Dell EMC iDRAC Service Module 3.6

Benutzerhandbuch

November 2021
Rev. A02

DELL Technologies

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

1

Einführung

Das iDRAC-Servicemodul (iSM) ist ein einfaches Softwaremodul, das Sie auf den PowerEdge-Servern yx2x oder höher installieren können. Das iSM ergänzt iDRAC-Schnittstellen – die Benutzeroberfläche (UI), RACADM CLI, Redfish und Web Services-Management (WS-Man) – mit zusätzlichen Überwachungsdaten. Sie können die iSM-Funktionen innerhalb des unterstützten Betriebssystems konfigurieren, je nach den von Ihnen installierten Funktionen und den einzigartigen Integrationsanforderungen Ihrer Umgebung.

Themen:

Neuerungen

Neue unterstützte Betriebssysteme

iDRAC-Servicemodul 3.6 unterstützt die folgenden Betriebssysteme:

- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP2
- Ubuntu Server 20.04 LTS
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

Neue und verbesserte Funktionen

Im Folgenden werden die neuen und verbesserten Funktionen des iDRAC-Servicemodul 3.6 beschrieben:

- Sicheres Laden von Bibliotheken, um ein Vorabladen auf Linux und VMware ESXi zu vermeiden.
- Überwachung der S.M.A.R.T.-Attribute von Chipsatz-SATA-Controller-Geräten im Software-RAID-Controller.
- Einbeziehung der S.M.A.R.T-Verlaufsprotokolldateien des Chipsatz SATAs in die SupportAssist-Erfassung.
- Automatischer Versand für Festplatten durch SupportAssist bei zwei Ereignissen für VMware ESXi:
  - Vorhersehbarer Fehler für physisches Laufwerk gemeldet.
  - Ein beschädigter Festplattenblock auf <Gerät> kann während eines Schreibvorgangs nicht neu zugewiesen werden.
- Verbesserte NVMe-Funktion zur Vorbereitung auf Entfernen im Linux-Betriebssystem: NVMe-Vorgang zur Vorbereitung auf Entfernen ist nicht zulässig, wenn ein NVMe-Laufwerk verwendet wird oder ein RAW-Lese- und Schreibvorgang auf dem NVMe-Laufwerk durchgeführt wird.
- Verbesserte Funktionen für iDRACHardReset und FullPowerCycle: Die Vorgänge für iDRACHardReset und FullPowerCycle werden unterstützt, wenn die Option für Secure Boot im BIOS aktiviert ist. Die mindestens erforderliche BIOS-Version ist 1.5.3 für yx5x PowerEdge-Server mit AMD-Prozessor.

Matrix der unterstützten Funktionen nach Betriebssystem

Die folgenden Funktionen werden auf yx2x-, yx3x, yx4x und yx5x PowerEdge-Servern unterstützt:

Tabelle 1. Von jedem Betriebssystem unterstützte Funktionen

Funktionen	Server	Betriebssysteme		
	Unterstützte PowerEdge-Versionen	Microsoft Windows (einschließlich der Hyper-V-Systeme)	Linux	Virtualisierung (VMware ESXi)
Freigabe von Betriebssysteminformationen	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Lifecycle-Controller-Protokollreplikation	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Automatische Systemwiederherstellung/Watchdog	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Windows Management Instrumentation-Provider	yx2x, yx3x, yx4x, yx5x	Ja	-	-
Vorbereitung zum Entfernen eines NVMe-Geräts über den iDRAC	yx3x, yx4x, yx5x	Ja	Ja	Ja
SupportAssist-Erfassung vom Hostbetriebssystem	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Betriebssystem- und Anwendungsdaten	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja (nur für PowerEdge-Server yx4x und neuer)
Remote-iDRAC-Kaltstart	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja (Befehlszeilendienstprogramm wird nur auf VMware ESXi 7.x unterstützt)
iDRAC-Zugriff über Host-BS	yx2x, yx3x, yx4x, yx5x	Ja	Ja	-
In-Band-Unterstützung für iDRAC SNMP-Warnmeldungen	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Unterstützung der Überwachung von Netzwerkschnittstellen über Redfish-Client	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
WS-Man remote aktivieren	yx2x, yx3x, yx4x, yx5x	Ja	-	-
FullPowerCycle	yx4x, yx5x	Ja	Ja	VMware ESXi 7.x: Ja
In-Band-SNMP-Get	yx2x, yx3x, yx4x, yx5x	Ja	Ja	-
Live-VIB-Installation	yx3x, yx4x, yx5x	-	-	Ja

Tabelle 1. Von jedem Betriebssystem unterstützte Funktionen (fortgesetzt)

Funktionen	Server	Betriebssysteme		
	Unterstützte PowerEdge-Versionen	Microsoft Windows (einschließlich der Hyper-V-Systeme)	Linux	Virtualisierung (VMware ESXi)
Anonymer SupportAssist-Erfassungsbericht	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
iDRAC-UI-Startprogramm	yx3x, yx4x, yx5x	Ja	Ja	-
IPv6-Unterstützung	yx3x, yx4x, yx5x	Ja	Ja	-
Automatischer Versand für selektive Ereignisse	yx4x, yx5x	Ja	Ja	Ja
SupportAssist-Erfassung mit selektiven PII	yx2x, yx3x, yx4x, yx5x	Ja	Ja	Ja
Single Sign-On (SSO)	yx4x, yx5x	Ja	Ja	-
Automatische Aktualisierung der iSM-Installation	yx4x, yx5x	Ja	Ja	-
Server-Storage-Korrelation (S2D)	yx3x, yx4x, yx5x	Ja	-	-
S.M.A.R.T-Monitoring im AHCI-Modus	yx3x, yx4x, yx5x	Ja	Ja	Ja
S.M.A.R.T-Monitoring im Software-RAID-Modus	yx3x, yx4x, yx5x	Ja	-	-

NV – nicht verfügbar

Unterstützte Plattformen auf iDRAC-Servicemodul

Die folgende Tabelle enthält eine Liste der unterstützten Plattformen auf dem iDRAC-Servicemodul.

Tabelle 2. Unterstützte Plattformen auf iDRAC-Servicemodul

yx5x PowerEdge-Server	yx4x PowerEdge-Server	yx3x PowerEdge-Server	yx2x PowerEdge-Server
R6515	XE7440	C4130	FM120
R7515	XE7420	C6320	M420
R6525	R240	FC 430	M520
C6525	R340	FC 630	M620
R7525	T140	FC 830	M820
	T340	M630	R220
	R740xd2	M630-VRTX	R320
	R840	M830	R420
	R940 xa	R230	R620
	MX740c	R330	R720

Tabelle 2. Unterstützte Plattformen auf iDRAC-Servicemodul (fortgesetzt)

yx5x PowerEdge-Server	yx4x PowerEdge-Server	yx3x PowerEdge-Server	yx2x PowerEdge-Server
	MX840c	R430	R720 XD
	R7425	R530	R820
	R7415	R630	R920
	R6415	R730	T320
	C6420	R730xd	T420
	FC 640	R830	T620
	M640	R930	
	M640-VRTX	T130	
	R440	T330	
	R540	T430	
	R640	T630	
	R740		
	R740xd		
	R940		
	T440		
	T640		

Koexistenz von OpenManage Server Administrator mit dem iDRAC Service Module

OpenManage Server Administrator (OMSA) und iDRAC-Servicemodul (iSM) können auf einem einzelnen System koexistieren. Wenn Sie die Monitoring-Funktionen während der iSM-Installation aktivieren und das iSM nach Abschluss der Installation erkennt, dass OMSA vorhanden ist, deaktiviert iSM die AutoSystemRecovery- und Lifecycle-Protokoll-Replikationsfunktionen, die sich überschneiden. Wenn der OMSA-Service angehalten wird, werden die deaktivierten iSM-Funktionen aktiviert.

ANMERKUNG: Die sich überschneidenden Funktionen sind **AutoSystemRecovery** und **Lifecycle-Protokoll-Replikation**.

Software-Verfügbarkeit

Die iDRAC Servicemodul-Software ist verfügbar auf:

- *Dell EMC OpenManage Systems Management Tools and Documentation* DVD
- Dell.com/support

Download von iSM

Anleitung zum Herunterladen des iSM:

1. Rufen Sie die Website Dell.com/support auf.
2. Klicken Sie auf der Support-Website auf **Alle Produkte Durchsuchen** > **Software** > **Enterprise Systemverwaltung** > **Remote Enterprise Systems Management** > **iDRAC Service Module** > **iDRAC Service Module - aktuelle Versionen** > **Treiber und Downloads**.

Zugriff auf Support-Inhalte von der Dell EMC Support-Website

Greifen Sie auf unterstützende Inhalte in Verbindung mit einer Reihe von Systemverwaltungstools über direkte Links zu, gehen Sie zur Dell EMC Support-Website oder verwenden Sie eine Suchmaschine.

- Direkte Links:
  - Für Dell EMC Enterprise Systems Management und Dell EMC Remote Enterprise Systems Management –https://www.dell.com/esmmanuals
  - Für Dell EMC Virtualization Solutions –https://www.dell.com/SoftwareManuals
  - Für Dell EMC OpenManage –https://www.dell.com/openmanagemanuals
  - For iDRAC –https://www.dell.com/idracmanuals
  - Für Dell EMC OpenManage Connections Enterprise Systems Management –https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Für Dell EMC Serviceability Tools –https://www.dell.com/serviceabilitytools
- Support-Site von Dell EMC:
  1. Navigieren Sie zu https://www.dell.com/support.
  2. Klicken Sie auf **Alle Produkte durchsuchen**.
  3. Klicken Sie auf der Seite **Alle Produkte** auf **Software** und klicken Sie dann auf den erforderlichen Link:
  4. Klicken Sie auf das gewünschte Produkt und anschließend auf die gewünschte Version.

Für Suchmaschinen: Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.

Weitere nützliche Dokumente

Sie können auf die folgenden Anleitungen unter dell.com/support zugreifen.

- Das *Benutzerhandbuch zum Integrated Dell Remote Access Controller (iDRAC)* enthält ausführliche Informationen zum Konfigurieren und Verwenden des iDRAC.
- Im *Benutzerhandbuch zum Dell Remote Access Controller RACADM* finden Sie Informationen zur Verwendung des Befehlszeilen-Dienstprogramms RACADM.
- Das *Benutzerhandbuch zu den Dell Update Packages* enthält Informationen über das Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Im *Dell Referenzhandbuch zu Ereignismeldungen* finden Sie Informationen zu den Ereignis- und Fehlermeldungen, die von der Firmware und anderen Agenten, die die Systemkomponenten überwachen, generiert werden.
- Im *Benutzerhandbuch zur Kommunikation zwischen Dell Lifecycle-Controller und Web Services-Schnittstelle* finden Sie Informationen und Beispiele für die Verwendung des WS-Man-Verwaltungsprotokolls (Web Services for Management).

Softwarelizenzvereinbarung

Die Softwarelizenz für die vom iSM unterstützten Betriebssystemversionen ist im Installationsprogramm enthalten. Lesen Sie die Datei `license_agreement.txt` . Durch Installieren oder Kopieren von einer der Dateien auf dem bereitgestellten Datenträger stimmen Sie den Bedingungen in der Datei `license_agreement.txt` zu.

2

Installationsvorbereitungen

Stellen Sie vor der Installation des iDRAC-Servicemoduls (iSM) Folgendes sicher:

- Es besteht Zugriff auf PowerEdge-Server yx2x oder höher. Eine Liste der unterstützten Plattformen finden Sie unter Unterstützte Plattformen.
- Sie verfügen über Administrator-Zugriffsrechte.
- Lesen Sie die Installationsanweisungen für Ihr Betriebssystem.
- Lesen Sie die jeweiligen Versionshinweise und die *Systems Software Support Matrix*.
- Lesen Sie die Informationen zu den Installationsvoraussetzungen, um sicherzustellen, dass Ihr System die Mindestanforderungen erfüllt oder überschreitet.
- Schließen Sie alle Anwendungen, die auf dem System ausgeführt werden, bevor Sie iSM-Anwendungen installieren.

Themen:

Voraussetzungen für die Installation

Eine Liste der Betriebssysteme, die auf iDRAC-Servicemodul (iSM) unterstützt werden, finden Sie unter Unterstützte Betriebssysteme.

Spezifische Voraussetzungen für ein Betriebssystem werden als Teil der Installationsvorgänge aufgeführt. Das iSM kann über die Benutzeroberfläche installiert werden. Das Installationsprogramm unterstützt außerdem die automatische Installation.

Unterstützte Betriebssysteme und Hypervisoren

Das iDRAC-Servicemodul wird auf den folgenden 64-Bit-Betriebssystemen unterstützt:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP2
- Ubuntu 20.04 LTS
- VMware vSphere (ESXi) 7.0 U1 unterstützt auf den PowerEdge-Servern yx3x*, yx4x und yx5x
- VMware vSphere (ESXi) 7.0 U2 unterstützt auf den PowerEdge-Servern yx3x*, yx4x und yx5x
- VMware vSphere (ESXi) 6.7 U3 unterstützt auf den PowerEdge-Servern yx3x, yx4x und yx5x

* Nur einige yx3x PowerEdge-Server unterstützen VMware ESXi 7.0 U1 und 7.0 U2. Eine Liste der unterstützten yx3x PowerEdge-Server finden Sie unter VMware vSphere 7.x auf Dell EMC PowerEdge-Servern – Kompatibilitätsmatrix.

