Dell EMC iDRAC Service Module 3.4.1

User's Guide

June 2020
Rev. A03

DELL Technologies

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

Introduction

This guide provides information and step-by-step instructions on how to install iDRAC Service Module on the supported operating systems.

The Integrated Dell Remote Access Controller(iDRAC) Service Module is a lightweight optional software application that can be installed on yx3x servers or later. The iDRAC Service Module complements iDRAC interfaces – Graphical User Interface (GUI), RACADM CLI, Redfish, 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.

The iDRAC Service Module architecture uses IP socket communication and provides additional Systems Management data (OS/device driver) to iDRAC and presents one-to-many consoles with access to Systems Management data through OS standard interfaces.

Topics:

What's New

- Support for yx5x platforms (R6515, R7515, R6525 and C6525)
- Support for RedHat Enterprise Linux 8.0 operating system on yx3x, yx4x, and yx5x servers
- ESXi 6.5 U3 operating system support on yx3x, yx4x and yx5x servers
- ESXi 6.7 U2 operating system support on yx3x and yx4x servers
- ESXi 6.7 U3 operating system support on yx5x servers

Supported features—operating systems matrix

The following features are supported on yx3x, yx4x, and yx5x servers:

Table 1. Supported features—operating systems matrix

Features	Generation	Operating Systems		
		Microsoft Windows (including HyperV systems)	Linux	Virtualization (VMware ESXi)
Sharing OS Information	yx3x, yx4x, yx5x	Yes	Yes	Yes
LC Log Replication	yx3x, yx4x, yx5x	Yes	Yes	Yes
Automatic System Recovery/Watchdog	yx3x, yx4x, yx5x	Yes	Yes	Yes

Table 1. Supported features—operating systems matrix (continued)

Features	Generation	Operating Systems		
Windows Management Instrumentation Providers	yx3x, yx4x, yx5x	Yes	No	No
Prepare to Remove NVMe device through iDRAC.	yx3x, yx4x, yx5x	Yes	Yes	Yes
SupportAssist Collection	yx3x, yx4x, yx5x	Yes	Yes	Yes
OS and Application Data	yx3x, yx4x, yx5x	Yes	Yes	Yes (only for yx4x and later servers)
Remote iDRAC hard reset	yx3x, yx4x, yx5x	Yes	Yes	Yes
iDRAC access through Host OS	yx3x, yx4x, yx5x	Yes	Yes	No
In-band Support for iDRAC SNMP alerts	yx3x, yx4x, yx5x	Yes	Yes	Yes
Network interface monitoring support through Redfish client	yx3x, yx4x, yx5x	Yes	Yes	Yes
Enable WSMan Remotely.	yx3x, yx4x, yx5x	Yes	No	No
Full PowerCycle	yx4x, yx5x	Yes	Yes	No
In-Band SNMP Get	yx3x, yx4x, yx5x	Yes	Yes	No
Live VIB installation	yx3x, yx4x, yx5x	No	No	Yes
SupportAssist-Anonymous Collection Report	yx3x, yx4x, yx5x	Yes	Yes	Yes
iDRAC GUI launcher	yx3x, yx4x, yx5x	Yes	Yes	No
IPv6 support	yx3x, yx4x, yx5x	No	Yes	No
Auto Dispatch for selective events	yx3x, yx4x, yx5x	Yes	No	No
SA collection with selective PII	yx3x, yx4x, yx5x	No	No	Yes
Single Sign-On (SSO)	yx3x, yx4x, yx5x	Yes	Yes	No
Auto-update iSM Installation	yx4x, yx5x	Yes	Yes	No

Documentation conventions for Dell EMC devices

The following table lists the documentation conventions for Dell EMC devices.

Table 2. Documentation Conventions for Dell EMC Devices

yx5x servers	yx4x servers	yx3x servers
R6515	R240	C4130
R7515	R340	C6320
R6525	T140	FC 430
C6525	T340	FC 630
	R740xd2	FC 830
	R840	M630
	R940 xa	M630-VRTX
	MX740c	M830
	MX840c	R230
	R7425	R330
	R7415	R430
	R6415	R530
	C6420	R630
	FC 640	R730
	M640	R730xd
	M640-VRTX	R830
	FD332	R930
	R440	T130
	R540	T330
	R640	T430
	R740	T630
	R740xd	
	R940	
	T440	
	T640	

Coexistence of OpenManage Server Administrator and iDRAC Service Module

In a system, both OpenManage Server Administrator (OMSA) and iDRAC Service Module can coexist. If you enable the monitoring features during the iDRAC Service Module installation, and after the installation is complete, if the iDRAC Service Module detects the presence of OMSA, iDRAC Service Module disables the set of monitoring features that overlaps. At any time if the OMSA service stops, the iDRAC Service Module features are enabled.

NOTE: The overlapping features are **AutoSystemRecovery** and **Lifecycle Log Replication**.

Software availability

The iDRAC Service Module software is available on:

- *Dell EMC OpenManage Systems Management Tools and Documentation* DVD

- Support site dell.com/support

Downloading iDRAC Service Module

You can download the iDRAC Service Module software from dell.com/support. In the support site, click **Browse all products** > **Software** > **Enterprise Systems Management** > **Remote Enterprise Systems Management** > **iDRAC Service Module**.

Before downloading iSM, select the required version and then click **Drivers & downloads**.

Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — **www.dell.com/SoftwareSecurityManuals**
- For Dell EMC OpenManage documents — **www.dell.com/OpenManageManuals**
- For Dell EMC Remote Enterprise Systems Management documents — **www.dell.com/esmmanuals**
- For iDRAC and Dell EMC Lifecycle Controller documents — **www.dell.com/idracmanuals**
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- For Dell EMC Serviceability Tools documents — **www.dell.com/ServiceabilityTools**
- 1. Go to **www.support.dell.com** .

  2. Click **Browse all products**.

  3. From **All products** page, click **Software**, and then click the required link from the following:
     - **Analytics**
     - **Client Systems Management**
     - **Enterprise Applications**
     - **Enterprise Systems Management**
     - **Public Sector Solutions**
     - **Utilities**
     - **Mainframe**
     - **Serviceability Tools**
     - **Virtualization Solutions**
     - **Operating Systems**
     - **Support**

  4. To view a document, click the required product and then click the required version.

- Using search engines:
  - Type the name and version of the document in the search box.

Software license agreement

The software license for the supported versions of the operating system of the iDRAC Service Module is on the installer. Read the `license_agreement.txt` file. By installing or copying any of the files on the media, you are agreeing to the terms in `license_agreement.txt` file.

Other documents you may need

You can access the following guides available at dell.com/support.

- The *Integrated Dell Remote Access Controller (iDRAC)* User's Guide provides detailed information about configuring, and using the iDRAC.
- The *Dell Remote Access Controller Racadm User's Guide* provides information about using the RACADM command-line utility.

- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell Event Messages Reference Guide* provides information about the event and error information that is generated by firmware and other agents that monitor system components.
- The *Dell Lifecycle Controller 2 Web Services Interface Guide* provides information and examples for using the Web services for Management (WSMan) Management protocol.

2

Preinstallation setup

Ensure that you assess the following before installing the iDRAC Service Module:

- yx3x servers or later. For the list of supported platforms, see Supported Platforms
- Minimum firmware version—
  - For iDRAC 8 - 2.70.70.70
  - For yx4x servers with iDRAC 9 - 3.36.36.36
  - For yx5x servers with iDRAC 9 - 3.40.40.40 (For R6515 and R7515) and 3.42.42.42 (For R6525 and C6525)
- Administrator privileges.
- Read the installation instructions for the operating system.
- Read the applicable release notes and the *Systems Software Support Matrix*.
- Read the Installation requirements to ensure that the system meets the minimum requirement.
- Close all applications running on the system before installing the iDRAC Service Module application.

Topics:

Installation requirements

Refer to Supported operating systems to see the list of operating systems that are supported on iDRAC Service Module.

NOTE: Prerequisites specific to an operating system are listed as part of the installation procedures.

NOTE: The iDRAC Service Module can be installed using a User Interface. The installer also supports a silent installation mechanism.

Supported operating systems

The iDRAC Service Module support is available on the following 64–bit operating systems:

- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 7.6
- VMware vSphere (ESXi) 6.5 U3 (Support on yx3x, yx4x and yx5x servers)
- VMware vSphere (ESXi) 6.7 U2 (Support on yx3x and yx4x servers)
- VMware vSphere (ESXi) 6.7 U3 (Support on yx5x servers)
- Ubuntu 18.04.2

NOTE: This release of iDRAC Service Module does not support SUSE Linux Enterprise operating system.

Supported platforms on Linux operating systems

The table lists the platforms that are supported by iDRAC Service Module 3.4 on Linux operating systems.

Table 3. Supported platforms on Linux operating systems

Dell Systems	SLES 15	Ubuntu 18.04.2	RHEL 7.6
15th generation servers			
R6515	Yes	Yes	Yes
R7515	Yes	Yes	Yes
R6525	Yes	Yes	Yes
C6525	Yes	Yes	Yes
14th generation servers			
T140	Yes	Yes	No
T340	Yes	Yes	No
R240	Yes	Yes	No
R340	Yes	Yes	No
R740xd2	Yes	Yes	No
MX740c	No	Yes	No
MX840c	No	Yes	No
R840	Yes	Yes	No
R940xa	Yes	Yes	No
R7425	Yes	No	No
R7415	Yes	No	No
R6415	Yes	No	No
C6420	Yes	Yes	No
FC640	Yes	Yes	No
FD332	Yes	Yes	No
M640	Yes	Yes	No
M640-VRTX	Yes	Yes	No
R440	Yes	Yes	No
R540	Yes	Yes	No
R640	Yes	Yes	No
R740	Yes	Yes	No
R740xd	Yes	Yes	No
R940	Yes	Yes	No
T440	Yes	Yes	No
C4140	Yes	Yes	No
T640	Yes	Yes	No
13th generation servers			
C4130	Yes	No	No

Table 3. Supported platforms on Linux operating systems (continued)

Dell Systems	SLES 15	Ubuntu 18.04.2	RHEL 7.6
C6320	Yes	No	No
FC 430	Yes	No	No
FC 630	Yes	No	No
FC 830	Yes	No	No
M630 VRTX	Yes	No	No
M630	Yes	No	No
M830	Yes	No	No
R230	Yes	No	No
R330	Yes	No	No
R430	Yes	No	No
R530	Yes	No	No
R630	Yes	No	No
R730	Yes	No	No
R730 XD	Yes	No	No
R830	Yes	No	No
R930	Yes	No	No
T130	Yes	No	No
T330	Yes	No	No
T430	Yes	No	No
T630	Yes	No	No
12th generation servers			
FM120	Yes	No	No
M420	Yes	No	No
M520	Yes	No	No
M620	Yes	No	No
M820	Yes	No	No
R220	Yes	No	No
R320	Yes	No	No
R420	Yes	No	No
R520	Yes	No	No
R620	Yes	No	No
R720	Yes	No	No
R720 XD	Yes	No	No
R820	Yes	No	No
R920	Yes	No	No
T320	Yes	No	No
T420	Yes	No	No

Table 3. Supported platforms on Linux operating systems (continued)

Dell Systems	SLES 15	Ubuntu 18.04.2	RHEL 7.6
T620	Yes	No	No

Supported platforms

iDRAC Service Module 3.4.1 supports yx3x, yx4x and yx5x servers.

