iDRAC Service Module 2.1
- iDRAC Service Module 2.2
- iDRAC Service Module 2.3
- iDRAC Service Module 2.4
- iDRAC Service Module 2.5
- iDRAC Service Module 2.5.1
- iDRAC Service Module 3.0.1
- iDRAC Service Module 3.0.2
- iDRAC Service Module 3.1
- iDRAC Service Module 3.2
- iDRAC Service Module 3.3
- iDRAC Service Module 3.3.1
- iDRAC Service Module 3.4

Supported managed server operating systems and hypervisors

- Microsoft Windows
  - Microsoft Windows Server 2019
- Linux
  - RedHat Enterprise Linux 8.0 operating system
  - RedHat Enterprise Linux 7.6 operating system
- Ubuntu
  - Ubuntu 18.04.02
- VMware
  - ESXi 6.5 U3
  - ESXi 6.7 U2

3

New and enhanced features

- Support for yx5x generation of PowerEdge servers
  - R6515
  - R7515
- Support for RedHat Enterprise Linux 8.0 operating system support on yx3x, yx4x and yx5x servers
- ESXi 6.5 U3 and ESXi 6.7 U2 operating system support on yx3x and yx4x

4

Known Issues

Issue 1: iDRAC Service module stops responding when iDRAC Firmware is downgraded.

Description: iDRAC Service module stops responding when iDRAC Firmware is downgraded from 3.30.30.30.

Workaround: Install iDRAC Service Module that is supported by the current version of iDRAC installed.

Tracking ID: 132574.

Issue 2: iDRAC Hard Reset on yx5x generation of AMD PowerEdge servers delays the communication between iDRAC and iDRAC Service Module.

Description: In yx5x generation of AMD PowerEdge servers, performing iDRAC Hard Reset delays the communication time between iDRAC and iDRAC Service Module.

Workaround: No workaround available.

Issue 3: Installation on CentOS 7.5 is not supported through OS Dell Update Package(DUP).

Description: Installation of iDRAC Service Module on CentOS 7.5 is not supported through OS Dell Update Package(DUP)

Workaround: Install iDRAC Service Module on CentOS through Webpack.

Tracking ID: 138573.

Topics:

Known issues on Microsoft Windows operating system

Issue 1: MOF file attribute difference observed in DCIM_BIOSPassword, DCIM_SystemAttribute and DCIM_SystemInteger classes.

Description: MOF File attribute class from iDRAC Service Module observed with additional characters.

Workaround: There is no functional impact. No action is required by the user.

Tracking ID: 122750.

Issue 2: Configuring the Windows Remote Management (WinRM) Listener using a server authenticating certificate

Description: 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 force-enables the WinRM listener using a self-signed certificate.

Workaround: To configure the Windows Remote Management (WinRM) listener, you can create a self-signed certificate using the PowerShell `New-SelfSignedCertificate` cmdlet 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: On RHEL 8.0, uploading Support Assist Collection report to Dell back-end server fails.

Description: On Red Hat Enterprise Linux 8.0 uploading of Support Assist Collection report to Dell backend server fails. A message will be logged in iDRAC Lifecycle controller with message ID SRV090.

Workaround: No workaround available.

Tracking number: 148281

Issue 2: iSM communication with iDRAC through IPv6 does not support "InBand iDRAC Launcher"

Description: iSM communication with iDRAC through IPv6 in Linux operating system does not support "InBand iDRAC Launcher" feature though the configuration shows successful message.

Workaround: Currently this feature is supported through IPv4 communication.

Tracking number: 133769

Issue 3: iSM Auto communication with iDRAC fails when USB NIC IP address is changed in iDRAC while iSM is running

Description: iSM Auto communication with iDRAC fails and the services do not start automatically when USB NIC IP address in iDRAC is changed while iSM is still in running state.

Workaround: There is no workaround available.

Tracking number: 118654

Issue 4: ismtechuser does not get deleted when iDRAC Service Module is uninstalled.

Description: ismtechuser does not get deleted when the user is logged in and, iDRAC Service Module is uninstalled.

Workaround: ismtechuser should be deleted manually.

Tracking number: 131851

Issue 5: Launching SSO for Sudo user on RHEL 8 displays iDRAC launcher script location path in OS logs.

Description: On Red Hat Enterprise Linux 8 operating system (64-bit), while launching iDRAC GUI for the first time using iDRAC Launcher.sh script or using the Dell EMC iDRAC GUI Launcher short-cut, the below message is displayed in the operating system logs.

```
"localhost dbus-daemon[2369]: [system] Activating via systemd: service
name='net.reactivated.Fprint'unit='fprintd.service' requested by ':1.18176' (uid=0 pid=126684
comm="sudo -l /opt/dell/srvadmin/iSM/bin/Invoke-
iDRACLau"label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023")"
```

Workaround: There is no functional impact. No action is required by the user.

Tracking number: 124514

Issue 6: IPMI driver may become responsive after iDRAC Hard Reset operation on certain Linux operating systems

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).

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

To reload the IPMI driver:

- 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.