Unterstützte Plattformen

iDRAC-Servicemodul 3.6 unterstützt die PowerEdge-Server yx2x, yx3x, yx4x und yx5x.

Unterstützte Plattformen auf Linux-Betriebssystemen

Die Tabelle enthält eine Liste der durch das iDRAC Servicemodul 3.6 unterstützten Plattformen auf Linux-Betriebssystemen.

Tabelle 3. Unterstützte Plattformen auf Linux-Betriebssystemen

Dell EMC Geräte	Ubuntu 20.04.	SUSE Linux Enterprise Server 15 SP2	Red Hat Enterprise Linux 8.3	Red Hat Enterprise Linux 7.9
yx5x PowerEdge-Server	Ja	Ja	Ja	Ja
yx4x PowerEdge-Server	Ja	Ja	Ja	Ja
yx3x PowerEdge-Server	Nein	Ja	Ja	Ja
yx2x PowerEdge-Server	Nein	Nein	Nein	Nein

ANMERKUNG: yx3x PowerEdge-Server: Eingeschränkte Unterstützung für das Betriebssystem Red Hat Enterprise Linux 8.0. Eine Liste der unterstützten Dell EMC Server finden Sie hier: https://linux.dell.com/files/supportmatrix/RHEL_Support_Matrix.pdf.

Unterstützte Plattformen auf Microsoft Windows-Betriebssystemen

Die Tabelle enthält eine Liste der durch das iDRAC-Servicemodul 3.6 unterstützten Plattformen auf Microsoft Windows-Betriebssystemen.

Tabelle 4. Unterstützte Plattformen auf Microsoft Windows-Betriebssystemen

Dell EMC Geräte	Microsoft Windows Server 2019	Microsoft Windows Server 2016
yx5x PowerEdge-Server	Ja	Ja
yx4x PowerEdge-Server	Ja	Ja
yx3x PowerEdge-Server	Ja	Ja
yx2x PowerEdge-Server	Nein	Ja

Unterstützte Plattformen auf Virtualisierungs-Hypervisor

Die Tabelle führt die von iSM 3.6 auf einem Virtualisierung-Betriebssystem unterstützten Plattformen auf.

Tabelle 5. Unterstützte Plattformen auf Virtualisierungs-Hypervisor

Dell EMC PowerEdge-Server	VMware ESXi	
	vSphere 7.0 U1 und 7.0 U2	vSphere 6.7 U3
yx5x PowerEdge-Server	Ja	Ja
yx4x PowerEdge-Server	Ja	Ja
yx3x PowerEdge-Server	Ja*	Ja
yx2x PowerEdge-Server	Nein	Nein

* Nur einige yx3x PowerEdge-Server unterstützen VMware ESXi 7.0 U1 und 7.0 U2. Eine Liste der unterstützten yx3x PowerEdge-Server finden Sie unter VMware vSphere 7.x auf Dell EMC PowerEdge Servern Kompatibilitätsmatrix.

Unterstützte Betriebssysteme auf dem Dell EMC Precision Rack System

Tabelle 6. Unterstützte Betriebssysteme auf dem Dell EMC Precision Rack System

Dell EMC Geräte	Microsoft Windows 10 RS5
R7920	Ja

Systemanforderungen

In der folgenden Tabelle werden die Systemanforderungen aufgelistet:

- Eines der unterstützten Betriebssysteme. Weitere Informationen zu den unterstützten Betriebssystemen finden Sie unter Unterstützte Betriebssysteme.
- Mindestens 2 GB RAM
- Mindestens 512 MB freien Festplattenspeicherplatz
- Administratorrechte
- Die RNDIS-Funktionalität (Remote Network Driver Interface Specification) für die Ermittlung eines Netzwerkgeräts über USB

3

Installieren des iDRAC Service Module

Das iDRAC-Servicemodul (iSM) lässt sich auf allen folgenden Betriebssystemen installieren:

- Microsoft Windows
- Linux
- VMware ESXi

Eine Liste der vom iSM unterstützten Betriebssystemen finden Sie unter Unterstützte Betriebssysteme.

Themen:

Erstinstallation des iDRAC-Servicemoduls über iDRAC Enterprise oder Datacenter oder iDRAC Express auf Microsoft Windows und Linux

Sie können das iDRAC-Servicemodul (iSM) über die Oberfläche von iDRAC Enterprise oder Datacenter oder iDRAC Express installieren. Das Installationsverfahren ist für die Installation von iSM über iDRAC oder iDRAC Express auf den Betriebssystemen Microsoft Windows und Linux gleich. Mit einem einfachen Klick über das iDRAC-Installationspaket auf dem Hostbetriebssystem. Wenn Sie diese Methode verwenden, anstatt das Installationsprogramm von der Dell EMC-Support-Website oder der OpenManage herunterzuladen DVD stellen Sie sicher, dass Sie eine Version von iSM installieren, die mit ihrer iDRAC Firmware kompatibel ist.

iSM muss auf dem Hostbetriebssystem installiert sein. Deshalb ist es zwingend erforderlich, dass ein Betriebssystem installiert ist und auf dem Hostgerät ausgeführt wird.

1. Starten Sie die virtuelle Konsole.
2. Melden Sie sich beim Hostbetriebssystem als Administrator an.
3. Wählen Sie in der Geräteliste das eingebundene Volume aus, das von SMINST identifiziert wird, und klicken Sie dann auf das entsprechende Skript, um die Installation zu starten. Um iSM zu installieren, führen Sie den entsprechenden Befehl für Ihr System aus:

   Für Windows: `ISM_Win.bat`

   Für Linux: `sh ISM_Lx.sh` oder `. ISM_Lx.sh`

   Für Ubuntu: `bash ism_Lx.sh`

   Nachdem die Installation abgeschlossen ist, zeigt iDRAC an, dass das iSM installiert ist, und gibt das neueste Installationsdatum an.

   ANMERKUNG: Das Installationsprogramm ist für 30 Minuten vom Hostbetriebssystem aus zugänglich, in diesem Zeitraum müssen Sie den Installationsvorgang starten. Andernfalls müssen Sie das iDRAC-Servicemodul-Installationsprogramm neu starten.

Installieren des iDRAC-Servicemoduls auf Microsoft Windows-Betriebssystemen

Das Installationsprogramm des iDRAC-Servicemoduls (iSM) für die unterstützten Betriebssysteme finden Sie auf der DVD „*System-Management-Tools und Dokumentation*“. Sie können das iSM-Installationsprogramm auch über dell.com/support herunterladen.

Sie können eine manuelle oder eine automatisierte Installation mithilfe der entsprechenden Befehlszeilenschalter durchführen. Sie können das iSM mithilfe von Konsolen wie OpenManage Essentials (OME) auch über den **push**-Mechanismus durchführen.

ANMERKUNG: Führen Sie die folgenden Schritte nur dann aus, wenn ein PowerShell-Modulpfad von Drittanbietern in Ihrer Betriebssystemumgebung fehlt:

1. Wechseln Sie zu **SYSMGMT** > **iSM** > **Windows** und führen Sie dann `iDRACSvcMod.msi` aus.
   Der **iDRAC-Service-Modul - InstallShield-Assistent** wird angezeigt.
2. Klicken Sie auf **Weiter**.
   Die **Lizenzvereinbarung** wird angezeigt.
3. Lesen Sie sich die Softwarelizenzvereinbarung durch, wählen Sie die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie aus den folgenden Optionen einen **Setup-Typ** aus und klicken Sie anschließend auf **Weiter**:
   - **Standard**: Alle Programmfunktionen werden installiert (erfordert am meisten Speicherplatz).
   - **Benutzerdefiniert**: Passen Sie die Installation an, indem Sie die zu installierenden Programmfunktionen zusammen mit dem Speicherort auswählen (empfohlen für fortgeschrittene Benutzer).

   ANMERKUNG: Die folgenden Schritte sind nur anwendbar, wenn Sie die Option **Benutzerdefiniert** im Fenster **Setup-Typ** auswählen:

   ANMERKUNG: Standardmäßig sind die Funktionen **In-Band-SNMP-Traps, iDRAC-Zugriff über Hostbetriebssystem, SNMP Get über Hostbetriebssystem, SNMP-Warnmeldungen über Hostbetriebssystem, WS-Man aktivieren** nicht aktiviert.

   a. Wählen Sie die Programmfunktionen aus, die Sie installieren möchten, und klicken Sie auf **Weiter**.
      Daraufhin wird das Fenster **Lifecycle-Controller-Protokoll-Replikation** angezeigt.
   b. Geben Sie den Speicherort an, an dem die Lifecycle-Controller-Protokolle repliziert werden sollen. Standardmäßig ist die Option **Standard (Windows-Protokolle/System)** ausgewählt und die Lifecycle-Controller-Protokolle werden in der Gruppe **System** im Ordner **Windows-Protokolle** in der **Ereignisanzeige** repliziert. Klicken Sie auf **Weiter**.

      ANMERKUNG: Sie können auch eine benutzerdefinierte Gruppe im Ordner **Anwendungs- und Dienstprotokoll** erstellen, indem Sie die Option **Benutzerdefiniert** im Fenster **Lifecycle-Controller-Protokoll-Replikation** auswählen.

   c. Wählen Sie den Authentifizierungsmodus, um WS-Man per Remote-Zugriff zu aktivieren und um ein selbstsigniertes Zertifikat zu wählen, falls das Authentifizierungszertifikat nicht gefunden wurde. Geben Sie eine WINRM-Portnummer ein, um die Kommunikation einzuleiten. Die Portnummer ist standardmäßig auf 5986 eingestellt.
5. Geben Sie für die Funktion **iDRAC-Zugriff über Hostbetriebssystem** eine eindeutige Portnummer zwischen 1024 und 65535 an.

   ANMERKUNG: Wenn die Portnummer nicht angegeben ist, wird 1266 standardmäßig zugewiesen. Wenn eine früher konfigurierte Portnummer verfügbar ist, wird dieser zugewiesen.

   Das Fenster **Zur Installation des Programms bereit** wird angezeigt.
6. Klicken Sie auf **Installieren**, um die Installation fortzusetzen.
   Klicken Sie auf **Zurück**, wenn Sie die Einstellungen vorher noch ändern möchten.

   Obwohl der iSM-Server installiert ist, wird die folgende Meldung in der Host-Protokolldatei angezeigt: **Die Kommunikation zwischen iDRAC-Servicemodul und iDRAC konnte nicht hergestellt werden. Weitere Informationen finden Sie in der aktuellen Installationsanleitung für das iDRAC-Servicemodul.** Weitere Informationen zur Fehlerbehebung finden Sie unter Häufig gestellte Fragen.

   Während der iSM-Installation wird manchmal eine Warnmeldung angezeigt: **Zeitüberschreitung durch das Objekt iDRAC-Servicemodul. Bitte überprüfen Sie, das der Dienst iDRAC-Servicemodul ordnungsgemäß gestartet wurde.** Diese Warnmeldung ist auf die Verzögerung bei der Aktivierung einer USB NIC und den Start des iSM-Diensts zurückzuführen. Es wird empfohlen, dass der Nutzer überprüft, dass der Status des iSM-Diensts nach Abschluss der Installation „abgeschlossen“ ist.

   Das iSM wurde erfolgreich installiert.
7. Klicken Sie auf **Fertigstellen**.
   Unter Microsoft Windows 2016 und Windows 2019 wird die iDRAC-USB-NIC-Gerätebeschreibung als **Remote-NDIS-kompatibles Gerät** angezeigt.

Automatische Installation des iDRAC-Servicemoduls auf Microsoft Windows

Sie können das iDRAC-Servicemodul (iSM) unter Verwendung der automatischen Installation ohne interaktive Konsole installieren.