Supported platforms on Microsoft Windows operating systems

The table lists the platforms that are supported by iDRAC Service Module 3.4.1 on Microsoft Windows operating systems.

Table 4. Supported platforms on Microsoft Windows operating systems

Dell EMC Devices	Microsoft Windows Server 2019
yx5x generation of PowerEdge servers	Yes
yx4x generation of PowerEdge servers	X
yx3x generation of PowerEdge servers	X

Supported platforms on Virtualization operating systems

The table lists the platforms that are supported by iDRAC Service Module 3.4.1 on Virtualization operating systems.

Table 5. Supported platforms on Virtualization operating systems

Dell EMC Devices	VMware		
	vSphere 6.5 U3	vSphere 6.7 U2	vSphere 6.7 U3
yx5x generation of PowerEdge servers	Yes	X	Yes
yx4x generation of PowerEdge servers	Yes	Yes	X
yx3x generation of PowerEdge servers	Yes	Yes	X

System requirements

- One of the supported operating systems. For more information on supported operating systems, see Supported operating systems.
- Minimum 2 GB RAM.
- Minimum 512 MB of hard drive space.
- Administrator rights.
- The Remote Network Driver Interface Specification (RNDIS) capability for discovering a network device over USB.

3

Installing iDRAC Service Module

The iDRAC Service Module can be installed in any of the following operating systems:

- Microsoft Windows operating systems.
- Supported Linux operating systems.
- VMware ESXi.

Topics:

Initial installation of iDRAC Service Module through iDRAC for Windows

You can install iSM from the iDRAC interface. Install iSM by a single-click installation using the iDRAC installer packager with the host OS. By using this installer package, you must not navigate to the Dell support or OM DVD to install iSM. This feature ensures that the compatible version of iSM is installed for the supported iDRAC firmware.

For initial installation of iSM through iDRAC:

1. Navigate to the **iDRAC Service Module Setup** page. Click the **Install Service Module** button.
   Service Module Installer dialog box is displayed.
2. Select the appropriate script for your system, and then click **Launch Virtual Console**.
3. In the **Security Warning** dialog box, click **Continue**.
   You can view the verifying application status in the dialog box.
4. In the **Security Warning** dialog box, accept the terms of license agreement, and then click **Run**.
5. Log in to the remote/local system (Host OS) by using your credentials.
   You can find the installer file in the local system.
   NOTE: The installer is available in the Host OS for 30 minutes. If you do not start the installation within 30 minutes, you must restart the service module installation.
6. Double-click the volume (SMINST), and run `ISM_Win.bat` script.
   iDRAC Service Module installer wizard is displayed.
7. Proceed with the typical installation steps, and complete the installation.

   NOTE: After the installation is complete, the installer file is deleted from the local/Host OS.

   NOTE: On the *iDRAC Service Module Setup* page, the *Install Service Module* button is disabled after the installation is complete. The service module status is displayed as, *Running*.

Initial installation of iSM through iDRAC Express

1. From the **iDRAC Service Module** setup page, click **Install Service Module**.
   The Service Module Installer is exposed to the Host OS, and a job has been created in iDRAC.

2. For Microsoft Windows OS, RDP to the server or go to the physical server console. For Linux OS, SSH to the host IP or go to the physical server console.
3. Find the mounted volume in your device list labeled **SMINST**, and click the appropriate script to start the installation. For Microsoft Windows OS, run the `ISM-Win.bat` script. For Linux OS, run the script `ISM-Lx.sh` from the shell.
4. After the installation is complete, iDRAC shows that the Service Module as **Installed** and displays the last installed date.

NOTE: The installer is available in the Host OS for 30 minutes. If you do not start the installation within 30 minutes, you must restart the Service Module installation.

Initial installation of iDRAC Service Module via iDRAC for Linux

For initial installation of iDRAC Service Module via iDRAC for Linux operating systems:

1. Transverse to mounted volume (SMINST).
2. Run the command `sh ISM_Lx.sh or .ISM_Lx.sh`.
3. Locate the exposed drive on Ubuntu using `fdisk -l` and then mount to a directory.
4. Run the command using bash `ISM_Lx.sh`.

Installing iDRAC Service Module on Microsoft Windows operating systems

The iDRAC Service Module installer for the supported operating systems is available on the *Systems Management Tools and Documentation* DVD. You can also download the iDRAC Service Module installer from **dell.com/support/home**.

You can perform a manual or an automated installation using appropriate command-line switches. You can install the iDRAC Service Module through the **push** mechanism using consoles like OpenManage Essentials (OME).

NOTE: Perform the following steps only if third-party PowerShell module path is missing in the operating system environment.

1. Browse to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard** is displayed.
2. Click **Next**.
   The **License Agreement** is displayed.
3. Read the software license agreement, select **I accept the terms in the license agreement**, and then click **Next**.
4. Select the **Setup Type** from the following options, and click **Next**.
   - **Typical** – All program features are installed (Requires the most disk space).
   - **Custom** – Customize the installation by choosing the program features you want to install along with the location (Recommended for advanced users).

     The available options are:
     - **Operating System Information**
     - **Automatic System Recovery**
     - **Lifecycle Log Replication**
     - **Windows Management Instrumentation (WMI) Providers**
     - **Windows Remote Management**
     - **iDRAC access via Host OS**
     - **iDRAC Hard Reset**
     - **Support Assist**
     - **iDRAC GUI Launcher**

NOTE: The following steps are applicable, only if you select the **Custom** option in the **Setup Type** window.

NOTE: By default, the **In-Band SNMP Traps** feature is not enabled.

a. Choose the program features you want to install and click **Next**.
   The **Lifecycle Controller Log Replication** window is displayed.
b. Specify the location where the LC logs are to be replicated. By default, **Typical (Windows Logs/System)** option is selected and the LC logs are replicated in the **System** group of the **Windows Logs** folder in the **Event Viewer**. Click **Next**.

   NOTE: You can also create a custom group in the **Application and Services Log** folder by selecting the **Custom** option in the **Lifecycle Controller Log Replication** window.

c. Select the authentication mode to enable WSMan remotely and also choose to install a self-signed certificate if the authentication certificate is not found. Provide a WINRM port number to establish the communication. By default, the port number is 5986.

5. Provide a unique port number between 1024 and 65535 to be used by iDRAC access via Host OS feature. If you do not provide a port number, *port number 1266* or a previously configured port (if any) is assigned by default.
   The **Ready to Install the Program** is displayed.
6. Click **Install** to continue with the installation.

   You can also click **Back** to change the preferences.

   NOTE: At times, although the iDRAC Service Module is installed, you may receive a message "The communication between iDRAC Service Module and iDRAC could not be established. Please refer to the latest iDRAC Service Module installation guide." in the Host OS logs. For more information on troubleshooting, refer Frequently asked questions.

   The iDRAC Service Module is successfully installed.
7. Click **Finish**.

Silent installation

You can install the iDRAC Service Module using silent installation in the background without any interactive console.

- To install iDRAC Service Module using silent installation, type `msiexec /i iDRACSvcMod.msi /qn` on the command prompt.
- To generate the install logs, type `msiexec /i iDRACSvcMod.msi /L*V <logname with the path>`
- To replicate the LC logs in an existing group or a custom folder, type `msiexec /i iDRACSvcMod.msi CP_LCLOG_VIEW="<existing group name or custom folder name>"`
- To install iDRAC access via Host OS iDRAC feature using silent installation, type `msiexec /i <location of the installer file>/iDRACSvcMod.msi ADDLOCAL=IBIA /qn`
- To install WSMan, type `msiexec.exe /i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2" CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1" /qn`
- To view the user interface in the supported languages, type `msiexec /i iDRACSvcMod.msi TRANSFORMS= <locale number>.mst`, where locale number is:

Table 6. Silent installation

Locale Number	Language
1031	German
1033	English (US)
1034	Spanish
1036	French
1041	Japanese
2052	Simplified Chinese

Modifying the iDRAC Service Module components on Microsoft Windows operating systems

To modify iDRAC Service Module components:

1. Browse to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard** is displayed.
2. Click **Next**.
3. Select **Modify**.
4. Enable or disable the features as required and then click **Next**.
   The **Lifecycle Controller Log Replication** window is displayed.
5. Specify the location where you need the LC logs to be replicated. By default, **Typical (Windows Logs/System)** option is selected and the LC logs are replicated in the **System** group of the **Windows Logs** folder in the **Event Viewer**. Click **Next**.

   NOTE: You can also create a custom group in the **Application and Services Log** folder by selecting the **Custom** option in the **Lifecycle Controller Log Replication** window.

   NOTE: You may have to restart the system in the following scenarios:
   - If you switch between **Typical (Windows Logs/System)** and **Custom** options.
   - If you switch from one custom folder to another folder.

   The **Ready to install** screen is displayed.
6. Provide a unique port number to be used by iDRAC access via Host OS feature.

   NOTE: Provide a port number between the range 1024 to 65535.

   NOTE: If you do not provide a port number, *port number 1266* or a previously configured port (if any) is assigned by default.

7. Click **Install** to continue the process.
   You can also click **Back** to change the preferences.
   The iDRAC Service Module is successfully modified.
8. Click **Finish**.