  Run `modprobe -r ipmi_si` to retry the operation.

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

  Run `modprobe ipmi_si` to restart the Host operating system.

Issue 7: IPv6 support on Linux operating systems not available

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

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

Workaround: Not available.

Issue 8: AVC denial logs are seen when iDRAC Service Module 3.3.0 or later is installed on RHEL 6.10 with SELinux enabled

Description: When iDRAC Service Module 3.3.0 or later 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:

- iDRAC Access via Host operating system
- Host SNMP Alerts

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

Tracking number: 102480

Issue 9: Communication between iSM and iDRAC disconnects when iSM with TLS capability is installed

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

Workaround: User has to uninstall and reinstall iSM 3.4.0

Tracking number: 114656

Known issues on VMware ESXi operating systems

Issue 1: IPMI driver may become responsive after iDRAC Hard Reset operation on certain VMware ESXi operating systems

Description: After performing an iDRAC Hard Reset operation on certain VMware ESXi operating systems, the IPMI driver (ipmi_si_drv on ESXi 6.5U2 and ipmi on ESXi 6.7U1 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_drv on ESXi 6.5U2 and ipmi on ESXi 6.7U1 Operating System).

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

To reload the IPMI driver:

- 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.

  Run the following commands

  ```
  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 OS to resolve the issue .

Issue 2: iSM uninstall or wbem stop causes ungraceful stop of iSM CMPI modules

Description: iSM uninstall or wbem stop causes ungraceful stop of iSM CMPI modules thereby resulting in system V semaphore leaks. Recurring system V semaphore leakage impacts iSM functionality.

This is a known issue affecting vSphere ESXi 6.7. For more information, see **https://kb.vmware.com/s/article/66775**

Tracking number: 118912

5

Limitations

Limitations on Microsoft Windows operating systems

- Do not specify user profile folders (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.
- When iDRAC Service Module is installed on Microsoft Windows operating systems using OS DUP, then the iSM **Modify and Repair** operation from the **Add/Remove** programs throws and error:

  Original source path of the file is now found

  You can unzip the iSM DUP, double-click the MSI, and run repair.

  Tracking number : 115250

Limitations on Linux operating system

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

  Tracking number: BITS088419
- When iDRAC Hard Reset is disabled in iDRAC and you perform **iDRACHardReset** from the Hypervidor operating systems such as Citrx Xen, the result indicates success although iDRAC is not reset.

  Tracking number: 87572
- In GNOME enabled Linux variants, if **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 Lifecycle Logs if the operating system is not awake before watchdog expiry time.

  Tracking number: 117904
- iSM starts communication with iDRAC using IPv4 stack by default. If you bring down **OS-BMC Passthrough** Host side interface using *ifconfig<interface-name>down*, the communication will switch to IPv6 once the interface is brought up.

  Tracking number: 117517

Limitations on VMware ESXi operating systems

- iDRAC Hard Reset using `winrm` command requires iDRAC Service Module to be in running state.

  Tracking number: 132478
- 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 fails to configure the **Os-to-iDRAC Passthru** in the USB NIC mode.
  - iDRAC Service Module functionality is restored when **local racadm set** is enabled.

  EventID for Lifecycle Controller Logs replicated to OS log is 0 for some of the past events.

  TrapID for In-band SNMP Traps is 0 for some of the past traps.
- **Description:** WSMan command 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
```

Tracking number: 91716, 90475

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

  Tracking number: 87572

6

User notes for supported 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
```

7

User notes for supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server

- To perform an **Express Install** on Red hat Linux and SUSE Linux Enterprise Server operating systems, run the following command from the **SYSMGMT/iSM/linux** directory:

  ```
  dcism-setup.sh -x
  ```

  For more information on the installation instructions, refer to the iDRAC Service Module User's Guide.
- By default, you do not have permission to run the script directly on the disk partition. Run the following command to run the script directly and initiate iDRAC Service Module installation:

  ```
  sh ISM_Lx.sh
  ```

8

Resources and support

For more information about the features of this release, see the documentation for iDRAC Service Module 3.4.1.

Latest Released Documents

To access the latest version of iDRAC Service Module documents:

- Go to **www.dell.com/ismmanuals**.
- Click the version of iDRAC Service Module.
- Clicks **Manuals & Documents**.

Accessing documents using direct links

You can directly access the documents using the following links:

URL	Product
www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
www.dell.com/esmmanuals	Enterprise System Management
www.dell.com/serviceabilitytools	Serviceability Tools
www.dell.com/omconnectionsclient	Client System Management

Accessing documents using the product search

1. Go to **www.dell.com/support**.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, PowerEdge or iDRAC. A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **Manuals & documents**.

Accessing documents using the product selector

You can also access documents by selecting your product .

1. Go to **www.dell.com/support**.
2. Click **Browse all products**.
3. Click the desired product category, such as Servers, Software, Storage, and so on.
4. Click the desired product and then click the desired version if applicable.

   NOTE: For some products, you may need to navigate through the subcategories
5. Click **Manuals & documents**.

9

Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues, see **www.dell.com/contactdell**.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.