- Geben Sie zur Installation des iDRAC-Servicemoduls unter Verwendung der automatischen Installation `msiexec /i iDRACSvcMod.msi /qn` in der Eingabeaufforderung ein.
- Um die Installationsprotokolldateien zu erzeugen, geben Sie Folgendes ein: `msiexec /i iDRACSvcMod.msi /L*V <logname with the path>`
- Geben Sie zur Replikation der Lifecycle-Controller-Protokolle in einer vorhandenen Gruppe oder einem benutzerdefinierten Ordner Folgendes ein: `msiexec /i iDRACSvcMod.msi CP_LCLOG_VIEW="<existing group name or custom folder name>"`
- Um diese Funktion mithilfe der automatischen Installation zu installieren, geben Sie Folgendes ein: `msiexec /i <location of the installer file>/iDRACSvcMod.msi /qn ADDLOCAL=<xxxx>`

  ANMERKUNG: <XXXX> kann eine beliebige Funktion sein, die in der folgenden Tabelle aufgeführt ist. Sie können mehr als eine Funktion installieren, fügen Sie dazu diese mit einem Komma getrennt an. Beispiel:

  ```
  msiexec /i <location of the installer file>/iDRACSvcMod.msi /qn ADDLOCAL=IBIA2,
  SupportAssist, SM
  ```

Parameter	Funktionen
OSInfo	Betriebssystem-Informationen
Watchdog	Automatische Systemwiederherstellung
LCLog	Lifecycle-Protokoll-Replikation
IBIA2	iDRAC-Zugriff über Host-BS
WMIPOP	WMI-Anbieter (Windows Management Instrumentation)
iDRACHardReset	Remote-iDRAC-Hardware-Reset
SupportAssist	SupportAssist
iDRAC_GUI_Launcher	iDRAC-UI-Startprogramm
FullPowerCycle	Vollständiges Aus- und Einschalten
SDSEventCorrelation	SDS-Ereigniskorrelation
SM	S.M.A.R.T.-Monitoring

- Geben Sie zur Installation von WS-Man Folgendes ein: `msiexec.exe /i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2" CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1" /qn`
- Geben Sie zur Anzeige der Benutzeroberfläche in den unterstützten Sprachen Folgendes ein: `msiexec /i iDRACSvcMod.msi TRANSFORMS= <locale number>.mst`. Die folgenden Gebietsschemanummern sind verfügbar:

Tabelle 7. Gebietsschemanummern und die unterstützten Sprachen

Gebietsschemanummer	Sprache
1031	Deutsch
1033	Englisch (US)
1034	Spanisch
1036	Französisch
1041	Japanisch
2052	Chinesisch (vereinfacht)

Ändern des iDRAC-Servicemoduls auf Microsoft Windows-Betriebssystemen

So ändern Sie iSM-Komponenten (iDRAC-Servicemodul):

1. Wechseln Sie zu **SYSMGMT** > **iSM** > **Windows** und führen Sie `iDRACSvcMod.msi` aus.
   Der **iDRAC-Service-Modul - InstallShield-Assistent** wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie **Ändern** aus.
4. Aktivieren oder deaktivieren Sie die Funktionen nach Bedarf und klicken Sie dann auf **Weiter**.
   Daraufhin wird das Fenster **Lifecycle-Controller-Protokoll-Replikation** angezeigt.
5. Geben Sie den Speicherort an, an dem die LC-Protokolldateien repliziert werden sollen. Standardmäßig ist die Option **Standard (Windows-Protokolle/System)** ausgewählt und die LC-Protokolle werden in der Gruppe **System** im Ordner **Windows-Protokolle** in der **Ereignisanzeige** repliziert.
6. Klicken Sie auf **Weiter**.

   ANMERKUNG: Sie können auch eine benutzerdefinierte Gruppe im Ordner **Anwendungs- und Dienstprotokoll** erstellen, indem Sie die Option **Benutzerdefiniert** im Fenster **Lifecycle-Controller-Protokoll-Replikation** auswählen.

   ANMERKUNG: Starten Sie gegebenenfalls das System in den folgenden Szenarien neu:
   - wenn Sie zwischen den Optionen **Standard (Windows-Protokolle/System)** und **Benutzerdefiniert** hin- und herschalten.
   - wenn Sie von einem benutzerdefinierten Ordner in einen anderen Ordner wechseln.

   Der Bildschirm **Bereit zur Programminstallation** wird angezeigt.
7. Geben Sie für iDRAC-Zugriff über die Hostbetriebssystem-Funktion eine eindeutige Portnummer zwischen 1024 und 65535 an.

   ANMERKUNG: Wenn die Portnummer nicht angegeben ist, wird 1266 standardmäßig zugewiesen. Wenn ein früher konfigurierter Port verfügbar ist, wird dieser zugewiesen.
8. Klicken Sie auf **Installieren**, um den Vorgang fortzusetzen.
   Klicken Sie auf **Zurück**, wenn Sie die Einstellungen ändern möchten.
   Das iDRAC-Servicemodul wurde erfolgreich geändert.
9. Klicken Sie auf **Fertigstellen**.

Reparieren des iDRAC-Servicemoduls auf Microsoft Windows-Betriebssystemen

Gehen Sie folgendermaßen vor, um eine fehlerhafte oder ausgefallene iSM-Komponente (iDRAC-Servicemodul) zu reparieren:

1. Wechseln Sie zu **SYSMGMT** > **iSM** > **Windows** und führen Sie `iDRACSvcMod.msi` aus.
   Der Bildschirm **iDRAC-Servicemodul – InstallShield-Assistent** wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie **Reparatur** aus und klicken Sie auf **Weiter**.
   Das Fenster **Bereit zur Programminstallation** wird angezeigt.
4. Klicken Sie auf **Reparieren**, um den Vorgang fortzusetzen.
   Klicken Sie auf **Zurück**, wenn Sie die Einstellungen ändern möchten.
   Die iDRAC-Servicemodulkomponente wurde erfolgreich repariert.
5. Klicken Sie auf **Fertigstellen**.

Deinstallieren des iDRAC-Servicemoduls unter Microsoft Windows-Betriebssystemen

Das iDRAC-Servicemodul (iSM) kann mithilfe von zwei verschiedenen Methoden deinstalliert werden:

- Unbeaufsichtigte Deinstallation mithilfe der Product ID
- Deinstallieren über die Funktion „Hinzufügen/Entfernen“

Unbeaufsichtigte Deinstallation des iDRAC-Servicemoduls mithilfe der Produkt-ID

Geben Sie den Befehl `msiexec /x {0B2D9B70-DD98-4E31-8A85-228AB0636C94} /qn` ein, um das iDRAC-Servicemodul über die Produkt-ID zu deinstallieren.

Deinstallieren des iDRAC-Servicemoduls über die Funktion zum Hinzufügen oder Entfernen

Um iSM über die Option „Hinzufügen oder Entfernen“ im Bedienfeld zu deinstallieren, gehen Sie zu **Start** > **Systemsteuerung** > **Programme und Funktionen**.

ANMERKUNG: Sie können die Deinstallation auch vornehmen, indem Sie nach dem Ausführen des Befehls `iDRACSvcMod.msi` **Deinstallieren** auswählen.

ANMERKUNG: Sie können die iSM-Protokolldateien in der Gruppe **Anwendung** des Ordners **Windows-Protokolle** in der Windows-**Ereignisanzeige** anzeigen.

Installieren des iDRAC-Servicemoduls auf VMware ESXi

VMware ESXi ist auf einigen Systemen werkseitig installiert. Eine Liste dieser Systeme finden Sie in der neuesten *Systems Software Support Matrix* unter **dell.com/support/manuals**.

iSM ist als Zip-Datei verfügbar und kann auf Systemen installiert werden, die VMware ESXi ausführen. Die Zip-Datei folgt der Namenskonvention **iSM-Dell-Web-3.6.0-<bldno>.VIB-<Version>i-Live.zip**, wobei <Version> die unterstütze ESXi-Version ist.

Folgende Zip-Dateien sind für die unterstützten ESXi-Versionen verfügbar:

- Für VMware ESXi 7.x: `ISM-Dell-Web-3.6.0-<bldno>.VIB-ESX7i-Live.zip`
- Für VMware ESXi 6.x: `ISM-Dell-Web-3.6.0-<bldno>.VIB-ESX6i-Live.zip`

Wenn VMware ESXi nicht auf Ihrem System installiert ist, befolgen Sie diese Schritte zum Installieren des iSM auf VMware ESXi:

1. Kopieren Sie die Zip-Datei des iSM-Offline Bundle an den Speicherort `/var/log/vmware` auf dem Hostbetriebssystem.
2. Führen Sie den folgenden Befehl aus:
   - Für VMware ESXi 7.x: `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`
   - Für VMware ESXi 6.x: `esxcli software vib install -d /var/log/vmware/<iDRAC Service Module file>`

Gehen Sie wie folgt vor, um ein Upgrade von ISM auf VMware ESXi durchzuführen:

1. Kopieren Sie die Zip-Datei des iSM-Offline Bundle an den Speicherort `/var/log/vmware` auf dem Hostbetriebssystem.
2. Führen Sie den folgenden Befehl aus:
   - Für VMware ESXi 7.x: `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`
   - Für VMware ESXi 6.x: `esxcli software vib update -d /var/log/vmware/<iDRAC Service Module file>`

ANMERKUNG: Die Funktionskonfiguration des iDRAC-Servicemoduls bleibt nach einem erzwungenen oder sofortigen Neustart nicht erhalten. Eine Sicherung der Konfigurationsdateien wird durch den ESXi-Hypervisor über das Skript `script /sbin/auto-backup.sh` erstellt, das in regelmäßigen Abständen alle 60 Minuten ausgeführt wird. Wenn Sie die Konfiguration beibehalten möchten, führen Sie manuell das Skript backup.sh aus, bevor Sie das System neu starten.

ANMERKUNG: Nach der Installation/Deinstallation des iDRAC Servicemodul Live-VIB-Pakets ist kein Neustart des Hostbetriebssystems erforderlich.

ANMERKUNG: Bei Repository-basierten Installationen wie VMware Update Manager (VUM) und apt-repository sind standardmäßig nicht alle Funktionen aktiviert.

Laden Sie die VMware vSphere-Befehlszeilenschnittstelle (vSphere CLI) von **http://vmwaredepot.dell.com/** herunter und installieren Sie sie auf Ihrem Microsoft Windows- oder Linux-System.

vSphere-CLI verwenden

So installieren Sie die iSM-Software unter Verwendung der vSphere CLI auf VMware ESXi:

1. Kopieren Sie die Datei `ISM-Dell-Web-3.6.0-<bldno>.VIB-<version>i-Live.zip` in ein Verzeichnis auf dem System.
2. Fahren Sie sämtliche Gast-Betriebssysteme auf dem ESXi-Host herunter und setzen Sie den ESXi-Host in den Wartungsmodus.
3. Wenn Sie die vSphere-CLI unter Windows verwenden, wechseln Sie zu dem Verzeichnis, in dem Sie die vSphere CLI-Dienstprogramme installiert haben. Wenn Sie vSphere CLI unter Linux verwenden, führen Sie den Befehl von einem beliebigen Verzeichnis aus.

   Für VMware ESXi 7.x:

   ```
   esxcli --server <IP Address of ESXi 7.x host> software component apply -d /var/log/vmware/
   <iDRAC Service Module file>
   ```

   Für VMware ESXi 6.x:

   ```
   esxcli --server <IP Address of ESXi 6.x host> software vib install -d /var/log/vmware/
   <iDRAC Service Module file>
   ```

   ANMERKUNG: Die PL-Erweiterung ist nicht erforderlich, wenn Sie vSphere CLI unter Linux verwenden.

4. Geben Sie den Stammbenutzernamen und das Kennwort des ESXi-Hosts ein, wenn Sie dazu aufgefordert werden.
   Die Befehlsausgabe zeigt eine erfolgreiche oder eine fehlgeschlagene Aktualisierung an.

So installieren Sie das iDRAC-Servicemodul mithilfe von VMware Update Manager (VUM):

So installieren Sie iSM unter Verwendung von VMware Update Manager (VUM):

1. Installieren Sie VMware vSphere ab Version 6.5 – vCenter Server, vSphere Client und VMware vSphere Update Manager – auf einem unterstützten Microsoft Windows-Betriebssystem.
2. Bei einem Desktop doppelklicken Sie auf **VMware vSphere Client** und melden Sie sich bei vCenter Server an.
3. Klicken Sie mit der rechten Maustaste auf **vSphere Client-Host** und klicken Sie dann auf **Neues Datenzentrum**.
4. Klicken Sie mit der rechten Maustaste auf **Neues Datencenter** und klicken Sie auf **Host hinzufügen**. Geben Sie Informationen für den ESXi Server wie angefordert an.
5. Klicken Sie mit der rechten Maustaste auf den gerade hinzugefügten ESXi-Host und klicken Sie auf **Wartungsmodus**.
6. Wählen Sie unter **Plug-ins** die Option **Plug-Ins verwalten** > **VMware Update Manager herunterladen**. Der Status wird aktiviert, wenn der Download erfolgreich ist. Befolgen Sie die Anweisungen zum Installieren des VUM-Clients.
7. Wählen Sie den **ESXi-Host** aus. Klicken Sie auf **Update Manager Admin-AnsichtPatch-RepositoryPatches importieren** und folgen Sie den Online-Anweisungen für ein erfolgreiches Hochladen des Patches.
   Das Offline-Bundle wird angezeigt.
8. Klicken Sie auf **Baselines und Gruppen**.
9. Klicken Sie auf die Registerkarte **Aus Baselines erstellen**, geben Sie den Baseline-Namen ein, wählen Sie **Hosterweiterung** als Baseline-Typ aus, und geben Sie die erforderlichen Informationen ein.
10. Klicken Sie auf **Admin Ansicht**.
11. Klicken Sie auf **Zur Baseline hinzufügen** für den Namen des hochgeladenen Patch und wählen Sie den in Schritt 8 erstellten Baselinenamen.
12. Klicken Sie auf **Kompatibilitätsansicht**.
13. Wählen Sie das Register **Update Manager**.
14. Klicken Sie auf **Anfügen**, wählen Sie die in Schritt 8 erstellte **Erweiterungsbaseline** und folgen Sie den Anweisungen.
15. Klicken Sie auf **Scannen** und wählen Sie **Patches und Erweiterungen** falls nicht standardmäßig gewählt, und klicken Sie auf **Scannen**.
16. Klicken Sie auf **Bereitstellen**, wählen Sie die erstellte **Hosterweiterung** aus und folgen Sie den Anweisungen.
17. Klicken Sie auf **Standardisieren** and folgen Sie nach Abschluss des Bereitstellens den Anweisungen.
    Die iSM-Installation ist abgeschlossen.