Repairing the iDRAC Service Module on Microsoft Windows operating systems

If you want to repair the iDRAC Service Module component that is faulty or non-functional:

1. Browse to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard**.
2. Click **Next**.
3. Select **Repair** and click **Next**.
   The **Ready to install** is displayed.
4. Click **Repair** to continue the process.
   You can also click **Back** to change the preferences.
   The iDRAC Service Module component is successfully repaired.
5. Click **Finish**.

Uninstalling the iDRAC Service Module on Microsoft Windows operating systems

The iDRAC Service Module can be uninstalled using two different methods:

- Unattended uninstall using the product ID
- Uninstalling using the add/remove feature

Unattended uninstall using the product ID

Type `msiexec /x {BE762CE4-B8D4-4BFC-BA12-16360808DCF3} /qn` to uninstall the iDRAC Service Module using the product ID.

Uninstalling using the add or remove feature

The iDRAC Service Module can be uninstalled by using the **Add** or **Remove** option from the control panel. To do so, go to **Start** > **Control Panel** > **Programs and Features** .

NOTE: You can also uninstall by selecting **Uninstall** after you run the `iDRACSvcMod.msi`.

NOTE: You can view the iDRAC Service Module logs in the **Application** group of the **Windows Logs** folder in the Windows **Event Viewer**.

Installing iDRAC Service Module on supported Linux operating systems

The complete iDRAC Service Module is packaged in a single Red Hat Package Manager (rpm). The package, accompanied by a shell script can install, uninstall, or enable/disable the features available.

As the Installer on Linux is a single rpm install, there is no granular install support. You can enable/disable the features through the scripted installs only.

NOTE: The Installer is available for all iDRAC Service Module supported 64–bit versions of Linux operating systems.

NOTE: On repository-based installs such as, Yellowdog Updater, Modified (YUM), VMware Update Manager (VUM) and Citrix XenServer supplemental pack, all the features are not enabled by default.

NOTE: The OS log collection feature of SupportAssist Collection is not supported on CentOS.

Preinstallation requirement for Linux operating systems

To install the iDRAC Service Module on systems running the supported Linux operating system, run `setup.sh`.

Ensure that the basic functional requirements are met, such as:

- OS-to-iDRAC Passthru is enabled automatically after installing iDRAC Service Module.
- The IPv4 Network stack is enabled in the Host Operating system.
- The USB subsystem is enabled.
- `udev` is enabled; required to start iDRAC Service Module automatically.

For more information on iDRAC, see the latest *Integrated Dell Remote Access Controller User's Guide* at **dell.com/support/home**.

Linux install dependency

The following are the list of dependent packages/executable(s) that need to be installed to complete the installation.

Table 7. Linux install dependency

Executable Commands	Package Name
/sys	fileSystem
grep	grep
cut, cat, echo, pwd,	coreutils
lsusb	usbutils

Table 7. Linux install dependency (continued)

Executable Commands	Package Name
find	findutils
Shell Script commands	bash
ifconfig	net-tools
ping	Iputils
chkconfig	Red Hat Enterprise Linux • chkconfig
install_initd	Red Hat Enterprise Linux • redhat-lsb-core
Systemctl	systemd
curl	libcurl
openssl	libssl

Installing The iDRAC Service Module on Linux operating system

1. The available features that can be installed are displayed on the screen. The available options are:
   - [1] Watchdog Instrumentation Service
   - [2] Lifecycle Log Information
   - [3] Operating System Information
   - [4] iDRAC access via Host OS
     - [a] Access via GUI, WSMan, Redfish, Remote RACADM
     - [b] In-band SNMP Traps
     - [c] Access via SNMP Get
   - [5] iDRAC SSO Launcher
     - [a] Read only
     - [b] Administrator
   - [6] iDRAC Hard Reset
   - [7] Support Assist
   - [8] Full Power Cycle
   - [9] All features
2. To install the required feature, enter the number of the respective feature.

   NOTE: Separate the number of the features to be installed by a comma.

   NOTE: To install the sub-features, enter **4.a, 4.b or 4.c**.

3. To install the selected features, enter **I**. If you do not want to continue the installation, enter **q** to quit.

NOTE: After installing different features, you can also modify the same.

NOTE: To know if iDRAC Service Module is installed on your Linux operating system, run the command `/etc/init.d/dcismeng status`. If the iDRAC Service Module is installed and running, the status **running** is displayed.

NOTE: Use the `systemctl status dcismeng.service` command instead of the `init.d` command to check if the iDRAC Service Module is installed on Red Hat Enterprise Linux 7.

NOTE: You must provide a unique port number between the range 1024 to 65535 if you chose to install iDRAC access via Host OS feature. If you do not provide a port number, *port number 1266* or a previously configured port (if any) is assigned by default.

NOTE: if OpenManage Server Administrator (OMSA) is already installed on 1311, the same port could not be utilized for iDRAC Service module.

NOTE: When iSM 3.4.0 or later is installed on Linux operating systems, a gnome warning is observed similar to: *"failed to rescan: Failed to parse /usr/share/applications/iDRACGUILauncher.desktop file: cannot process file of type application/x-desktop"*.

Silent installation

You can install the iDRAC Service Module silently in the background without a user console. This can be achieved by using `setup.sh` with parameters.

The parameters that can be passed to use `setup.sh` are:

Table 8. Silent installation

Parameter	Description
-h	Help: Displays the help
-i	Install: Installs and enables the selected features
-x	Express: Installs and enables all available features
-d	Delete: Uninstall the iDRAC Service Module component
-w	Automatic System Recovery: Enables the Automatic System Recovery Instrumentation Service
-l	LC LOG: Enables the Lifecycle Log Replication
-o	OS Information: Enables the Operating System Information
-a	Autostart: Start the installed service after the component has been installed
-O	iDRAC access via Host OS: Enables the iDRAC access GUI, WS-man, Redfish, Remote Racadm
-s	Enables the in-band SNMP traps
-g	Enables access via SNMP Get
-Sr	Enables the iDRAC SSO login as Readonly user
-Sa	Enables the iDRAC SSO login as Administrator

NOTE: On Linux operating systems, if a feature modifying operation with silent option is enabled from the Linux webpack (using setup.sh), then the previously enabled feature states will be overridden by the new features select during modifying operation.

Uninstalling the iDRAC Service Module on Linux operating system

The iDRAC Service Module can be uninstalled in two different methods:

- Using uninstall script
- Using RPM command

Uninstalling the iDRAC Service Module using the uninstall script

The script used for uninstalling the iDRAC Service Module is `dcism-setup.sh`. Run the shell script and select *d* to uninstall the iDRAC Service Module.

Uninstalling the iDRAC Service Module using the RPM command

The iDRAC Service Module can be uninstalled using the RPM command `rpm -e dcism` in the command line.

Installing the iDRAC Service Module on VMware ESXi

VMware ESXi is factory-installed on some systems. For a list of these systems, see the latest *Systems Software Support Matrix* at **dell.com/support**.

The iDRAC Service module is available as a .zip file for installing on systems running VMware ESXi operating system. The .zip file follows the naming convention **ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>i-Live.zip**, where <version> is the supported ESXi version.

The zip files for the supported ESXi versions are:

- For ESXi – `ISM-Dell-Web-3.4.1-<bldno>.VIB-ESX6i-Live.zip`

NOTE: The feature configuration of iDRAC Service Module is not retained as is after a forced/ungraceful reboot. A backup of the configuration files is created by the ESXi hypervisor through the script /sbin/auto-backup.sh that runs periodically for every 60 minutes. If you want to retain the configuration, manually run the backup.sh script before you reboot the system.

NOTE: No reboot of the Host OS is required after installing or uninstalling the iDRAC Service Module Live VIB package.

Download VMware vSphere Command Line Interface (vSphere CLI) from **http://vmwaredepot.dell.com/DEL/** and install on the Microsoft Windows or Linux system.

Using the vSphere CLI

To install the iDRAC Service Module software on VMware ESXi using the vSphere CLI:

1. Copy and unzip the `ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>i-Live.zip` file to a directory on the system.
2. Shut down all guest operating systems on the ESXi host and put the ESXi host in maintenance mode.
3. If you are using vSphere CLI on Windows, go to the directory where you have installed the vSphere CLI utilities.
   If you are using vSphere CLI on Linux, perform the command from any directory.
4. Perform the following command:

   For VMware ESXi 6.7:`esxcli --server <IP Address of ESXi 6.7 host> software vib install -d /var/log/vmware/<iDRAC Service Module file>`.

   For VMware ESXi 6.5:`esxcli --server <IP Address of ESXi 6.5 host> software vib install -d /var/log/vmware/<iDRAC Service Module file>`.

   NOTE: The .pl extension is not required if you are using vSphere CLI on Linux.

5. Type the root username and password of the ESXi host when prompted.
   The command output displays a successful or a failed update.

Installing iDRAC Service Module using VMware Update Manager

To install the iDRAC Service Module using VMware Update Manager (VUM):

1. Install VMware vSphere 6.5 or later versions (vCenter Server, vSphere Client, and VMware vSphere Update Manager) on a supported Microsoft Windows operating system.
2. On the desktop, double-click **VMware vSphere Client** and login to vCenter Server.
3. Right-click **vSphere Client host** and click **New Datacenter**.
4. Right-click **New Datacenter** and click **Add Host**. Provide information for the ESXi server per online instructions.
5. Right-click the **ESXi host** added in **step 4** and click **Maintenance Mode**.
6. From **Plug-ins**, select **Manage Plug-ins** > **download VMware Update Manager**. (The status is enabled if the download is successful.) Follow the instructions to install the VUM client.

7. Select the **ESXi host**. Click **Update Manager** > **Admin view** > **Patch Repository** > **Import Patches** and follow the online instructions to upload the patch successfully.
   The offline bundle is displayed.
8. Click **Baselines and Groups**.
9. Click **create from Baselines** tab, mention baseline name and select **Host Extension** as baseline type.
   Complete the rest as per instructions.
10. Click **Admin View**.
11. Click **Add to Baseline** (against the uploaded patch name) and select the baseline name that you have created in step 8.
12. Click **Compliance view**. Select the **Update Manager** tab. Click Attach and select the **Extension Baseline** created in step 8 and follow the instructions.
13. Click **Scan** and select **Patches and Extensions** (if not selected by default) and click **Scan**.
14. Click **Stage**, select created **Host Extension** and follow the instructions.
15. Click **Remediate** and follow the instructions once the staging is completed.
    iDRAC Service Module installation is complete.