    ANMERKUNG: Weitere Informationen zum VMWare Update Manager finden Sie auf der offiziellen VMWare-Website.

ANMERKUNG: Sie können iSM aus dem VUM-Repository unter **https://vmwaredepot.dell.com/** installieren.

Aktualisieren des iDRAC-Servicemoduls auf VMware ESXi

So installieren Sie das iDRAC-Servicemodul mithilfe von VMware Update Manager (VUM):

1. Installieren Sie VMware vSphere ab Version 6.5 (vCenter Server, vSphere Client und VMware vSphere Update Manager) auf einem unterstützten Microsoft Windows-Betriebssystem.
2. Bei einem Desktop doppelklicken Sie auf **VMware vSphere Client** und melden Sie sich bei vCenter Server an.
3. Klicken Sie mit der rechten Maustaste auf **vSphere Client-Host** und klicken Sie dann auf **Neues Datenzentrum**.
4. Klicken Sie mit der rechten Maustaste auf **Neues Datencenter** und klicken Sie auf **Host hinzufügen**. Machen Sie Angaben zum ESXi-Server gemäß den Online-Anweisungen.
5. Klicken Sie mit der rechten Maustaste auf den in **Schritt 4** hinzugefügten **ESXi-Host** und klicken Sie auf **Wartungsmodus**.
6. Wählen Sie unter **Plug-ins** die Option **Plug-Ins verwalten** > **VMware Update Manager herunterladen**. (Dieser Status wird nach erfolgreichem Download aktiviert) Folgen Sie dann den Anweisungen für die Installation des VUM-Clients.
7. Wählen Sie den ESXi-Host aus. Klicken Sie auf **Update Manager** > **Admin-Ansicht** > **Patch-Repository** > **Patches importieren** und folgen Sie den Online-Anweisungen für ein erfolgreiches Hochladen des Patches.

   Das Offline-Bundle wird angezeigt.
8. Klicken Sie auf **Baselines und Gruppen**.
9. Klicken Sie auf **erstellen** im Register "Baselines", geben Sie den Baseline-Namen an, und wählen Sie als Baseline-Typ **Host-Erweiterung** aus.

   ANMERKUNG: Wählen Sie die neueste Version des iDRAC- Service-Moduls zum Erstellen der Baseline.

   Folgen Sie den restlichen Anweisungen.
10. Klicken Sie auf **Admin Ansicht**.
11. Klicken Sie auf **Zur Baseline hinzufügen** (gegen den heruntergeladenen Patchnamen) und wählen Sie den in Schritt 8 erstellten Baselinenamen.
12. Klicken Sie auf **Kompatibilitätsansicht**. Wählen Sie das Register **Update Manager**. Klicken Sie auf **Anfügen**, wählen Sie die in Schritt 8 erstellte **Erweiterungsbaseline** und folgen Sie den Anweisungen.
13. Klicken Sie auf **Scannen**, und wählen Sie **Patches und Erweiterungen** aus (falls nicht standardmäßig markiert), und klicken Sie auf **Scannen**.
14. Klicken Sie auf **Bereitstellen**, wählen Sie die erstellte **Host-Erweiterung** aus, und folgen Sie den Anweisungen.
15. Klicken Sie auf **Standardisieren** and folgen Sie nach Abschluss des Bereitstellens den Anweisungen.

    Die Installation des iDRAC-Servicemoduls ist abgeschlossen

    ANMERKUNG: Das Hostbetriebssystem wird neu gestartet, während Sie ein Upgrade von iSM über VMware Update Manager durchführen.

    ANMERKUNG: Weitere Informationen zum VMWare Update Manager finden Sie auf der offiziellen VMWare-Website.

    ANMERKUNG: Sie können das iDRAC-Servicemodul über das VUM-Repository **https://vmwaredepot.dell.com/** installieren.

Installieren von iDRAC Servicemodule unter Verwendung von vSphere Lifecycle Manager in vSphere Client

ANMERKUNG: Stellen Sie vor der Installation sicher, dass die heruntergeladene iSM-Version mit VMware ESXi 7.x kompatibel ist.

Gehen Sie wie folgt vor, um iSM unter Verwendung von vSphere Lifecycle Manager (vLCM) in vSphere Client (VC) zu installieren:

1. Installieren Sie den vSphere Client (VCSA) über einem unterstützten Microsoft Windows-Betriebssystem.
2. Melden Sie sich über das Internet bei einem vSphere Client an.
3. Klicken Sie mit der rechten Maustaste auf **vSphere Client-Host** und klicken Sie dann auf **Neues Datenzentrum**.
4. Klicken Sie mit der rechten Maustaste auf **Neues Datencenter** und klicken Sie auf **Host hinzufügen**. Machen Sie Angaben zum ESXi-Server gemäß den Online-Anweisungen.
5. Klicken Sie auf **Menü** > **Lifecycle Manager** > **Einstellungen** > **Patch-Setup** > **NEU** und aktivieren Sie das Online-Repository.
6. Klicken Sie auf **Aktionen** > **Updates synchronisieren**.

iSM VIB wird in VC heruntergeladen.

7. Wählen Sie den ESXi-Host aus. Klicken Sie auf **Baselines** > **Angebrachte Baselines** > **Anbringen** > **Erstellen** > **Baseline anbringen** und befolgen Sie die Onlineanweisungen zum Hochladen des Patch.
8. Klicken Sie auf **Staging** und folgen Sie den Anweisungen.
9. Nachdem der Staging-Vorgang abgeschlossen ist, klicken Sie auf **Korrigieren** und befolgen Sie die Anweisungen.

   Die iSM-Installation ist abgeschlossen.

Verwenden von Power CLI

So installieren Sie das iSM mithilfe der Power-CLI:

1. Installieren Sie die unterstützte PowerCLI von ESXi auf einem unterstützten Microsoft Windows-Betriebssystem.
2. Kopieren Sie die Datei `ISM-Dell-Web-3.6.0-<bldno>.VIB-<version>i-Live.zip` auf den ESXi-Host.
3. Wechseln Sie zum bin-Verzeichnis.
4. Starten Sie VI-Server verbinden. Geben Sie den Server und weitere Anmeldeinformationen an.
5. Melden Sie sich beim ESXi-Host an, indem Sie die unterstützte vSphere-CLI von ESXi 6.x U3 oder ESXi 7.x verwenden und erstellen Sie einen Datenspeicher.
6. Erstellen Sie den Ordner **iSM-Dell-Web-3.6.0-<bldno>.VIB-<Version>I** auf dem ESXi 6.x U3- oder ESXi 7.x-Host im Verzeichnis **/vmfs/volumes/<Datenspeichername>**.
7. Kopieren Sie die ESXi-Zip-Datei auf dem ESXi 6.x U3- oder ESXi 7.x-Host in das Verzeichnis **/vmfs/volumes/<Datenspeichername>iSM-Dell-Web-3.6.0-<bldno>.VIB-<Version>I**.
8. Entpacken Sie die Zip-Datei in dem oben genannten Verzeichnis.
9. Führen Sie folgenden Befehl in der Power-CLI aus:

   Fü ESXi 7.x:

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-3.6.0-<bldno>.VIB-<version>i/metadata.zip
   ```

   Fü ESXi 6.x:

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-3.6.0-<bldno>.VIB-<version>i/metadata.zip
   ```

10. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der iSM erfolgreich auf dem Host installiert wurde:

    Für ESXi 7.x: `esxcli software component list|grep DEL-dcism`.

    Fü ESXi 6.x: `esxcli software vib list|grep -i dcism`.

    iSM wird angezeigt.
11. Starten Sie das Hostbetriebssystem, nachdem iSM mit dem oben genannten Power CLI-Befehl installiert wurde.

    Weitere Informationen zu Power CLI finden Sie auf der VMware-Website.

Deinstallieren des iDRAC-Servicemoduls auf VMware ESXi

Um iSM auf VMware ESXi zu deinstallieren, verwenden Sie den folgenden Befehl:

- Für VMware ESXi 7.x: `esxcli software component remove -n DEL-dcism`
- Für VMware ESXi 6.x: `esxcli software vib remove -n dcism`

Installieren des iDRAC-Servicemoduls auf unterstützten Linux-Betriebssystemen

Das komplette iSM ist in einem einzigen Red Hat Package Manager (rpm) zusammengefasst. Mithilfe dieses Pakets, zu dem auch ein Shell-Skript gehört, können Sie die verfügbaren Funktionen installieren, deinstallieren oder aktivieren und deaktivieren.

Bevor Sie iSM installieren, müssen Sie die OSC-Paketerfassung über `rpm -ivh dcism-osc*.rpm` installieren.

Da das Installationsprogramm auf Linux eine einzige rpm-Installation beinhaltet, können Einzelinstallationen nicht unterstützt werden. Sie können die Funktionen nur über die skriptbasierte Installation aktivieren oder deaktivieren.

ANMERKUNG: Das Installationsprogramm ist für alle von iSM unterstützten 64-Bit-Versionen von Linux-Betriebssystemen verfügbar.

Installationsvoraussetzungen für Linux-Betriebssysteme

Zur Installation von iSM auf Systemen, auf denen ein unterstütztes Linux-Betriebssystem ausgeführt wird, führen Sie `setup.sh` aus.

Stellen Sie sicher, dass die grundlegenden Funktionsvoraussetzungen erfüllt sind, wie z. B.:

- **Betriebssystem-auf-iDRAC-Passthrough** wird nach dem Installieren des iSM automatisch aktiviert.
- Der IPv4-Netzwerkstapel auf dem Hostbetriebssystem ist aktiviert.
- Das USB-Subsystem ist aktiviert.
- `udev` ist aktiviert. Dies ist zum automatischen Starten von iSM erforderlich.

Weitere Informationen zu iDRAC finden Sie im aktuellen *Benutzerhandbuch zum Integrated Dell Remote Access Controller* unter **Dell.com/support/home**.

Linux-Abhängigkeiten

Im Folgenden finden Sie eine Liste der abhängigen Pakete und ausführbaren Dateien, die ebenfalls installiert werden müssen, um die Installation abzuschließen.

Tabelle 8. Linux-Abhängigkeiten

Ausführbare Befehle	Paketname
/sys	fileSystem
grep	grep
cut, cat, echo, pwd	coreutils
lsusb	usbutils
find	findutils
Shell-Skriptbefehle	bash
ifconfig	net-tools
ping	lputils
chkconfig	Red Hat Enterprise Linux • chkconfig SUSE Linux Enterprise Server • aaa_base
install_initd	Red Hat Enterprise Linux • redhat-lsb-core SUSE Linux Enterprise Server • insserv
systemctl	systemd
curl	libcurl
openssl	libssl

Installieren des iDRAC-Servicemoduls auf Linux-Betriebssystemen

1. Die verfügbaren Funktionen, die installiert werden können, werden auf dem Bildschirm angezeigt:
   - [1] Watchdog-Instrumentation Service
   - [2] LifeCycle-Protokollinformationen
   - [3] Betriebssysteminformationen
   - [4] iDRAC-Zugriff über Host-BS
     - [a] Zugriff über GUI, WS-man, Redfish, Remote RACADM
     - [b] In-Band-SNMP-Traps
     - [c] Zugriff über SNMP-Get
   - [5] iDRAC SSO Launcher
     - [a] Schreibgeschützt
     - [b] Administrator
   - [6] Chipsatz-S.M.A.R.T.-Monitoring
   - ○ [a] periodische S.M.A.R.T-Protokollerfassung
   - [7] iDRAC-Kaltstart
   - [8] SupportAssist
   - [9] Vollständiges Aus- und Einschalten
   - [10] Alle Funktionen
2. Um eine bestimmte Funktion zu installieren, geben Sie die jeweilige Nummer ein. Trennen Sie die Nummern der zu installierenden Funktionen durch ein Komma. Um beispielsweise die Unterfunktionen zu installieren, geben Sie **4.a, 4.b oder 4.c** ein.
3. Geben Sie zur Installation der ausgewählten Funktionen **I** ein. Wenn Sie nicht mit der Installation fortfahren möchten, geben Sie **q** (für quit/beenden) ein.

   ANMERKUNG: Nach der Installation verschiedener Funktionen können Sie diese entsprechend ändern.

   Führen Sie auf Linux-Betriebssystemen, die systemd unterstützen, den folgenden Befehl aus: `systemctl status dcismeng.service`.

   Um zu überprüfen, ob iSM auf dem Linux-Betriebssystem installiert ist, führen Sie den Befehl `/etc/init.d/dcismeng status` aus. Wenn iSM installiert ist und ausgeführt wird, wird der Status **wird ausgeführt** angezeigt.

   Sie müssen eine eindeutige Portnummer im Bereich zwischen 1024 und 65535 angeben, wenn Sie sich dafür entscheiden, die Funktion „iDRAC-Zugriff über Host-BS“ zu installieren. Wenn Sie keine Portnummer eingeben, wird standardmäßig die *Portnummer 1266* oder ein zuvor konfigurierter Port (falls vorhanden) zugewiesen. Wenn OpenManage Server Administrator bereits auf Port 1311 installiert ist, kann derselbe Port nicht für iSM verwendet werden.