    NOTE: For more information on VMWare Update Manager, see the VMWare official website.

    NOTE: You can install iDRAC Service Module from the VUM repository **https://vmwaredepot.dell.com/**.

Upgrading iDRAC Service Module using VMware Update Manager

To upgrade iDRAC Service Module using VMware Update Manager (VUM):

1. Install VMware vSphere 6.5 or later versions (vCenter Server, vSphere Client, and VMware vSphere Update Manager) on a supported Microsoft Windows operating system.
2. On the desktop, double-click **VMware vSphere Client** and login to vCenter Server.
3. Right-click **vSphere Client host** and click **New Datacenter**.
4. Right-click **New Datacenter** and click **Add Host**. Provide information for the ESXi server per online instructions.
5. Right-click the **ESXi host** added in **step 4** and click **Maintenance Mode**.
6. From **Plug-ins**, select **Manage Plug-ins** > **download VMware Update Manager**. (The status is enabled if the download is successful.) Follow the instructions to install the VUM client.
7. Select the ESXi host. Click **Update Manager** > **Admin view** > **Patch Repository** > **Import Patches** and follow the online instructions to upload the patch successfully.
   The offline bundle is displayed.
8. Click **Baselines and Groups**.
9. Click **create** from Baselines tab, mention baseline name and select **Host Extension** as baseline type.

   NOTE: Select the latest iDRAC Service Module version to create the baseline.

   Complete the rest as per instructions.
10. Click **Admin View**.
11. Click **Add to Baseline** (against the uploaded patch name) and select the baseline name that you have created in step 8.
12. Click **Compliance view**. Select the **Update Manager** tab. Click Attach and select the **Extension Baseline** created in step 8 and follow the instructions.
13. Click **Scan** and select **Patches and Extensions** (if not selected by default) and click **Scan**.
14. Click **Stage**, select created **Host Extension** and follow the instructions.
15. Click **Remediate** and follow the instructions after the staging is completed.
    iDRAC Service Module upgrade is complete.

    NOTE: The Host OS will reboot while upgrading iSM using VMware Update Manager.

    NOTE: For more information about VMware Update Manager, see the VMware official website.

    NOTE: You can upgrade iDRAC Service Module from the VMware Update Manager repository **https://vmwaredepot.dell.com/**.

Using the Power CLI

To install the iDRAC Service Module using Power CLI:

1. Install the supported PowerCLI of ESXi on the supported Microsoft Windows operating system.
2. Copy the `ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>i-Live.zip` file to the ESXi host.
3. Navigate to the bin directory.
4. Run Connect-VIServer and provide the server and other credentials.
5. Log on to the ESXi host using supported vSphere CLI of ESXi host and create a datastore.
6. Create a folder **ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>I** on ESXi host under **/vmfs/volumes/<datastore_name>** directory.
7. Copy the ESXi zip file on ESXi host to **/vmfs/volumes/<datastore_name>ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>I** directory.
8. Unzip the zip file in the above specified directory.
9. Run the following command in Power CLI.

   For ESXi 6.7 `Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/<datastore_name>name>/ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>i/ cross_oem-dell-dciSM-esxi_3.4.1.ESXi670-0000-metadata.zip .`

   For ESXi 6.5 `Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/<datastore_name>name>/ISM-Dell-Web-3.4.1-<bldno>.VIB-<version>i/ cross_oem-dell-dciSM-esxi_3.4.1.ESXi650-0000-metadata.zip .`
10. Run the following command to check if the iDRAC Service Module is installed successfully on the host. `esxcli software vib list|grep -i dcism`.
11. iDRAC Service Module is displayed.

NOTE: Reboot the host OS once iSM is installed using the above Power CLI command.

NOTE: For more information on Power CLI, see the VMWare official website.

Upgrading iDRAC Service Module on VMware ESXi

To upgrade iDRAC Service Module, run `esxcli software vib update -v <viburl for latest version>`.

NOTE: Minimum supported iDRAC Service Module version is 3.1 for upgrade.

Uninstalling the iDRAC Service Module on VMware ESXi

The iDRAC Service Module can be uninstalled using the following command:

```
$ esxcli software vib remove -n dcism
```

Installing iDRAC Service Module when the System Configuration Lock Down Mode is enabled

When the System Configuration Lock Down Mode is enabled through iDRAC, no configuration operations can be performed for iDRACService Module. All the features that were enabled before the System Configuration Lock Down Mode was turned on will continue to be enabled. If iSM is installed after the System Configuration Lock Down Mode is enabled, then only the iSM features that were enabled earlier will be available for the users. Whenever the System Configuration Lock Down Mode is turned off in iDRAC, then all the configuration operations can be performed.

Support for iDRAC URI to get iSM installer

Starting from yx4x servers, you can download the iSM web packs by using the following URL:**https:// <iDRACIP>/ software/ism/package.xml**. You can download the packages only when iSM LC DUP is uploaded and available in iDRAC. You can also load it in iDRAC by enabling the iDRAC LC autoupdate.

To download the packages, use the filename present in the xml to append to the URL.

Example:

```
<PayloadConfiguration>
<Image filename="OM-iSM-Dell-Web-LX-3.4.1.tar.gz" id="5DD5A8BA-1958-4673-BE77-40B69680AF5D" skip="false" type="APAC" version="3.4.1"/>
<Image filename="OM-iSM-Dell-Web-LX-3.4.1.tar.gz.sign" id="E166C545-82A9-4D5D-8493-B834850F9C7A" skip="false" type="APAC" version="3.4.1"/>
<Image filename="OM-iSM-Dell-Web-X64-3.4.1.exe" id="5015744F-F938-40A8-B695-5456E9055504" skip="false" type="APAC" version="3.4.1"/>
<Image filename="ISM-Dell-Web-3.4.1-VIB-ESX6i-Live.zip" id="1F3A165D-7380-4691-A182-9D9EE0D55233" skip="false" type="APAC" version="3.4.1"/>
<Image filename="RPM-GPG-KEY-dell" id="0538B4E9-DA4D-402A-9D96-A4A55EE2234C" skip="false" type="APAC" version=""/>
<Image filename="sha256sum" id="06F61B54-58E2-41FB-8CE3-B7137A60E4B7" skip="false" type="APAC" version=""/>
</PayloadConfiguration>
```

To download Microsoft Windows web pack, access the following URL: **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-X64–3.4.1.exe**.

To download VMware ESXi Live VIB package from LC, access the following URL: **https://<iDRACIP>/software/ism/ISM-Dell-Web-3.4.1-VIB-ESX6i-Live.zip**.

To download Red Hat Enterprise Linux web pack, access the following URL: **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-LX-3.4.1.tar.gz**.

Support for idrac.local and drac.local as iDRAC FQDN

You can connect iSM to the iDRAC GUI from Host OS by typing drac.local or idrac.local in the web browser irrespective of multicast Domain Name System (mDNS) support on the Host OS.

4

Configuring the iDRAC Service Module

You can configure the iDRAC Service Module using the:

- iDRAC web interface
- RACADM CLI command
- WSMAN command

Topics:

Configuring the iDRAC Service Module from iDRAC Web Interface

To use the iDRAC Service Module from the iDRAC Web interface for yx3x servers, go to **Overview** > **Server** > **Service Module**.

To use the iDRAC Service Module from the iDRAC Web interface for yx4x and yx5x servers, go to **iDRAC settings** > **Settings** > **iDRAC Service Module setup**.

Configuring the iDRAC Service Module from RACADM

The iDRAC Service Module can be accessed and configured through RACADM CLI commands. To know the status of the features that are provided by the iDRAC Service Module, use `racadm get idrac.servicemodule` command. This command lists the features of the iDRAC Service Module and their status. The features are:

- OSInfo
- LCLReplication
- WMI Information
- Auto System Recovery Action
- iDRAC access via Host OS
- iDRACHardReset
- HostSNMPAlert
- HostSNMPGet
- iDRAC SSO Launcher

To set or configure the features, use `racadm set idrac.servicemodule. <feature name> <enabled or disabled>`.

NOTE: The name of the feature or the attribute that are listed starting from an # symbol cannot be modified.

To use the iDRAC Service Module from RACADM, see the objects in the **Service Module** group in the *RACADM Command Line Reference Guide for iDRAC8, iDRAC9, and CMC* available at **dell.com/support**.

Configuring the iDRAC Service Module from WSMan

The iDRAC Service Module can be accessed and configured through WSMan using the command

To configure the iDRAC Service Module use `winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_iDRACCardService?`

```
CreationClassName=DCIM_iDRACCardService+Name=DCIM:iDRACCardService+SystemCreationClassName=
DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:root -p:calvin -r:https://<Host IP
address>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic
@{Target="iDRAC.Embedded.1";AttributeName="AgentLite.1#<feature>";AttributeValue="1"}
```

To use the iDRAC Service Module from WSMan, see the Dell Lifecycle Controller 2 Web Services Interface Guide provides information and examples for utilizing the Web services for Management (WSMan) Management protocol, available at **dell.com/support**.

5

iDRAC Service Module monitoring features

The services provided are:

- OS information
- Lifecycle Controller Log replication into operating system
- Automatic system recovery
- Windows Management Instrumentation providers inclusive of storage data
- Prepare to remove NVMe SSD device
- Remote iDRAC hard reset
- iDRAC access via Host OS
- In-band support for iDRAC SNMP alerts
- Enable WSMan remotely
- Auto-updation of iDRAC Service Module
- FullPowerCycle
- Support Assist on the Box

NOTE: **FullPowerCycle** and **Support Assist on the Box** are supported only on the yx4x and yx5x Servers.

Topics:

- Operating system information
- Lifecycle Controller log replication into operating system
- Automatic System Recovery
- Windows Management Instrumentation Providers
- Prepare to remove NVMe PCIe SSD device
- Remote iDRAC hard reset
- iDRAC access via Host OS
- Accessing iDRAC Via GUI, WSMan, Redfish, Remote RACADM
- In-band support for iDRAC SNMP alerts
- Enable WSMan Remotely
- Auto-updating iDRAC Service Module
- FullPowerCycle
- SupportAssist on the Box
- Enabling the In-band SNMP Get feature—Linux
- Enabling the In-band SNMP Get feature—Windows
- iDRAC GUI Launcher
- Single sign-on (SSO) to iDRAC GUI from Host OS administrators desktop
- IPv6 communication between iSM and iDRAC over OS-BMC Passthru
- Enhanced security between iSM and iDRAC communication using TLS protocol

Operating system information

OpenManage Server Administrator currently shares operating system information and host name with iDRAC. The iDRAC Service Module provides similar information such as host OS name, server host IP address information, OS version, Fully Qualified Domain Name (FQDN) with iDRAC. The network interfaces on the host OS are also displayed. By default, this monitoring feature is enabled. This feature is available even if OpenManage Server Administrator is installed on the host OS.

You can also view Host OS network interface details, or such information through Redfish client plug-in for browsers.

NOTE: The minimum iDRAC firmware version required to view information using Redfish client is 3.00.00.00.

NOTE: If the network configuration on the Host OS is configured using netplan, then iSM will be unable to monitor the network interfaces' change in states, DHCP configuration of an interface for instance. Hence you may not be able to view the change of the Host OS network interface details in the iDRAC interfaces.

Lifecycle Controller log replication into operating system

Replicates the Lifecycle Controller (LC) logs to the OS logs. All events that have the OS Log option as the target (in the Alerts page or in the equivalent RACADM or WSMan interfaces) are replicated in the OS log. This process is similar to the System Event Log (SEL) replication performed by OpenManage Server Administrator.

The default set of logs to be included in the OS logs are the same as the logs configured for SNMP traps/alerts. Only the events logged in the LC log after the iDRAC Service Module was installed are replicated to the OS Log. If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate SEL entries in the OS log.

In iDRAC Service Module, you can customize the location to replicate the LC logs. By default, the LC logs are replicated in the **System** group of the **Windows logs** folder in the Windows **Event Viewer**. You can replicate the LC logs to an existing group or create a new folder in the **Application and Services Logs** folder in the Windows **Event Viewer**. When iSM is already installed and if the Host OS undergoes a reboot or iSM is restarted, and iDRAC has some LC logs generated during this duration of host time down, then iSM logs these LC logs as past events in the OS log as soon as the service starts.

NOTE: You can choose the location to replicate the LC logs only during iDRAC Service Module custom installation or iDRAC Service Module modification.

NOTE: The source name of the iDRAC Service Module LCL logs has been changed from **iDRAC Service Module** to **Lifecycle Controller Log**.

Automatic System Recovery

Automatic System Recovery feature is a hardware-based timer, which is used to reset the server in the event of a hardware failure. You can perform automatic system recovery operations such as reboot, power cycle, or power off after a specified time interval. This feature is enabled only when the operating system watchdog timer is disabled. If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate watchdog timers.

You can configure three parameters in this feature from iDRAC interfaces:

1. **Watchdog state**: The default state is enabled when OMSA is not present, and when BIOS or OS watchdog timer is disabled.
2. **Watchdog timeout**: The default value is 480 seconds. The minimum value is 60 seconds and the maximum value is 720 seconds.
3. **Watchdog timeout Recovery Action or Auto Recovery Action**: The actions can be **Powercycle**, **Power Off**, **Reboot** or **None**.

Windows Management Instrumentation Providers

Windows Management Instrumentation Providers available with iDRAC Service Module exposes hardware data through Windows Management Instrumentation (WMI). WMI is a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF) to manage Server hardware, operating systems and applications. WMI Providers helps to integrate with Systems Management Consoles such as Microsoft System Center and enables scripting to manage Microsoft Windows Servers.

The namespace used is `\\root\cimv2\dcim`. The supported queries are **Enumeration** and **Get**. You can use any of the WMI client interfaces such as **winrm**, **Powershell**, **WMIC**, **WBEMTEST** to query the iDRAC supported profiles via the Host OS.

Prepare to remove NVMe PCIe SSD device

You can remove a Non-Volatile Memory Express (NVMe) Pheripheral Component Interconnect Express (PCIe) Solid State Device (SSD) without shutting down or rebooting the system. When you are removing a device, all the activities associated with the device must be stopped to prevent data loss. To prevent loss of data use the Prepare to Remove option, which stops all the device-associated background activities, after which you can remove the NVMe PCIe SSD physically.

NOTE: Follow the VMware documented prerequisites before performing **Prepare to Remove** operation in VMware ESXi.

Remote iDRAC hard reset

iDRAC may become unresponsive due to various reasons. iSM can fully reset an unresponsive iDRAC8 or iDRAC9 controller by temporarily removing power to the iDRAC controller without affecting operating system production. This feature can only be disabled from the iDRAC Service Module page in iDRAC using any of the iDRAC interfaces.

To reset iDRAC, use the following Windows PowerShell or Linux shell command:

```
./Invoke-iDRACHardReset
```

NOTE: This feature only works with iDRAC8 on the yx3x servers or later and if logged into the operating system as an administrator.

iDRAC access via Host OS

Using PowerEdge Servers, you can manage the hardware or the firmware of a device through iDRAC by configuring an iDRAC dedicated network. Through the dedicated network port, you can access the iDRAC interfaces such as GUI, WSMan, RACADM, and Redfish client.

The prerequisite to manage the hardware or the firmware is to have a dedicated connection between a device and the supported iDRAC interface. Using the iDRAC access via Host OS feature, you can connect to an iDRAC interface from an OS IP or host irrespective of the connection between a device and an iDRAC dedicated network. This feature allows you to monitor the hardware or firmware even if the iDRAC is not connected to the network.

You can select any of the following sub features to enable the iDRAC access via Host OS:

- **Access via GUI, WSMan, Redfish, Remote RACADM**
- **In-band SNMP Traps**
- **Access via SNMP Get**

If you select **iDRAC access via Host OS**, all the sub features are selected by default. If you want to select any one of the individual sub feature, you can select a particular feature and enable it.

For more information, see iDRAC Access via Host OS whitepaper.

Accessing iDRAC Via GUI, WSMan, Redfish, Remote RACADM

Access via GUI, WSMan, Redfish, Remote RACADM feature enables a Host OS administrator to access iDRAC interfaces remotely via the Host OS. Type the URL `https:// <Host OS IP Address>: <ListenPortNumber>` in the browser of the remote management station to access the iDRAC GUI.

NOTE: The ListenPortNumber is the port number configured while enabling the iDRACAccessviaHostOS feature in iSM.

In-band support for iDRAC SNMP alerts

Using iDRAC, an out-of-band server management and monitoring tool, the SNMP traps/alerts can be recorded in the log. However, from a host OS systems management using in-band agent perspective, the preference is more on the SNMP alert

received from the host OS than the traps received from iDRAC. When an SNMP alert is received from iDRAC, it would be challenging to determine the source of the alert as it is from an iDRAC IP and not the system IP.

Starting from yx4x servers, all events that have the **SNMP Trap** option as the target (in the Alerts page or in the equivalent RACADM or WSMan interfaces) can be received as SNMP trap through the OS using the iDRAC Service Module. For iDRAC firmware 3.0.0 or later, this feature does not require iSM LCL replication feature to be enabled. Only the events logged in the LC log after the iDRAC Service Module was installed are sent as SNMP traps.

Using iDRAC Service Module, you can receive SNMP alerts from the host OS which is similar to the alerts that are generated by iDRAC.

NOTE: By default this feature is disabled. Though the In-band SNMP alerting mechanism can coexist along with iDRAC SNMP alerting mechanism, the recorded logs may have redundant SNMP alerts from both the sources. It is recommended to either use the in-band or out-of-band option, instead of using both.

NOTE: You can use the In-band SNMP feature on yx3x Servers or later with a minimum iDRAC firmware version 2.30.30.30.

For more information, see In-Band iDRAC SNMP Alerts whitepaper.

Enable WSMan Remotely

Currently with the WMI information feature, you can connect to the host Microsoft Windows WMI namespace to monitor the system hardware. The WMI interface on the host is enabled by default and you can access it remotely. However, if you wish to access the WMI interfaces using WINRM's WMI adapter, you have to enable it manually as it is not enabled by default. Using this feature, you can access the WINRM WMI namespaces remotely by enabling it during installation.

This feature can be accessed using PowerShell commands. The commands used are as follows:

Table 9. Enable WSMan Remotely

Command	Description
`Enable-iSMWSMANRemote –Status enable –Forcereconfigure yes –Createselfsigncert yes –IPAddress <IP address> –Authmode Basic, Kerberos, Certificate`	Enabling and configuring the remote WSMan feature
`Enable-iSMWSMANRemote –Status get`	Viewing the status of remote WSMan feature
`Enable-iSMWSMANRemote –Status disable`	Disable remote WSMan feature
`Enable-iSMWSMANRemote –Status enable –Forcereconfigure yes –Createselfsigncert yes –IPAddress <IP address>`	Reconfigure the remote WSMan feature

NOTE: You must have a server authenticating certificate and a https protocol to work with this feature.

Auto-updating iDRAC Service Module

You can auto-update the iDRAC Service Module. It aims at making the update process easier for you, by integrating iSM update with the iDRAC auto-update process.

NOTE: If iDRAC auto-update is enabled, iDRAC Service Module LC DUP must be updated to the latest version from dell.com/support.

NOTE: You do not have to download the updates from support.dell.com. The updated iSM package is locally available in iDRAC.

NOTE: iDRAC Service Module LC DUP in iDRAC will be removed when the iDRAC LC Wipe option is used. You will have to download the iDRAC Service Module LC DUP from dell.com/support.

- To install or update iSM, type `dcism-sync.exe` in the command prompt. Complete the steps in the installation wizard.
- To display the help content, type`--help/-h`.

- To do silent install or update, type `--silent/-s`.
- To uninstall the current version and install the update package available in LC, type `--force/-f`.

  NOTE: This option overwrites the previous configuration.
- To get details about the update package version and the installed version of iDRAC Service Module, type `--get—version/-v`.
- To download the iDRAC Service Module update packages to the user specified directory, type `--get—update/-g`.
- To install specific features, the same as CLI arguments used with `msiexec.exe`, type `dcism-sync.exe —p "feature"`.

  For example, to install iDRAC access via Host OS iDRAC feature on Windows, type `dcism-sync.exe -p "ADDLOCAL=IBIA"`.

FullPowerCycle

FullPowerCycle is a calling interface function that provides a way to reset the server auxiliary power. An increasing amount of server hardware runs on server auxiliary power; and troubleshooting of some server issues requires you to physically unplug the server power cable to reset the hardware running on auxiliary power. Forcing someone to physically unplug/plug the power cables leads to a significant cost and hassle for customers and support personnel.

The FullPowerCycle feature enables the administrator to connect or disconnect the auxiliary power remotely without visiting the data center. This feature is supported on and after yx4x servers.

When a Full Power Cycle **Request** is issued through this interface, the system power is not immediately affected. Instead, a flag is set, that is queried when the system transitions to S5. For FullPowerCycle feature to take effect, after issuing the request command you have to issue system shutdown command also. If the flag is set on S5 entry, the system will temporarily be forced into a lower power state, similar to removing and replacing AC. The flag can be cleared using the **Cancel** function any time the system is in the S0 state prior to the system entering the S5 state.

You can avail different options of FullPowerCycle on your system. Use the following commands to request, get status, and cancel the Full Power Cycle on your system:

For Windows Operating systems, shortcut menus are available for the FullPowerCycle Activate (request), FullPowerCycle Cancel and FullPowerCycle get status operations.

- To request FullPowerCycle on your system, type `./Invoke-FullPowerCycle —status request`.

  NOTE: A message is displayed that the VirtualAC Power Cycle operation is triggered by the server operating system.
- To get the status of the Full Power Cycle on your system, type `./Invoke-FullPowerCycle -status get`.
- To cancel the Full Power Cycle on your system, type `./Invoke-FullPowerCycle -status cancel`.

  NOTE: A message is displayed that the system is going for turn off at the scheduled date and time.
- To request FullPowerCycle on Linux operating system, type `/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle request`
- To cancel FullPowerCycle on Linux operating system, type `/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle cancel`
- To get FullPowerCycle status on Linux operating system, type `/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle get-status`

Following messages are displayed after each successful FullPowerCycle operation on operating system log and LCL.

Request message:`"The Full Power Cycle operation is triggered by the server operating system (OS) user <user name> from the OS on date <date>. However, the server components will be AC power cycled when the server is shut down".`

Cancel Message: `"The Full Power Cycle operation is successfully cancelled by the server operating system (OS) user <user name> from the OS on date <date>".`

NOTE: FullPowerCycle feature is not available for ESXi operating systems.

NOTE: FullPowerCycle feature can be used only with local/domain administrator or root/sudo users.

SupportAssist on the Box

SupportAssist saves time and streamlines the technical support cases. A collection based on an event creates an open service request with SupportAssist. Scheduled collections helps to monitor and maintain your environment. These collections include the hardware data, RAID controller logs, OS, and Application Data. The features supported are :

- **SupportAssist Registration** — iSM supports the SupportAssist Registration. This is a one time activity. You can enter the required details such as name, email, address, and number to complete the registration.
- **SupportAssist Collection**— The SupportAssist Collection feature in iDRAC collects information about the hardware, OS and relevant application data and compresses this information.

SupportAssist also provides:

- Proactive issue identification
- Automated case creation
- Support contact initiated by a Dell technical support agent

NOTE: You must complete the registration to take the advantages of SupportAssist.

You can view the following items in the SupportAssist dashboard.

Service Request Summary

In the Service Request Summary session, you can view the details of the following requests:

- Open
- Closed
- Submitted

Support Assist Overview

You can view the **Service Contract** details such as Contract Type and Expiration Date and the **Automatic Collection** settings details in this session.

On the **Service Requests** tab, you can also view the list of requests created and the status, description, source, service request ID, date opened, the date closed, and so on.

If you click the **Collection Log** tab, you can view the collection time, job ID, collection type, data collected, collection status, sent time, and so on.

NOTE: Starting from yx4x servers, when you manually initiate SupportAssist collection from iDRAC, the USB mass storage device is not exposed to the host OS. The transfer of OS Collector files and the collected log files is handled internally between iDRAC and iSM.

NOTE: The OS and Application Data collection on ESXi is supported only by yx4x and later servers.

SupportAssist Registration

Before you begin the registration, ensure that iDRAC Service Module is installed and running in the host OS, and a proper Internet connection is available.

1. Log in to iDRAC. From the **Maintenance** drop-down menu, select the **SupportAssist** feature.
   The **SupportAssist Registration** wizard is displayed.
2. On the **Welcome** tab, click **Next**.
3. On the **Contact and Shipping Info** tab, provide your primary contact information such as **First Name**, **Last Name**, **Phone Number**, **Alternate Number**, **Email Address**, **Company Name**, **Address Line 1**, **Address Line 2**, **City**, **State**, **Zip Code**, and **Country**.

   NOTE: You can add the secondary contact information, by clicking the **Add Secondary Contact Information** option.

   NOTE: To continue with the registration, you must fill all the mandatory information required.

4. After filling the contact and shipping information, click **Next**.
5. Read the software license agreement, select **I accept the terms of the license agreement**, and then click **Register**.

   NOTE: It might take few minutes to complete the registration process. After the registration is completed successfully, you will get a welcome email from SupportAssist to the email address being registered.

6. On the **Summary** tab, view the **Registration ID** and **Automatic Features** current setting details.
7. To close the **SupportAssist Registration** wizard, click **Close**.
   In the SupportAssist page, if you navigate to the bottom you can view the contact information.
8. Click the **Edit** option to make any changes in the primary or secondary contact information. Click **Save** to apply the changes.

SupportAssist Collection

The SupportAssist Collection feature in iDRAC collects information about the hardware, OS and relevant application data and compresses the information being collected. Run the OS Collector tool manually to generate the SupportAssist Collection Report. Using iDRAC Service Module, the OS Collector tool automatically collects relevant OS and hardware information. Automatic Support Log collection includes OS and Application Information Collection.

By using iDRAC Service Module, you reduce the number of manual steps to collect the Technical Support Report as the collection process is automated.

Data to Collect

SupportAssist automatically creates and send a collection to technical support when there is an event-based trigger and or on a scheduled cadence. You can collect the following type of information:

- **System Information**
- **Storage Logs**
- **OS and Application Data**
- **Debug Logs**

You can also perform the SupportAssist collection function from an operating system shell to a specified file path using:

```
./ Invoke-SupportAssistCollection [--filepath/-f]
```

NOTE: This shell command is only supported on iDRAC9 in the yx4x servers and later and if logged into the operating system as an administrator.

NOTE: On Windows Core OS, user will have to go to the absolute path to execute the `Invoke-SupportAssistCollection.exe` command.

Collection Preferences

User can select or set the collection preferences using this feature. You can select any of the following types of collection preferences to save the collection reports:

- **Send Now**— You will get a notification that 'the job has been successfully added to the job queue' after you click the **Collect** option.
- **Save Locally**
- **Save to Network**— If you select this option, you must provide the **Network Settings** details such as **Protocol**, **IP Address**, **Share Name**, **Domain Name**, **User Name**, and **Password**.

You can select any of the collection preferences and click **Collect** to receive the data.

NOTE: This feature is available by default when you install iDRAC Service Module 2.0 or later versions on systems running supported Microsoft or Linux operating systems. You cannot disable the feature.

NOTE: The OS log collection feature of Automatic SupportAssist Collection is not supported on CentOS.

NOTE: The OS and Application Data collection on ESXi is supported only by yx4x and later servers.

Anonymous Collection of Report

Starting from iDRAC Service Module version 3.1, you can perform SupportAssist Collection/Upload without completing the registration process. Until iSM 3.0.2, the registration was a prerequisite to perform SupportAssist Collection.

The supported iDRAC firmware for the anonymous collection is iDRAC 3.15.15.15 in the yx4x and yx5x servers and 2.60.60.60 in the yx3x servers.

NOTE: You can perform Anonymous SupportAssist Collection upload using blank username or password in proxy environment on the yx3x servers.

SupportAssist Collection Settings

You can navigate in the SupportAssist dashboard page in iDRAC and click the **Settings** drop-down menu, to open the SupportAssist Collection Settings.

Set Archive Directory

You can store the copies of collections performed by SupportAssist into a directory. You must click the **Set Archive Directory** button to set the location.

Identification Information

You can include the identification information in the data sent by clicking the drop-down menu and selecting any of the following options:

- **No**
- **Yes**

Email Notifications

You can select the preference to receive email notifications when a new support case is opened or a new SupportAssist collection is uploaded. From the **Receive Email Notifications** drop-down menu, select any of the following:

- **Yes**
- **No**

You can also select the language preference. The available languages are:

- **English**
- **German**
- **French**
- **Japanese**
- **Spanish**
- **Simplified Chinese**

Automatic Collection

By default, the automatic collection feature is enabled. To disable this feature, use the drop-down menu:

- **Enable**
- **Disable**

You can also specify the time for scheduled collection by selecting any of the following options from the **Schedule automatic collections** drop-down menu:

- **Weekly**
- **Monthly**
- **Quarterly**
- **Never**

You can also set the automatic collection as recurring.

To view the ProSupport Plus Recommendations report, select **Yes** from the **Send ProSupport Plus Recommendations Report** drop-down menu.

After setting the preferences, click **Apply** to save the changes.

iSM SupportAssist Disk Auto Dispatch

Starting iSM 3.4, if the server hits one of the following SNMP events: **PDR16 and PDR63**, then you get a recommendation from Dell EMC support via email regarding the dispatch of the predictive failure or a bad disk block such as SSDs subject to the prevailing licensing terms and conditions. Once you receive the email, you need to follow up and provide the service address to Dell EMC support for the delivery of the dispatched parts.

NOTE: This feature is available only on Windows operating systems.

iSM 3.4.0 or later supports filter and non-filter **OSApp Collection** (OS and Application Data collection) on ESXi. This selection can be made from **Collection Preferences**.

Non-filtered selected Collection contains **vmsupport** logs for **Logs**, **Network**, **Storage**, **Configuration**, **Installer**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines**, and **hostProfiles**.

Filtered selected Collection contains **vmsupport** logs for **Storage**, **Configuration**, **Installer**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines**, and **hostProfiles**.

Enabling the In-band SNMP Get feature—Linux

Install and configure **net-snmp** package to accept SNMP requests from remote systems. This feature is disabled by default.

For installing the in-band SNMP get feature through setup.sh installer complete the following tasks:

1. Start the iSM installation using the setup.sh script by executing `./setup.sh`
2. Review the license agreement and accept to proceed with the installation.
3. On the next page, the list of features are shown. Select the **Access via SNMP Get** sub option under the **iDRAC access via Host OS** feature by entering **4.c** , and press **Enter**.
4. After the feature is enabled, start the installation process of the selected features by entering **I** and press **Enter**.
5. After the installation is finished successfully, start the iDRAC Service Module process.
   If SNMP Agent service is not enabled on iDRAC, iSM configures and enables the SNMP Agent.
6. To view the SNMP Agent properties, on the iDRAC GUI, Go to **Settings**.
7. Click **iDRAC Service Module Setup**.
8. Under **Monitoring** session, view that **SNMP Get via Host OS** option is enabled.
9. Open a new '**PuTTY Configuration**' window, provide your Host Name IP address and click **Open**.
10. Click **Yes**, for the **PuTTY Security Alert**.
11. Log in to iDRAC using the proper credentials.
12. Type ***racadm get iDRAC.ServiceModule.HostSNMPGet*** and enter.
    You can view that **HostSNMPGet** is enabled.

    NOTE: If the In-Band SNMP Get feature was not enabled during the Installation of iSM, it can be enabled later through iDRAC GUI/Racadm command.

    - Through iDRAC GUI — **iDRAC Settings->Settings->iDRAC Service Module Setup->Enable SNMP Get via Host OS->Enable or Disable**
    - Through Racadm — **racadm set idrac.servicemodule.HostSnmpGet "Enabled"or "Disabled"**

    NOTE: iDRAC GUI/Racadm commands for In-Band SNMP Get feature is applicable only for yx4x and yx5x servers. On yx3x servers, you must use the iSM installer for enabling/disabling this feature.

    NOTE: When SNMP Get feature is enabled, it creates an iDRAC user "**iSMSnmpUser**" for SNMPv3 support internally. If the user already exists, iSM logs an error message saying "Unable to create the "iSMSnmpUser" on iDRAC because the username already exists. Then SnmpGet via Host OS feature is disabled." and the feature is disabled. In such cases, the you must remove the "iSMSnmpUser" in iDRAC and disable and enable the **Enable SNMP Get via Host OS** feature on iDRAC GUI once again. The user, "iSMSnmpUser" created by iSM is deleted when the feature is disabled or iSM is uninstalled. SNMP Get feature will not work when there are maximum number of iDRAC Users created and there are no further slots.

Enabling the In-band SNMP Get feature—Windows

The In-band SNMP Get feature allows you to query the system management data over the SNMP service on the host operating system. The host SNMP services should be enabled and configured s a prerequisite for this feature.

The SNMP service on the iDRAC should be enabled. If it is not enabled, then iDRAC Service Module will enable and configure the SNMP service on the iDRAC. This feature can be enabled or disabled using any of the iDRAC interfaces or the installer.

This feature supports SNMP v1 and v2 on Microsoft Windows Operating Systems and SNMP v1, v2 and v3 on Linux operating systems.

NOTE: iDRAC GUI/Racadm commands for In-Band SNMP Get feature is applicable only for yx4x and later servers.

NOTE: iDRAC Service Module 3.4.1 supports only the iDRAC SNMP OID 1.3. 6.1. 4.1.674.10892.5.

iDRAC GUI Launcher

Using iDRAC Service Module 3.1 or later, you can launch iDRAC GUI from your local system. Double click the **iDRAC GUI Launcher** icon. The iDRAC GUI login page opens in the default browser. Use the iDRAC credentials to login to the iDRAC home page. This is supported only on the Microsoft Windows operating systems. The short cut is available on the start menu after the successful installation of iSM 3.1 or later.

NOTE: When the iDRAC Service Module is disabled, the iDRAC GUI Launcher icon is also disabled.

NOTE: If the default browser proxy is set to use the system proxy, then you will see a failure to launch the iDRAC GUI. You have to copy the IP address from the address bar and enter it in the exception list of 'proxy settings'.

Single sign-on (SSO) to iDRAC GUI from Host OS administrators desktop

Overview

Starting iSM 3.4, host administrators will have an option to launch iDRAC from within the host OS. **iDRAC SSO launcher** requires a desktop environment of the host OS.

NOTE: Non-administrators cannot access this feature on the host OS.

The single sign-on (SSO) feature enables an authenticated OS administrator to directly access the iDRAC web interface without requiring login of separate iDRAC administrator credentials. On installing this feature, a **Program Menu** shortcut that is called **Invoke-iDRACLauncher** on Microsoft Windows operating systems is created. On the Linux operating system, iSM creates a shortcut under **Applications**, where the user can double-click and launch the iDRAC dashboard. iSM provides a command-line interface that is called **Invoke-iDRACLauncher** on Microsoft Windows operating systems and **Invoke-iDRACLauncher.sh** on Linux operating systems.

Users can choose from two types of privileges to login to iDRAC.

- As a **Readonly** user: An express or typical install of iSM installs **iDRAC SSO launcher** enabling the administrator to log in to iDRAC as a **ReadOnly** user. Besides the ability to view component health status, logs, and inventory, this enables few additional **SupportAssist** operations required by the service personnel
- As an **Administrative** user: Installing this feature by selecting the **Administrator** privilege enables the Host OS administrator to log in to iDRAC as an Operator user. The user will be able to perform all the operations as that of an iDRAC root user except configuring or deleting iDRAC users or clearing the Lifecycle Log.

NOTE: See the *iDRAC 9 User's Guide* for specific privileges granted to a *Readonly* or *Operator* user account.

Disable Single Sign-On into iDRAC from Host OS: The user can also opt to **Disable** this feature completely. When iSM is installed by disabling this feature, launching **iDRAC GUI launcher** launches the iDRAC login page with the default browser.

NOTE: *Invoke-iDRACLauncher* is independent of the iSM service and can be invoked even if iSM service is stopped.

NOTE: When browsers are not installed on the Host OS or *Invoke-iDRACLauncher* is not able to launch iDRAC due to browser issue, a session is created in iDRAC already. An iDRAC admin user can log in to iDRAC and delete the sessions.

Following are the iDRAC GUI Launcher behavior with different **OS-to-iDRAC Passthru**states:

- When **OS-to-iDRAC Passthru** setting in iDRAC is disabled, Invoke-iDRACLauncher prompts if you want to enable OSBMC-Passthru in USBNIC mode.
- When **OS-to-iDRAC Passthru** setting is already configured in LOM mode, the iDRAC Launcher does not launch the iDRAC GUI.
- When **OS-to-iDRAC Passthru** setting is disabled in iDRAC and **Disable iDRAC Local Configuration using Settings** is also disabled or lockdown mode is enabled in iDRAC, iDRAC GUI is not launched.
  NOTE: When *Local Configuration using Settings* or *Local Configuration using RACADM* is disabled in iDRAC, iDRAC login screen is displayed.

NOTE: When an iDRAC SSO session is active on the Host OS, closing the related terminal closes the browser with SSO session as well.

NOTE: Ensure to invoke *iDRAC GUI Launcher* from a GUI supported and capable interface.

NOTE: iDRAC GUI Launcher does not open the iDRAC UI when the USBNIC interface on the Host OS is configured with IPv6 address.

Prerequisites

Linux packages:

1. Browser such as **Mozilla firefox**.
2. Sudo.
3. yx4x and later servers.
4. iDRAC firmware versions 3.30.30.30 and above.

Limitations for Linux operating systems

The limitations of the **iDRAC SSO Launcher** for Linux operating systems are:

1. iSM does not support desktop utilities other than GNOME.
2. iSM does not support browsers other than **Mozilla firefox**.

NOTE: When local configuration over KCS/racadm is disabled in iDRAC, then iDRAC login screen will be displayed.

IPv6 communication between iSM and iDRAC over OS-BMC Passthru

Starting iSM 3.4, iSM supports both IPv4 and IPv6 modes of communication. Once you install iSM, iSM service attempts to connect to iDRAC using IPv4 link-local address. If there is no IP address on the Host USBNIC interface, iSM tries to configure IPv4 address on the Host side. This USBNIC interface configuration on the Host OS from iSM is done only once. iSM remains disconnected from iDRAC if there is any subsequent scenario of incomplete configuration of USBNIC on the Host OS. In case the connection fails even after configuring IPv4 address, iSM tries to connect to iDRAC using IPv6.

NOTE: This feature is supported only on Linux operating systems.

NOTE: If IPv6 network stack is disabled on the Host OS, then iSM retries to communicate with iDRAC using IPv4.

If either of the protocols are disabled, then iSM will not try to connect to iDRAC using the disabled protocol.

NOTE: If the iDRAC firmware version does not support IPv6 on USBNIC, the connection between iSM and iDRAC is established using IPv4.

Respective audit messages are logged by iSM indicating the protocol version using which iSM connected with iDRAC.

NOTE: When iDRAC USBNIC is already configured with only IPv6 address on the Host OS and then iSM is installed on the Host, then iSM communication with iDRAC will start using IPv4 protocol.

Unsupported features with IPv6 protocol

The features that are not supported when iSM is configured with IPv6 protocol and IPv4 configuration is not available on the USBNIC interface are:

- InBand iDRAC Access
- iDRAC GUI Launcher
- iDRAC SSO Launcher
- idrac.local and drac.local
- Auto-update of iSM

Enhanced security between iSM and iDRAC communication using TLS protocol

Starting iSM 3.4, the data communication between iSM and iDRAC happens through TLS protected USBNIC INET sockets. This ensures protection of all the data that transports from iDRAC to iSM over USBNIC. iSM and iDRAC use self-signed certificates to control Authentication. The self-signed certificates have 10 years of validity. Fresh self-signed certificates are generated while installing iSM every time. Reinstall or upgrade iSM if the certificates expire.

NOTE: iSM reinstall (repair) does not work on Linux operating systems. It is mandatory to uninstall and then install iSM on Linux operating systems.

NOTE: When iSM's TLS (client) certificate expires, then communication between iSM and iDRAC fails and an OS audit log is generated indicating the same. This requires you to reinstall iSM on the Host OS.

Both iDRAC and the Host TLS versions should be 1.1 or above. Communication between iSM and iDRAC fails if the TLS protocol version negotiation fails. If iSM with TLS capability is installed on an iDRAC firmware which does not support TLS communication over USBNIC, it will work with the non-TLS channel as in the older versions of iSM.

NOTE: If iSM is installed or upgraded to version 3.4.0 or later before iDRAC is upgraded to version 3.30.30.30 or later, then iSM should be uninstalled and re-installed to establish new TLS certificate.

NOTE: iSM with TLS capability is supported on iDRAC firmware versions 3.30.30.30 and above.

NOTE: iSM without TLS capability does not function on a TLS-capable version of iDRAC firmware. For example: iSM 3.3 or older which are not TLS-capable is not supported on iDRAC firmware 3.30.30.30 and later.

NOTE: If iSM 3.3.0 is installed on iDRAC 3.30.30.30 firmware, multiple events with ISM0050 are observed in LCLog.

6

Frequently asked questions

This section lists some frequently asked questions about the iDRAC Service Module.

Do I need to uninstall OpenManage Server Administrator before installing or running the iDRAC Service Module?

No. Before you install or run the iDRAC Service Module, ensure that you have stopped the features of OpenManage Server Administrator that the iDRAC Service Module provide.

NOTE: Uninstalling the OpenManage Server Administrator is not required.

How do I know that the iDRAC Service Module is installed in my system?

To know if the iDRAC Service Module is installed on your system,

- On Windows:

  Run the `service.msc` command. Find from the list of services if there is a service by name **DSM iDRAC Service Module**.

- On Linux:

  Run the command `/etc/init.d/dcismeng status`. If the iDRAC Service Module is installed and running, the status displayed will be **running**.

NOTE: Use the `systemctl status dcismeng.service` command instead of the `init.d` command to check if the iDRAC Service Module is installed on Red Hat Enterprise Linux 7.

How do I know which version of the iDRAC Service Module I have in my system?

To check the version of the iDRAC Service Module in the system, click **Start** > **Control Panel** > **Programs and Features**. The version of the installed iDRAC Service Module will be listed in the **Version** tab. You can also check the version by go to **My Computer** > **Uninstall or change a program**.

What is the minimum permission level required to install the iDRAC Service Module?

To install the iDRAC Service Module, you must have operating system Administrator level privileges.

Whenever I try to install the iDRAC Service Module, it shows an error message **This is not a supported server**.

Consult the User Guide for additional information about the supported servers. What should I do now?

Before installing the iDRAC Service Module, ensure that the server or the system on which the iDRAC Service Module is to be installed is a yx3x or later server. Also make sure that you have a 64-bit system.

I see the message**The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel** in the OS log, even when the OS to iDRAC Pass-through over USBNIC is configured properly. Why do I get this message?

iDRAC Service Module uses the OS to iDRAC Pass-through over USBNIC to establish communication with iDRAC. Sometimes, the communication is not established though the USBNIC interface is configured with correct IP endpoints. This may happen when the host OS routing table has multiple entries for the same destination mask and the USBNIC destination is not listed as the first one in routing order.

Table 10. Details

Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
default	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

In the example **enp0s20u12u3** is the USBNIC interface. The link-local destination mask is repeated and the USBNIC is not the first one in order. This results in the connectivity issue between iDRAC Service Module and iDRAC over the OS to iDRAC Pass-through. To troubleshoot the connectivity issue, you can perform one of the following steps:

Ensure that the iDRAC USBNIC IPv4 address (by default it's 169.254.1.1) is reachable from the host OS. If not:

- Change the iDRAC USBNIC address on a unique destination mask.
- Delete the unwanted entries from the routing table to ensure USBNIC is chosen by route when the host wants to reach the iDRAC USBNIC IPv4 address.

Whenever I try to install the iDRAC Service Module, an error message This operating system is not supported is displayed.

The iDRAC Service Module can be installed only on the supported operating systems. For information on operating systems that are supported, see Supported operating systems.

I used the remote iDRAC hard reset feature to reset the iDRAC. However, the IPMI is unresponsive and I am not able to troubleshoot.

If you try to use the remote iDRAC hard reset feature on **VMware ESXi 5.5 U3** or **ESXi 6.0 U1**, the IPMI drivers becomes unresponsive, because of this the iDRAC Service Module communication is stopped. You may have to reboot the server and load the IPMI driver again to resolve the issue.

Where do I find the Replicated LifeCycle log on my Operating System?

To view the replicated LifeCycle logs:

Table 11. Frequently asked question

Operating System	Location
Microsoft Windows	**Event viewer** > **Windows Logs** > ***<Existing group or Custom folder>***. All the iDRAC Service Module LifeCycle logs are replicated under the source name **iDRAC Service Module**.
Red Hat Enterprise Linux	**/var/log/messages**
VMware ESXi	**/var/log/syslog.log**

What is the default SNMP protocol configured in iDRAC Service Module to send alerts in Linux operating systems?

By default, the SNMP multiplexing protocol (SMUX) is configured in iDRAC Service Module to send alerts.

SMUX is not supported on my system. Which protocol should I configure to send alerts?

If SMUX is not supported on your system, Agent-x is used as a default protocol.

How do I configure iDRAC Service Module to use the Agent-x protocol to send alerts by default?

You can configure Agent-x as the default protocol using `./Enable-iDRACSNMPTrap.sh 1/agentx -force` command. If `-force` is not specified, ensure that the net-SNMP is configured and restart the snmpd service.

What are the Linux-dependent packages or executables I should install while completing the Linux installation?

To see the list of Linux-dependent packages, see Linux dependencies.

I created a custom folder in Windows Event Viewer, but the LC logs are not replicated in my custom folder. What do I have to do now to replicate the LC logs?

Ensure to close the Windows **Event Viewer** after creating the custom folder. Open the Windows **Event Viewer** again to view the replicated LC logs.

I chose custom install option from the Graphical User Interface during iDRAC Service Module installation and disabled a feature, but I am not able to enable the feature using any of the other interfaces. How do I enable the feature again?

On systems running Microsoft 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 Graphical User Interface mode.

For example, you may not be able to enable a feature using the RACADM CLI commands, that was disabled from the Graphical User Interface during iDRAC Service Module installation.

I am not able to access the iDRAC page through the host OS as an Active Directory user over LDAP. I am trying to access the iDRAC page through the host OS, but I get an error saying that the site cannot be reached. How do I troubleshoot the issue?

When you are trying to access the iDRAC page through the host OS, you may get an error saying that the site cannot be reached. Ensure that the iDRAC network is configured for authentication as an LDAP user. You can also login as a local user or a guest.

I am not able to access the iDRAC page through the host OS after performing an iDRAC factory reset operation, such as `racadm racresetcfg`. How do I troubleshoot the issue?

Ensure that the OS to iDRAC passthru channel is enabled. By default, it is disabled in factory mode. To enable the OS to IDRAC passthru channel on iDRAC, use the following command, `racadm set idrac.os-bmc.adminstate 1`.

I am seeing 169.254.0.2 as the source IP address in the iDRAC SNMP trap received via iSM. How do I troubleshoot the issue?

On Linux OS, the iDRAC SNMP traps received via Host OS displays the hostname or source IP address as 169.254.0.2 instead of the actual Host OS name or IP address. This is decided by the OS to populate the entry before rendering the trap to the user.

I have configured OS to iDRAC pass-through to LOM and when I try to run dcism-sync, the update operation fails. What can be done?

OS to iDRAC pass-through should be configured to USB-NIC mode. This is a pre-requisite for iDRAC Service Module installation and update.

When Hyper-V is enabled in the Host OS, iSM is unable to communicate with iDRAC. What should I do?

Enable the remote NDIS device under **Network Adapter**.

I am able to enable or disable the WMIInfo feature of iSM on Linux and VMware ESXi Operating Systems using racadm and WSMan commands. Does this impact my iSM configuration on the Host OS?

The WMIInfo feature of iSM is applicable only for Microsoft Windows Operating Systems. However, enabling or disabling this feature from any of the iDRAC interfaces on any Operating System other than Microsoft Windows does not impact the iSM configuration on the Host OS.

If I delete the IP address of the USBNIC interface on the Host OS, then iSM is unable to communicate with iDRAC.

Starting iSM version 3.3, iSM configures 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 configuration and does not override the interface settings. To restore the communication between iSM and iDRAC, please restart the iSM service on the Host OS.

After installing iSM using the Batch file **ISM_Win.BAT** from the iDRAC exposed logical partition "SMINST" on Microsoft

Windows OS, I see a console message saying "The system cannot find the file specified."

After iSM is installed successfully, the logical partition **SMINST** gets unmounted from the Host OS. This message appears if the BAT script is invoked from the **SMINST** partition itself. The installation is successful. No action is required by the user.

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
```

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

When I install iSM 3.4.0 or later on Linux operating systems such as Red Hat Enterprise Linux, I see some messages in OS logs such as *G_IS_SIMPLE_ACTION (simple)' failed: failed to rescan: Failed to parse /usr/share/applications/iDRACGUILauncher.desktop file: cannot process file of type application/x-desktop*.

The messages are related to the GNOME desktop manager. Various OS groups have Bugzilla items for this scenario to be addressed. For example: https://bugzilla.redhat.com/show_bug.cgi?id=1594177. No action is required by the user.

I see a blank terminal on RHEL 7.6 or RHEL 8.0 when I click on *iDRAC GUI Launcher* shortcut from **Menu** > **Accessories.**

The visibility of text on the terminal depends on GNOME version on the resident OS. An alternative is to run the launcher from a GUI-capable shell. For example: `bash#> sh /opt/dell/srvadmin/iSM/bin/iDRACLauncher.sh` as a sudo user.

In case, the OS-to-iDRAC Passthru is disabled in iDRAC, the user will see a blank terminal when iDRAC GUI is launched from the Linux OS such as RHEL 7.6 and RHEL 8.0. Select **y** or **Y**, and press **Enter** to indicate configuration of USBNIC interface on the Host OS.

Alternatively, you can enable the OS-to-iDRAC Passthru in iDRAC in USBNIC mode and re-run the iDRAC launcher from the Host OS.

7

Linux and Ubuntu installer packages

The installer packages for the supported Linux and Ubuntu OS are as follows:

Table 12. Linux installer packages

Supported Linux Operating System	Installer Packages
Red Hat Enterprise Linux 7	SYSMGMT\iSM\linux\RHEL7\x86_64\dcism-3.4.1-<bldno>.el7.x86_64.rpm
Red Hat Enterprise Linux 8	SYSMGMT\iSM\linux\RHEL8\x86_64\dcism-3.4.1-<bldno>.el8.x86_64.rpm
Ubuntu 18	SYSMGMT\iSM\linux\Ubuntu18\x86_64\dcism-3.4.1-<bldno>.ubuntu18.deb

NOTE: You can use any of the listed installer package to install iDRAC Service Module on CentOS.