   Wenn iSM 3.4.0 oder höher auf Linux-Betriebssystemen installiert ist, wird eine Warnung von GNOME mit dem Wortlaut *"Erneutes Scannen nicht möglich: Die Datei /usr/share/applications/iDRACGUILauncher.desktop konnte nicht analysiert werden: Dateien des Typs application/x-desktop" können nicht verarbeitet werden* oder ähnlich angezeigt.

Automatische Installation des iDRAC-Servicemoduls auf Linux

Sie können iSM ohne Nutzerkonsole im Hintergrund installieren. Verwenden Sie dazu den Befehl `setup.sh` mit Parametern.

Folgende Parameter können zusammen mit dem Befehl `setup.sh` verwendet werden:

Tabelle 9. Parameter für die automatische Installation

Parameter	Beschreibung
-h	Hilfe: zeigt die Hilfe an
-i	Installieren: Installiert und aktiviert die ausgewählten Funktionen
-x	Express: Installiert und aktiviert alle verfügbaren Funktionen
-d	Löschen: Deinstallation von iSM
-w	Watchdog: Aktiviert den Watchdog Instrumentation Service
-i	Lifecycle-Controller-Protokoll: aktiviert Lifecycle-Protokollinformationen
-o	Betriebssysteminformationen: aktiviert die Betriebssysteminformationen

Tabelle 9. Parameter für die automatische Installation (fortgesetzt)

Parameter	Beschreibung
-a	Autostart: startet den Service nach der Installation der iSM-Komponente
-O	iDRAC-Zugriff über das Hostbetriebssystem: ermöglicht dem iDRAC-Zugriff auf Benutzeroberfläche, WS-Man, Redfish, Remote-RACADM
-s	Aktiviert In-Band-SNMP-Traps
-g	Ermöglicht den Zugriff über SNMP-Get
-Sr	Aktiviert iDRAC SSO-Anmeldung als Nutzer mit Nur-Lesen-Berechtigung
-Sa	Aktiviert die iDRAC SSO-Anmeldung als Administrator
-Sm	Aktiviert das Chipsatz-S.M.A.R.T-Monitoring
-Sp	Ermöglicht die periodische Erfassung von S.M.A.R.T-Protokollen

ANMERKUNG: Wenn auf Linux-Betriebssystemen ein funktionsändernder Vorgang mit Hintergrundoption vom Linux-Webpaket über setup.sh aktiviert wird, dann werden die zuvor aktivierten Funktionsstatusarten von den neuen, während des Änderungsvorgangs ausgewählten Funktionen überschrieben.

Deinstallieren des iDRAC-Servicemoduls auf einem Linux-Betriebssystem

Das iSM kann mithilfe einer von zwei verschiedenen Methoden deinstalliert werden:

- Verwendung des Deinstallationsskripts
- Verwendung des RPM-Befehls

Deinstallieren des iDRAC-Servicemoduls über das Deinstallationsskript

Der Befehl, der für die Deinstallation des iSM verwendet wird, ist `dcism-setup.sh`. Führen Sie den Shell-Befehl aus und wählen Sie *d* aus, um das iSM zu deinstallieren.

Um das iSM im unbeaufsichtigten Modus zu deinstallieren, führen Sie `./setup.sh -d` aus.

Deinstallieren des iDRAC-Servicemoduls über den RPM-Befehl

iSM kann über den RPM-Befehl `rpm -e dcism` aus der Befehlszeile heraus deinstalliert werden.

ANMERKUNG: Bei der Deinstallation von iSM 3.5 mit dem Befehl `rpm -e dcism` wird das von iSM installierte OSC-Paket nicht deinstalliert. Sie können das OSC-Paket mithilfe des Befehls `rpm -e dcism-osc` deinstallieren.

Deinstallieren des iDRAC-Servicemoduls über den dpkg-Befehl

Im Ubuntu-Betriebssystem kann iSM mithilfe des dpkg-Befehls `dpkg --remove dcism` aus der Befehlszeile heraus deinstalliert werden.

Sie können das OSC-Paket mithilfe des Befehls `dpkg --purge dcism-osc` deinstallieren.

Installieren des iDRAC-Servicemoduls bei aktiviertem Sperrmodus der Systemkonfiguration im iDRAC

Wenn der Sperrmodus der Systemkonfiguration über iDRAC aktiviert ist, können keine Konfigurationsvorgänge für das iDRAC-Servicemodul durchgeführt werden. Alle Funktionen, die aktiviert wurden, bevor der Sperrmodus der Systemkonfiguration eingeschaltet wurde, bleiben weiterhin aktiviert. Wenn iSM installiert wird, nachdem der Sperrmodus der Systemkonfiguration aktiviert wurde, stehen

nur die iSM-Funktionen, die davor aktiviert wurden, den Nutzern zur Verfügung. Wenn der Sperrmodus der Systemkonfiguration in iDRAC ausgeschaltet wird, können alle Konfigurationsvorgänge durchgeführt werden.

Unterstützung für iDRAC URI zum Abrufen des Installationsprogramms für iDRAC-Servicemodul

Sie können iSM-Webpakete über die folgende URL herunterladen: **https://<iDRACIP>/software/ism/package.xml**. Sie können die Pakete herunterladen nur wenn iSM LC-DUP hochgeladen wird und mit den iDRAC. Das Laden in iDRAC kann auch durch Aktivieren der automatischen iDRAC-LC-Aktualisierung erfolgen.

Nachfolgend finden Sie Beispiel-XML-Code mit einem angegebenen Image-Dateinamen zum Herunterladen des Pakets.

```
<PayloadConfiguration>
<Image filename="OM-iSM-Dell-Web-LX-3.6.0.tar.gz" id="5DD5A8BA-1958-4673-BE77-40B69680AF5D"
skip="false" type="APAC" version="3.6.0"/>
<Image filename="OM-iSM-Dell-Web-LX-3.6.0.tar.gz.sign" id="E166C545-82A9-4D5D-8493-
B834850F9C7A" skip="false" type="APAC" version="3.6.0"/>
<Image filename="OM-iSM-Dell-Web-X64-3.6.0.exe" id="5015744F-F938-40A8-B695-5456E9055504"
skip="false" type="APAC" version="3.6.0"/>
<Image filename="ISM-Dell-Web-3.6.0-VIB-ESX6i-Live.zip" id="1F3A165D-7380-4691-
A182-9D9EE0D55233" skip="false" type="APAC" version="3.6.0"/>
<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>
```

Zum Herunterladen der Pakete hängen Sie den vorhandenen Image-Dateinamen aus der XML-Datei an die URL an. Beispiel:

- Microsoft Windows Webpakete können hier heruntergeladen werden: **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-X64–3.6.0.exe**.

Das VMware ESXi Live-VIB-Paket vom Lifecycle Controller kann hier heruntergeladen werden: **https://<iDRACIP>/software/ism/ISM-Dell-Web-3.6.0-VIB-ESX6i-Live.zip**.

Das Red Hat Enterprise Linux Webpaket kann hier heruntergeladen werden: **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-LX-3.6.0.tar.gz**.

Unterstützung für idrac.local und drac.local als iDRAC-FQDN

Sie können iSM über das Hostbetriebssystem mit der iDRAC-Benutzeroberfläche verbinden, indem Sie `drac.local` oder `idrac.local` im Webbrowser eingeben, unabhängig davon, ob das Hostbetriebssystem Multicast-DNS (Domain Name System) unterstützt.

ANMERKUNG: Diese Funktion wird nur über eine IPv4-Adresse unterstützt.

4

Konfigurieren des iDRAC Servicemoduls

die iDRAC-Servicemodul-Funktionen können Remote über verschiedene iDRAC-Schnittstellen konfiguriert werden, z. B. die Benutzeroberfläche, die CLI und WS-Man.

Themen:

Konfigurieren des iDRAC-Servicemoduls über die iDRAC-Webschnittstelle

Melden Sie sich bei der iDRAC-Benutzeroberfläche mit der iDRAC-IP-Adresse als root- oder Administrator-Nutzer an.

Um iSM über die iDRAC-Webschnittstelle für yx2x-und yx3x-PowerEdge-Server zu verwenden, gehen Sie zu **Übersicht** > **Server** > **Servicemodul**.

Um iSM über die iDRAC-Webschnittstelle für yx4x-und yx5x-PowerEdge-Server zu verwenden, gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **iDRAC-Servicemodule einrichten**.

Konfigurieren des iDRAC-Servicemoduls über RACADM

Auf iSM kann über RACADM CLI-Befehle zugegriffen und es von dort konfiguriert werden. Um den Status der von iSM bereitgestellten Funktionen zu überprüfen, verwenden Sie den Befehl `racadm get idrac.servicemodule`. Die Funktionen werden:

- ChipsetSATASupported
- HostSNMPAlert
- HostSNMPGet
- iDRACHardReset
- iDRACSSOLauncher
- LCLReplication
- OSInfo
- ServiceModuleEnable
- SSEventCorrelation
- WatchdogRecoveryAction
- WatchdogResetTime
- WatchdogState
- WMIInfo

Verwenden Sie den Befehl `racadm set idrac.servicemodule. <feature name> <enabled or disabled>`, um die Funktionen festzulegen oder zu konfigurieren.

ANMERKUNG: Funktionsnamen und Attribute, die mit dem Symbol # beginnen, können nicht geändert werden.

Informationen zur Verwendung von iSM über RACADM finden Sie in den Objekten in der Gruppe **Servicemodul** im *RACADM Befehlszeilen-Referenzhandbuch für iDRAC8, iDRAC9 und CMC* auf **Dell.com/support**.

Konfigurieren des iDRAC-Servicemoduls über WS-Man

Auf iSM kann über WS-Man mit diesem Befehl zugegriffen und es von dort konfiguriert werden:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/
DCIM_iDRACCardService?
CreationClassName=DCIM_iDRACCardService+Name=DCIM:iDRACCardService+SystemCreationClassName=DCI
M_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"}
```

Informationen zur Verwendung des iSM über WS-Man finden Sie im *Handbuch zur Dell Lifecycle Controller 2 Webservices-Schnittstelle*. Dieses Handbuch enthält Informationen und Beispiele für die Verwendung von WS-Man und ist auf **Dell.com/support** verfügbar.

5

Sicherheitskonfigurationen und Kompatibilität

Das iDRAC-Servicemodul (iSM) wird mit der standardmäßigen Sicherheitskonfiguration bereitgestellt, um vor bestimmten Gefahren wie DLL-Hijacking, DLL-Manipulationen und Offenlegung von Daten zu schützen. In diesem Abschnitt wird die Sicherheitskonfiguration beschrieben, mit der iSM installiert wird.

Themen:

Verbesserte Sicherheit zwischen iSM- und iDRAC-Kommunikation durch Verwendung des TLS-Protokolls

Die Datenkommunikation zwischen iSM und iDRAC verwendet TLS-geschützte USBNIC-INET-Sockel. Dadurch wird der Schutz aller Daten gewährleistet, die vom iDRAC über USBNIC zum iSM übertragen werden. iSM und iDRAC verwenden selbst signierte Zertifikate zur Steuerung der Authentifizierung. Die selbst signierten Zertifikate sind 10 Jahre lang gültig. Neue selbst signierte Zertifikate werden jedes Mal bei jeder neuen Installation vom neuen iSM erzeugt. Installieren oder aktualisieren Sie das iSM, wenn die Zertifikate ablaufen.

ANMERKUNG: Die Neuinstallation (Reparatur) von iSM ist auf Linux-Betriebssystemen nicht möglich. Sie müssen iSM auf Linux-Betriebssystemen deinstallieren und anschließend installieren.

ANMERKUNG: Wenn das TLS-Clientzertifikat von iSM abläuft, schlägt die Kommunikation zwischen iSM und iDRAC fehl und es wird ein Auditprotokoll des Betriebssystems erzeugt. Anschließend müssen Sie iSM auf dem Hostbetriebssystem neu installieren.

Sowohl der iDRAC als auch die Host TLS-Versionen müssen 1.1 oder höher sein. Die Kommunikation zwischen iSM und iDRAC schlägt fehl, wenn die TLS-Protokollversionsverhandlung fehlschlägt. Wenn iSM mit TLS-Funktionalität auf iDRAC-Firmware installiert ist, die TLS-Kommunikation über USBNIC nicht unterstützt, funktioniert es mit dem Nicht-TLS-Kanal wie in den früheren Versionen von iSM.

Wenn iSM installiert oder auf Version 3.4.0 oder höher aktualisiert wird, bevor iDRAC auf Version 3.30.30.30 oder höher aktualisiert wird, muss iSM deinstalliert und neu installiert werden, um ein neues TLS-Zertifikat einzurichten. iSM mit TLS-Funktionalität wird von iDRAC-Firmware ab Version 3.30.30.30 unterstützt.

iSM ohne TLS-Funktionalität funktioniert auf einer TLS-fähigen Version der iDRAC-Firmware nicht. Beispiel: iSM 3.3 oder frühere Versionen ohne TLS-Fähigkeit werden von iDRAC-Firmware 3.30.30.30 und höher nicht unterstützt. Wenn iSM 3.3.0 auf iDRAC-Firmware der Version 3.30.30.30 installiert ist, treten in der Lifecycle-Controller-Protokolldatei mehrere Ereignisse mit ISM0050 auf.

ANMERKUNG: Wenn der FIPS-Modus (Federal Information Processing Standards) entweder auf dem Hostbetriebssystem oder iDRAC aktiviert sind, wird die Kommunikation zwischen iSM und iDRAC nicht hergestellt.

Policy-Einstellungen für Betriebssystem-BMC-Passthrough auf VMware ESXi

Im olgenden werden die Befehle und die betroffenen Parameter der Policy-Einstellungen für die Betriebssystem-BMC-Passthrough-Schnittstelle auf VMware ESXi aufgeführt:

```
esxcli network vswitch standard portgroup policy security set -u -p "iDRAC Network"
```

Allow Promiscuous: false

Allow MAC Address Change: false

Allow Forged Transmits: false

```
esxcli network vswitch standard policy security set -v vSwitchiDRACvusb -f false -m false
```

Override vSwitch Allow Promiscuous: false

Override vSwitch Allow MAC Address Change: false

Override vSwitch Allow Forged Transmits: false

Authentifizieren von DLLs und gemeinsam genutzten Objekten vor dem Laden

Das sichere Laden von Bibliotheken in iSM verhindert Angriffe wie DLL-Hijacking, DLL-Preloading und Binary Planting. Um iSM vor solchen Angriffen zu schützen, verhindert diese Funktion Folgendes:

- Laden dynamischer Bibliotheken von jedem beliebigen Pfad.
- Laden unsignierter Bibliotheken.

Diese Funktion führt eine Pfadüberprüfung und eine Authenticode-Signaturüberprüfung für DLLs und freigegebene Objekte durch. Ein Ausfallsereignis wird im Falle eines Fehlschlagens der DLL und der Shared Objects ausgelöst. Wenn die Authentifizierungsvalidierung nicht erfolgreich ist, wird die entsprechende Bibliothek nicht geladen und in der Protokolldatei des Betriebssystems geprüft.

6

iSM-Monitoring-Funktionen

Mit dem iSM können Sie Aspekte der Serverleistung überwachen und managen, z. B. Aus- und Einschalten, Sicherheit, Warnmeldungen und ein spezielles Gerätemanagement, um die Integrität und Verfügbarkeit des Systems zu optimieren und aufrechtzuerhalten.

ANMERKUNG: **FullPowerCycle** und **Support Assist on the Box** werden nur von den PowerEdge-Servern yx4x und yx5x unterstützt.

Themen:

S.M.A.R.T.-Monitoring

Die S.M.A.R.T.-Monitoring-Funktion unterstützt SATA-Festplatten mit SATA im AHCI-Modus und im RAID-Modus. Sie verfügt über integrierte Funktionen zum Überwachen von S.M.A.R.T.-Warnmeldungen über vom iDRAC unterstützte Prüfmethoden für Festplatten mit SATA-Chipsatz-Controller. Zuvor wurden die Warnmeldungen von einem Open-Source-Hilfsprogramm überwacht, um die Festplatten im RAID-Modus zu überwachen.

Tabelle 10. Attributwerte und Beschreibung

Attributwerte	Beschreibung
Aktiviert	Die Chipsatz-SATA-Controller werden in Echtzeit auf S.M.A.R.T.-Ereignisse überwacht.
Deaktiviert	S.M.A.R.T.-Überwachung ist deaktiviert.
-	Chipsatz-SATA-Controller ist nicht verfügbar.

ANMERKUNG: Standardmäßig ist das S.M.A.R.T-Attribut auf **Aktiviert** oder **NV** eingestellt, wenn die Konfiguration Chipsatz-SATA nicht unterstützt.

S.M.A.R.T.-Überwachung ist eine Funktion, die über das iSM-Installationsprogramm installiert wird. Der Nutzer kann das iSM-Installationspaket installieren/ändern, um die S.M.A.R.T.-Monitoring-Funktion zu deaktivieren. Diese Funktion ist auf einer von Dell EMC unterstützten S.M.A.R.T.-fähigen SATA-Festplatten verfügbar.

Wenn die Festplatte S.M.A.R.T.-fähig ist und die Funktion aktiviert ist, überwacht das iSM die Festplatten und erzeugt entsprechende Ereignisse. Der standardmäßige Monitoring-Zeitraum ist 24 Stunden und kann nicht manuell konfiguriert werden. Es werden nur Ereignisse des Typs PDR16 (vorhersehbarer Fehler) und PDR22 (Temperaturschwellenwert überschritten) überwacht.

Wenn ein Betriebssystemfehler aufgrund von S.M.A.R.T.-Fehlern des Laufwerks vorliegt, wird das Ereignis nicht vom Betriebssystem erkannt. Wenn Festplatten Teil eines Storage-Pools sind, überwacht das iSM solche Laufwerke nicht auf S.M.A.R.T.-Fehler.

Auf den PowerEdge-Servern yx3x ist das Monitoring von S. M. A. R. T über Software-RAID nur für das Ereignis „PDR22“ verfügbar.

ANMERKUNG: S.M.A.R.T erfordert außerdem die Installation der iDRAC9-Firmware 4.00.00.00 oder höher.

Betriebssystem-Informationen

OpenManage Server Administrator teilt sich derzeit Betriebssysteminformationen und Hostnamen mit iDRAC. Das iDRAC-Servicemodul (iSM) stellt ähnliche Informationen bereit, beispielsweise den Namen des Betriebssystems, IP-Adressinformationen, Betriebssystemversion und den FQDN (Fully Qualified Domain Name) mit iDRAC. Die Netzwerkschnittstellen auf dem Hostbetriebssystem werden ebenfalls angezeigt. Standardmäßig ist diese Überwachungsfunktion aktiviert. Diese Funktion ist auch dann verfügbar, wenn OpenManage Server Administrator auf dem Hostbetriebssystem installiert ist.

Sie können auch Daten der Hostbetriebssystem-Netzwerkschnittstelle oder entsprechende Informationen über das Redfish-Client-Plug-in für Browser anzeigen.

ANMERKUNG: Die niedrigste erforderliche iDRAC-Firmware-Version zum Anzeigen von Informationen über den Redfish-Client ist 3.00.00.00.

ANMERKUNG: iSM unterstützt jetzt die DHCP-Clients dhclient, dhcpd, Wicked, Netplan und intern mit Network Manager. Wenn die Netzwerkkonfiguration auf dem Hostbetriebssystem mit einem anderen DHCP-Client konfiguriert ist, kann iSM die Statusänderung der Netzwerkschnittstelle nicht überwachen, z. B. die DHCP-Konfiguration einer Schnittstelle. Daher sind Sie möglicherweise nicht in der Lage, die Änderung der Netzwerkschnittstellendetails des Hostbetriebssystems, wie z. B. DHCP-Status, DHCP-Server, Standard-Gateway, DNS-Server in den iDRAC-Schnittstellen anzuzeigen.

Replikation des Lifecycle-Controller-Protokolls in das Betriebssystem

Die Lifecycle-Controller-Protokollreplikation repliziert die LC-Protokolldateien (Lifecycle Controller) in die Betriebssystem-Protokolldateien. Alle Ereignisse, die die Option „Betriebssystemprotokoll“ als Ziel auf der Warnmeldungsseite oder in den entsprechenden RACADM oder WS-Man-Schnittstellen haben, werden in den Betriebssystem-Protokolldateien repliziert. Dieser Prozess ähnelt der Systemereignisprotokoll-Replikation (SEL) durch OpenManage Server Administrator.

Die standardmäßigen Protokolldateien, die in die Betriebssystem-Protokolldateien aufgenommen werden sollen, sind dieselben wie für SNMP Traps oder Warnmeldungen konfigurierte Protokolle. Die Ereignisse, die in der Lifecycle-Controller-Protokolldatei protokolliert werden, nachdem das iSM installiert wurde, werden jedoch in die Betriebssystem-Protokolldatei repliziert. Wenn OpenManage Server Administrator installiert ist, ist diese Monitoringfunktion zur Vermeidung doppelter SEL-Einträge in der Betriebssystemprotokolldatei deaktiviert.

In iSM können Sie den Speicherort für die Replikation der Lifecycle-Controller-Protokolldateien anpassen. Standardmäßig werden die Lifecycle-Controller-Protokolldateien in der Gruppe **System** im Ordner **Windows-Protokolle** in der **Ereignisanzeige** repliziert. Sie können die Lifecycle-Controller-Protokolle in eine vorhandene Gruppe replizieren oder einen Ordner im Ordner **Anwendungs- und Dienstprotokolle** im Fenster **Ereignisanzeige** erstellen. Wenn iSM bereits installiert ist und das Hostbetriebssystem einen Neustart durchläuft oder iSM neu gestartet wird und iDRAC einige Lifecycle-Controller-Protokolldateien enthält, die während dieser Host-Ausfallzeit erzeugt werden, dann werden diese Lifecycle-Controller-Protokolldateien bei der Erstellung des Service als vergangene Ereignisse in der Betriebssystemprotokolldatei gespeichert.

ANMERKUNG: Sie können den Speicherort für die Replikation der Lifecycle-Controller-Protokolldateien nur während der benutzerdefinierten Installation von iSM oder der iSM-Modifizierung auswählen.

ANMERKUNG: Der Quellenname der iSM-Lifecycle-Controller-Protokolldateien wurde vom **iDRAC-Servicemodul** in **Lifecycle-Controller-Protokoll** geändert.

Automatische Systemwiederherstellung

Die automatische Systemwiederherstellungsfunktion ist ein Hardware-basierter Zeitgeber, der verwendet wird, um den Server im Falle eines Hardwarefehlers wiederherzustellen. Sie können automatische Systemwiederherstellungsvorgänge wie z. B. Neustart, Aus-/Einschalten oder Ausschalten nach einem festgelegten Zeitintervall ausführen. Diese Funktion ist nur dann aktiviert, wenn der Watchdog-Zeitgeber des Betriebssystems deaktiviert ist. Wenn OpenManage Server Administrator installiert ist, ist diese Überwachungsfunktion zur Vermeidung doppelter Watchdog-Zeitgeber deaktiviert.

Sie können drei Parameter in dieser Funktion über iDRAC-Schnittstellen konfigurieren:

1. **Watchdog-Zustand**: Der Standardstatus ist aktiviert, wenn OMSA nicht vorhanden ist und wenn der BIOS- oder Betriebssystem-Watchdog-Zeitgeber deaktiviert ist.
2. **Watchdog-Timeout**: Der Standardwert ist 480 Sekunden. Der Mindestwert beträgt 60 Sekunden, der Maximalwert 720 Sekunden.
3. **Wiederherstellungsmaßnahme oder Autom. Wiederherstellungsmaßnahme für Watchdog-Timeout**: Die Aktionen können **Aus- und Einschalten**, **Ausschalten**, **Neustart** oder **Keine** sein.

ANMERKUNG: Wenn im Windows Betriebssystem das Ereignis DLL-Authentifizierungsfehler (SEC0704) ausgelöst wird, wird die auf der Seite „iSM-Einstellungen“ konfigurierte automatische Systemwiederherstellungsmaßnahme durchgeführt. iSM muss repariert oder neu installiert werden, um den Standardzustand wiederherzustellen.

Windows Management Instrumentation-Provider

Die mit iSM verfügbaren WMI-Anbieter (Windows Management Instrumentation) bieten Hardware-Daten über WMI. Bei WMI handelt es sich um eine Gruppe von Erweiterungen des Windows-Treibermodells, die eine Betriebssystemschnittstelle bereitstellen, über die instrumentierte Komponenten Informationen und Benachrichtigungen zur Verfügung stellen. WMI ist die Microsoft-Implementierung des Web-Based Enterprise Management (WBEM) und Common Information Model (CIM) der Distributed Management Task Force (DMTF) für die Verwaltung von Serverhardware, Betriebssystemen und Anwendungen. WMI-Anbieter helfen bei der Integration mit Systemverwaltungskonsolen wie Microsoft System Center und ermöglichen das Scripting zur Verwaltung von Microsoft Windows Server-Lösungen.

Der verwendete Namespace ist `\\root\cimv2\dcim` . Die unterstützten Abfragen sind **Enumeration** und **Get**. Sie können jede WMI-Client-Benutzeroberfläche wie z. B. **winrm**, **Powershell**, **WMIC**, **WBEMTEST** zur Abfrage der von iDRAC unterstützten Profile über das Hostbetriebssystem nutzen.

ANMERKUNG: Wenn mehrere WMI-Klassen gleichzeitig aufgelistet werden, kann das iSM die Kommunikation mit dem iDRAC neu starten. Es sind keine Maßnahmen erforderlich.

Vorbereiten zum Entfernen eines NVMe-PCIe-SSD-Geräts

Sie können NVMe-PCIe-SSDs (Non-Volatile Memory Express Peripheral Component Interconnect Express Solid State Device) ohne Herunterfahren oder Neustarten des Systems entfernen. Wenn Sie ein Gerät entfernen, müssen alle Aktivitäten im Zusammenhang mit dem Gerät gestoppt werden, um Datenverlust zu verhindern. Beenden Sie alle Aktivitäten manuell, bevor Sie den Task „Auf Entfernen vorbereiten“ durchführen. Um Datenverlust zu vermeiden, verwenden Sie die Option „Auf Entfernen vorbereiten“, nach der Sie die NVMe-PCIe-SSD physisch entfernen können. Der Vorgang zum Vorbereiten auf Entfernen führt die Validierung durch und überprüft, ob das Gerät mit einer Aktivität ausgelastet ist oder nicht. Wenn das Gerät mit einer Aktivität ausgelastet ist, wird der Vorgang „Auf Entfernen vorbereiten“ nicht fortgesetzt.

ANMERKUNG: Folgen Sie den von VMware dokumentierten Voraussetzungen vor der Durchführung des Vorgangs **Vorbereitung zum Entfernen** in VMware ESXi.

Remote-iDRAC-Kaltstart

iDRAC reagiert möglicherweise aus verschiedenen Gründen nicht mehr. iSM können vollständig zurücksetzen einer nicht antwortenden iDRAC8- oder iDRAC9-Controller durch vorübergehend entfernen Stromversorgung des iDRAC Controller ohne Beeinträchtigung Betriebssystem Produktion. Diese Funktion kann nur auf der iSM-Seite im iDRAC über eine der iDRAC-Schnittstellen deaktiviert werden.

Um iDRAC zurückzusetzen, verwenden Sie den folgenden Windows PowerShell- oder Linux Shell Befehl:

```
./Invoke-iDRACHardReset
```

ANMERKUNG: Der Shell-Befehl wird nur auf VMware ESXi 7.x unterstützt.

In allen ESXi-Betriebssystemen können Sie den iDRAC-Reset remote mithilfe des folgenden WinRM-Remote-Befehls durchführen:

```
winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cimschema/2/root/cimv2/
dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:"root-
username" -p:"password" -r:https://"Host-IP":443/wsman -a:basic -encoding:utf-8 -skipCNCheck
-skipCACheck -skipRevocationcheck
```

ANMERKUNG: Die Remote-iDRAC-Hardware-Reset-Funktion funktioniert nur mit iDRAC8 auf den PowerEdge-Servern yx3x oder höher und bei Anmeldung auf dem Betriebssystem als Administrator.

iDRAC-Zugriff über Host-BS

Mit PowerEdge-Servern können Sie die Hardware oder die Firmware eines Geräts über iDRAC verwalten, indem Sie ein iDRAC-dediziertes Netzwerk konfigurieren. Über den dedizierten Netzwerkport können Sie auf die iDRAC-Schnittstellen wie z. B. UI, WS-Man, RACADM und Redfish-Client zugreifen.

Voraussetzung für die Verwaltung der Hardware oder der Firmware ist eine dedizierte Verbindung zwischen einem Gerät und der unterstützten iDRAC-Schnittstelle. Mithilfe der iDRAC-Zugriffsfunktion über Hostbetriebssystem können Sie eine Verbindung zu einer iDRAC-Schnittstelle von einer IP-Adresse des Betriebssystems oder einem Host unabhängig von der Verbindung zwischen einem Gerät und einem iDRAC-dedizierten Netzwerk herstellen. Diese Funktion ermöglicht Ihnen die Überwachung der Hardware oder Firmware, selbst wenn der iDRAC nicht mit dem Netzwerk verbunden ist.

Sie können jede der folgenden Unterfunktionen wählen, um über das Hostbetriebssystem auf den iDRAC zuzugreifen.

- **Zugriff über GUI, WS-Man, Redfish, Remote RACADM**
- **In-Band SNMP-Traps**
- **Zugriff über SNMP-Get**

Wenn Sie **iDRAC-Zugriff über Hostbetriebssystem** wählen, werden alle Unterfunktionen standardmäßig ausgewählt. Wenn Sie eine der Unterfunktionen einzeln auswählen möchten, können Sie die entsprechende Funktion wählen und diese aktivieren.

Weitere Informationen finden Sie unter iDRAC-Zugriff über Hostbetriebssystem.

Zugriff auf iDRAC über GUI, WS-Man, Redfish und Remote RACADM

Die Funktion **Zugriff über GUI, WS-Man, Redfish, Remote RACADM** ermöglicht es dem Administrator des Hostbetriebssystems, über das Hostbetriebssystem remote auf iDRAC-Schnittstellen zuzugreifen. Geben Sie die URL `https:// <Host OS IP Address>: <ListenPortNumber>` im Browser der Remote-Management-Station zum Zugriff auf die iDRAC-UI ein.

ANMERKUNG: „ListenPortNumber“ ist die Portnummer, die während der Aktivierung der Funktion „iDRACAccessviaHostOS“ des iSM konfiguriert wurde.

In-Band-Unterstützung für iDRAC SNMP-Warnmeldungen

Alle Ereignisse, die die Option **SNMP Trap** als Ziel auf der Seite „Warnmeldungen“ oder in den entsprechenden RACADM- oder WS-man-Schnittstellen haben, können über das Betriebssystem mit dem iSM als SNMP Trap empfangen werden. Ab iDRAC-Firmware 3.0.0 oder höher erfordert diese Funktion nicht die Aktivierung der iSM-LCL-Replikationsfunktion. Nur die Ereignisse, die nach der Installation des iSM in der Lifecycle-Controller-Protokolldatei protokolliert werden, werden als SNMP Traps gesendet.

Unter Verwendung des iSM können Sie SNMP-Warnmeldungen vom Hostbetriebssystem empfangen, die den vom iDRAC generierten Warnmeldungen gleichen.

Standardmäßig ist diese Funktion deaktiviert. Obwohl der In-Band-SNMP-Warnmechanismus mit dem iDRAC-SNMP-Warnmechanismus koexistieren kann, verfügen die aufgezeichneten Protokolle möglicherweise über redundante SNMP-Warnmeldungen von beiden Quellen. Es wird empfohlen, entweder die In-Band- oder Out-of-Band-Option anstelle von beiden zu verwenden.

ANMERKUNG: Sie können die In-Band-SNMP-Funktion auf PowerEdge-Servern yx3x oder höher mit einer Mindestversion der iDRAC-Firmware von 2.30.30.30 verwenden.

Weitere Informationen finden Sie im Whitepaper: In-Band iDRAC-SNMP-Warnmeldungen.

WS-Man remote aktivieren

Sie können aktuell mit der Funktion „WMI-Information“ auf den Host-Namespace von Microsoft Windows WMI zugreifen, um die System-Hardware zu überwachen. Die WMI-Schnittstelle des Hosts ist standardmäßig aktiviert und Sie haben Remote-Zugriff darauf. Wenn Sie jedoch per WMI-Adapter auf die WMI-Schnittstellen zugreifen möchten, müssen Sie dies manuell tun, da dies keine Standardeinstellung ist. Mit dieser Funktion können Sie per Remote-Zugriff auf die WINRM WMI-Namespaces zugreifen, indem Sie sie während der Installation aktivieren.

Auf diese Funktion kann über die PowerShell-Befehle zugegriffen werden. Die Befehle, die verwendet werden, lauten:

Tabelle 11. WS-Man remote aktivieren

Befehl	Beschreibung
`Enable-iSMWSMANRemote –Status enable – Forcereconfigure yes –Createselfsigncert yes – IPAddress <IP address> –Authmode Basic, Kerberos, Certificate`	Aktivieren und Konfigurieren der Remote-WS-Man-Funktion
`Enable-iSMWSMANRemote –Status get`	Anzeigen des Status der Remote-WS-Man-Funktion
`Enable-iSMWSMANRemote –Status disable`	Deaktivieren der Remote-WS-Man-Funktion
`Enable-iSMWSMANRemote –Status enable – Forcereconfigure yes –Createselfsigncert yes – IPAddress <IP address>`	Konfigurieren der Remote-WS-Man-Funktion

ANMERKUNG: Sie müssen über ein Server-Authentifizierungszertifikat und eine https-Protokoll verfügen, damit diese Funktion genutzt werden kann.

AutoUpdate von iSM

Sie können iSM mithilfe des iDRAC AutoUpdate-Prozesses aktualisieren.

ANMERKUNG: Wenn iDRAC AutoUpdate aktiviert ist, muss iSM LC DUP auf die neueste Version von Dell.com/support aktualisiert werden.

ANMERKUNG: Sie müssen die Aktualisierungen nicht von support.dell.com herunterladen. Das aktualisierte iSM-Paket ist in iDRAC lokal verfügbar.

ANMERKUNG: iSM LC DUP in iDRAC wird entfernt, wenn die Option iDRAC LC Wipe verwendet wird. Sie müssen das iSM LC DUP von Dell.com/support herunterladen.

Tabelle 12. Befehle zum Installieren und Aktualisieren von iSM

Befehle zur Ausführung in der Eingabeaufforderung	Beschreibungen
`dcism-sync.exe`	Zum Installieren oder Aktualisieren von iSM. Führen Sie die Schritte im Installationsassistenten aus.
`--help/-h`	Zur Anzeige des Inhalts der Hilfe.
`--silent/-s`	Zur Installation oder zum Update im Hintergrund.
`--force/-f`	Zum Deinstallieren der aktuellen Version und zur Installation des verfügbaren Update-Pakets im Lifecycle Controller.

Tabelle 12. Befehle zum Installieren und Aktualisieren von iSM (fortgesetzt)

Befehle zur Ausführung in der Eingabeaufforderung	Beschreibungen
	ANMERKUNG: Diese Option überschreibt die vorherige Konfiguration.
`--get—version/-v`	Zum Abrufen von Details über die Updatepaketversion und die installierte Version von iSM.
`--get—update/-g`	Zum Herunterladen der iSM-Updatepakete in das vom Nutzer angegebene Verzeichnis.
`dcism-sync.exe —p "feature"`	Zur Installation spezieller Funktionen wie bei CLI-Argumenten, die mit `msiexec.exe` verwendet werden. Geben Sie beispielsweise zur Installation des iDRAC-Zugriffs über die Funktion Host-BS-iDRAC unter Windows `dcism-sync.exe -p "ADDLOCAL=IBIA"` ein.

FullPowerCycle

FullPowerCycle ist eine aufrufende Schnittstellenfunktion, die eine Methode zum Zurücksetzen der Server-Hilfsstromversorgung bietet. Eine zunehmende Anzahl von Serverhardware wird über den Serverhilfsstrom ausgeführt. Beim Troubleshooting einiger Serverprobleme müssen Sie das Netzkabel des Servers physisch von der Stromversorgung trennen, um die Hardware zurückzusetzen, die mit Hilfsstrom ausgeführt wird.

Mit der Funktion „FullPowerCycle“ kann der Administrator den Hilfsstrom ohne Besuch des Rechenzentrums remote aktivieren bzw. deaktivieren. Diese Funktion wird auf den PowerEdge-Servern yx4x und neuer unterstützt.

Wenn eine FullPowerCycle-**Anfrage** über diese Schnittstelle eingegeben wird, wirkt sich dies nicht sofort auf die Systemversorgung aus. Stattdessen wird eine Markierung gesetzt, die abgefragt wird, wenn das System zu S5 übergeht. Zur Aktivierung der Funktion „FullPowerCycle“ muss nach dem Anfragebefehl noch ein Befehl zum Herunterfahren des Systems ausgeführt werden. Wenn die Markierung auf den S5-Eintrag gesetzt wird, wird das System vorübergehend in einer niedrigeren Versorgungszustand zwangsversetzt, ähnlich wie beim Entfernen und Austauschen eines Netzteils. Die Markierung kann unter Verwendung der **Abbrechen**-Funktion immer dann gelöscht werden, wenn sich das System im S0-Zustand befindet, bevor das System in den S5-Zustand übergeht.

Sie können verschiedene Optionen für FullPowerCycle auf Ihrem System nutzen. Verwenden Sie die folgenden Befehle zur Anforderung, zur Statusabfrage und zum Abbrechen von FullPowerCycle auf Ihrem System:

Für Windows Betriebssysteme stehen für die Aktivierung von FullPowerCycle (Anforderung), das Abbrechen von FullPowerCycle und Statusabfrage von FullPowerCycle Rechtsklickmenüs zur Verfügung.

Tabelle 13.

Befehle zum Ausführen in der PowerShell-Konsole	Beschreibungen
`Invoke-FullPowerCycle —status request`	Zum Anfordern von FullPowerCycle auf Ihrem System. **ANMERKUNG:** Es wird die Meldung angezeigt, dass der VirtualAC-Ein- /Ausschaltzyklus durch das Serverbetriebssystem ausgelöst wird.
`Invoke-FullPowerCycle -status Get`	Zum Abfragen des Status des FullPowerCycle auf Ihrem System. **ANMERKUNG:** Es wird die Meldung angezeigt, dass sich das System zum geplanten Datum und zur geplanten Uhrzeit abschaltet.
`Invoke-FullPowerCycle -status cancel`	Zum Abbrechen von FullPowerCycle auf Ihrem System.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle request`	Zum Anfordern von FullPowerCycle auf Ihrem Linux-Betriebssystem.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle cancel`	Zum Abbrechen von FullPowerCycle auf Ihrem Linux-Beriebssystem.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle get-status`	Zum Abfragen des Status des FullPowerCycle auf Ihrem Linux-Betriebssystem.

Folgende Meldungen werden nach erfolgreicher Ausführung des Vorgangs „FullPowerCyle“ im Betriebssystemprotokoll und LCL angezeigt.

Anforderungsnachricht:`"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".`

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

ANMERKUNG: Die Funktion FullPowerCycle ist für das Betriebssystem ESXi 7.x verfügbar, jedoch nicht für die Betriebssysteme ESXi 6.x.

ANMERKUNG: Die Funktion „FullPowerCycle“ kann nur von lokalen oder Domainadministratoren sowie von Root- oder Sudo-Nutzern verwendet werden.

On-The-Box SupportAssist

SupportAssist spart Zeit und optimiert die technischen Support-Fälle. Eine auf einem Ereignis basierende Datenerfassung erstellt mit SupportAssist einen offenen Service Request. Geplante Datenerfassungen helfen bei der Überwachung und Wartung Ihrer Umgebung. Zu diesen Erfassungen zählen Hardwareinformationen, RAID-Controller-Protokolldateien, Betriebssystem und Anwendungsdaten. Die unterstützten Funktionen sind:

- **SupportAssist-Registrierung**: iSM unterstützt die SupportAssist-Registrierung. Dies ist eine einmalige Aktivität. Sie können die erforderlichen Details wie Name, E-Mail, Adresse und Nummer eingeben und die Registrierung abschließen.
- **SupportAssist-Erfassung**: Die SupportAssist-Erfassungsfunktion in iDRAC erfasst Informationen über die Hardware, das Betriebssystem und relevante Anwendungsdaten und komprimiert diese Informationen.

SupportAssist bietet außerdem:

- Proaktive Problemerkennung
- Automatische Fall-Erstellung
- Support-Kontakt durch einen Mitarbeiter des technischen Supports von Dell initiiert

ANMERKUNG: Sie müssen die Registrierung abschließen, um die Vorteile von SupportAssist zu nützen.

Sie können die folgenden Elemente im SupportAssist-Dashboard anzeigen.

Kurzbeschreibung des Service Request

In der Kurzbeschreibung des Service Request können Sie die Details der folgenden Anfragen anzeigen:

- Offen
- Geschlossen
- Eingereicht

SupportAssist-Übersicht

Sie können die Einzelheiten des **Servicevertrags** wie z. B. Vertragstyp und das Ablaufdatum und die Einstellungen für **Automatische Erfassung** in dieser Sitzung anzeigen.

Auf der Registerkarte **Service-Requests** können Sie auch die Liste der erstellten Anfragen und den Status anzeigen, die Beschreibung, Quelle, Service-Request-ID, Eröffnungsdatum, Schließungsdatum usw.

Wenn Sie auf die Registerkarte **Erfassungsprotokoll** klicken, können Sie Erfassungszeit, Job-ID, Erfassungstyp, erfasste Daten, Erfassungsstatus, Sendezeit usw. anzeigen.

ANMERKUNG: Wenn Sie die SupportAssist-Erfassung von iDRAC manuell einleiten, wird das USB-Massenspeichergerät dem Hostbetriebssystem nicht zur Verfügung gestellt. Die Übertragung von Betriebssystem-Erfassungsdateien und die erfassten Protokolldateien werden intern zwischen iDRAC und iSM verarbeitet.

ANMERKUNG: Die Erfassung von Betriebssystem- und Anwendungsdaten auf ESXi wird nur von den PowerEdge-Servern der Generation yx4x und höher unterstützt.

Registrierung von SupportAssist

Bevor Sie mit dem Registrierungsprozess beginnen, stellen Sie sicher, dass das iSM auf dem Hostbetriebssystem installiert ist und ausgeführt wird und eine funktionierende Internetverbindung verfügbar ist.

1. Melden Sie sich bei iDRAC an.
2. Wählen Sie aus dem Dropdown-Menü **Wartung** die Funktion **SupportAssist** aus.
   Der Assistent **SupportAssist-Registrierung** wird angezeigt.
3. Klicken Sie im **Begrüßungsfenster** auf **Weiter**.
4. Geben Sie in der Registerkarte **Kontakt- und Versandinformationen** Ihre primären Kontaktinformationen ein, z. B. **Vorname**, **Nachname**, **Telefonnummer**, **Alternative Nummer**, **E-Mail-Adresse**, **Unternehmensname**, **Adresszeile 1**, **Adresszeile 2**, **Stadt**, **Staat**, **Postleitzahl** und **Land**.

   ANMERKUNG: Sie können sekundäre Kontaktinformationen hinzufügen, indem Sie auf die Option **Sekundäre Kontaktinformationen hinzufügen** klicken.

   ANMERKUNG: Um mit der Registrierung fortzufahren, müssen Sie alle erforderlichen Pflichtangaben ausfüllen.

5. Nach dem Ausfüllen der Kontakt- und Lieferdaten klicken Sie auf **Weiter**.
6. Lesen Sie sich die Softwarelizenzvereinbarung durch, wählen Sie die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus und klicken Sie dann auf **Registrieren**.

   ANMERKUNG: Es kann einige Minuten dauern, den Registrierungsvorgang abzuschließen. Nachdem die Registrierung erfolgreich abgeschlossen wurde, erhalten Sie eine Willkommens-E-Mail von SupportAssist unter der angegebenen E-Mail-Adresse.

7. Auf der Registerkarte **Zusammenfassung** können Sie die **Registrierungs-ID** und die aktuellen Einstellungseinzelheiten für **Automatische Funktionen** anzeigen.
8. Zum Schließen des Assistenten **SupportAssist-Registrierung** klicken Sie auf **Schließen**.
   Wenn Sie auf der SupportAssist-Seite ganz nach unten navigieren, können Sie die Kontaktinformationen anzeigen.
9. Klicken Sie auf die Option **Bearbeiten**, um Änderungen an den primären oder sekundären Kontaktinformationen vorzunehmen.
10. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

SupportAssist Collection

Die Erfassungsfunktion von SupportAssist in iDRAC erfasst Informationen über die Hardware, das Betriebssystem und drelevanten Anwendungsdaten und komprimiert diese. Derzeit müssen Sie das Collector Tool für das Betriebssystem manuell ausführen, um den SupportAssist-Erfassungsbericht zu generieren. Über das iDRAC-Servicemodul erfasst das Collector-Tool für das Betriebssystem automatisch relevante Informationen zu Betriebssystem und Hardware. Die automatische Support-Protokollerfassung umfasst das Erfassen von Betriebssystem- und Anwendungsdaten.

Durch die Verwendung des iDRAC-Servicemoduls verringern Sie die Zahl der manuellen Arbeitsschritte zur Erfassung des Berichts für den technischen Support von Dell durch die Automatisierung des Erfassungsvorgangs.

Zu erfassende Daten

SupportAssist erstellt und sendet automatisch eine Erfassung an den technischen Support von Dell, wenn ein ereignisbasierter Auslöser vorhanden ist oder wenn Sie einen Zeitplan konfiguriert haben. Sie können die folgenden Arten von Informationen erfassen:

- **Systeminformationen**
- **Speicherprotokolle**
- **Betriebssystem- und Anwendungsdaten**
- **Debug-Protokolle**

Sie können auch die Funktion zur SupportAssist-Erfassung aus einer Betriebssystem-Shell heraus in einem festgelegten Pfad ausführen:

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

ANMERKUNG: Dieser Shellbefehl wird nur auf dem iDRAC9 mit den PowerEdge-Servern der Generation yx4x oder höher und bei Anmeldung am Betriebssystem als Administrator unterstützt.

ANMERKUNG: Auf dem Betriebssystem Windows Core müssen Sie zum absoluten Pfad navigieren, um den Befehl `Invoke-SupportAssistCollection.exe` auszuführen.

Erfassungseinstellungen

Sie können die Erfassungseinstellungen über die Funktion „Erfassungseinstellungen“ auswählen oder einstellen. Sie können eine beliebige der folgenden Arten von Erfassungseinstellungen zum Speichern der Erfassungsberichte auswählen:

- **Jetzt Senden**: Sie erhalten eine Benachrichtigung, dass der **Job erfolgreich der Warteschlange hinzugefügt wurde**, nachdem Sie auf die Option **Erfassen** geklickt haben.
- **Lokal speichern**
- **Im Netzlaufwerk speichern**: Wenn Sie diese Option auswählen, müssen Sie die Einzelheiten der **Netzwerkeinstellungen** wie z. B. **Protokoll**, **IP-Adresse**, **Freigabename**, **Domainname**, **Nutzername** und **Kennwort** angeben.

Sie können beliebige Erfassungseinstellungen auswählen und auf **Erfassen** klicken, um die Daten zu erhalten.

ANMERKUNG: Diese Funktion ist standardmäßig bei der Installation des iDRAC-Servicemoduls ab Version 2.0 auf Systemen, auf denen unterstützte Microsoft- oder Linux-Betriebssysteme ausgeführt werden, verfügbar. Sie können diese Funktion nicht deaktivieren.

ANMERKUNG: Die Erfassung der Betriebssystemprotokolldateien wird von der automatischen SupportAssist-Erfassung auf CentOS nicht unterstützt.

ANMERKUNG: Die Erhebung von Betriebssystem- und Anwendungsdaten auf ESXi wird nur von den PowerEdge-Servern yx4x und höher unterstützt.

Anonyme Erfassung von Berichten

Sie können SupportAssist Erfassungs- und Upload-Vorgänge durchführen, ohne den Registrierungsprozess abzuschließen. Bis zum iDRAC Servicemodul 3.0.2 war die Registrierung Voraussetzung für die SupportAssist-Erfassung.

Die unterstützte iDRAC-Firmware für die anonyme Erfassung ist iDRAC 3.15.15.15 auf den PowerEdge-Servern yx4x und yx5x und 2.60.60.60 auf yx3x.

ANMERKUNG: Sie können den Upload der anonymen SupportAssist-Datenerfassung durchführen, indem Sie die Felder Nutzername oder Kennwort in einer Proxy-Umgebung auf dem PowerEdge-Server yx3x leer lassen.

Korrelation von Software-Ereignissen zu Hardwarefehlern für Microsoft SDS

Die Ereignisprotokolldateien für Hardware Storage-Pool-Warnmeldungen oder-Ereignisse werden von iSM mit der Serverspeicher-Korrelationsfunktion überwacht. Das Server-Speicher-Subsystem wird überwacht, wenn Dell EMC Speichercontroller im RAID-Modus verwendet werden. Aber in Storage Spaces (SS) oder Storage Space Direct (S2D) wird das Server-Speicher-Subsystem im Passthrough-Modus überwacht oder der SATA-Chipsatz wird verwendet, um den Storage-Pool zu erstellen. Mit dieser Funktion werden die Hardware definierten Warnmeldungen, die durch das LC-Protokoll (Lifecycle Controller) erfasst werden, und die softwarebasierten Warnmeldungen, die von Betriebssystem-Protokolldateien erfasst werden, zusammengeführt und die Warnmeldungen werden in den iDRAC Lifecycle-Protokolldateien registriert.

Diese Funktion wird mit dem iSM-Paket installiert und ist standardmäßig aktiviert. Sie können die Einstellungen in den iDRAC-Einstellungen ändern. Im Rahmen des Monitoring prüft iSM die Protokolle auf potenzielle Fehler und Warnungen. iSM integriert die SS-Korrelationsereignisse auf dem Host in ein entsprechendes Lifecycle-Controller-Ereignis. Die SSLCMAP sollte nur die Lifecycle-Protokolldateien und SupportAssist-Warnmeldung erreichen. Sie können die SSLCMAP im iDRAC nicht für ein anderes Warnmeldungsziel konfigurieren.

Die folgenden Voraussetzungen gelten für die S2D-Protokollerfassung:

- Die SS-Ereigniskorrelationsfunktion muss auf der Servicemodulseite der iDRAC-Benutzeroberfläche aktiviert werden.
- Der PII-Filter muss auf der Servicemodulseite in der iDRAC-Benutzeroberfläche deaktiviert werden.

Tabelle 14. Windows Ereignismeldung, die unter LC-Protokollen zugeordnet ist, die unter der S2D-Ereigniskorrelation überwacht werden

Windows-Ereignisquelle: Quell-ID	Windows-Ereignismeldung	Zugeordnet auf iDRAC-LC-Protokoll
StorageSpaces – Treiber – 100	Die Konfiguration konnte vom physischen Laufwerk %1 nicht gelesen werden oder es wurden beschädigte Daten für Storage-Pool %2 zurückgegeben. Daher ist die Konfiguration im Arbeitsspeicher	**Meldungs-ID** : SDS0001

Tabelle 14. Windows Ereignismeldung, die unter LC-Protokollen zugeordnet ist, die unter der S2D-Ereigniskorrelation überwacht werden (fortgesetzt)

Windows-Ereignisquelle: Quell-ID	Windows-Ereignismeldung	Zugeordnet auf iDRAC-LC-Protokoll
	möglicherweise eine veraltete Kopie der Konfiguration. Rückgabecode: %3	
StorageSpaces – Treiber – 102	Für die meisten der physischen Laufwerke von Storage-Pool %1 ist beim Konfigurationsupdate ein Fehler aufgetreten, wodurch der Pool in einen Fehlerstatus gewechselt ist. Rückgabecode: %2	**Meldungs-ID** : SDS0002
StorageSpaces – Treiber – 103	Der Kapazitätsverbrauch von Storage-Pool %1 hat den für den Pool festgelegten Schwellenwert überschritten. Rückgabecode: %2	**Meldungs-ID** : SDS0003
StorageSpaces – Treiber – 200	Der Kopfbereich des Laufwerks für das physische Laufwerk %1 konnte nicht gelesen werden. Wenn Sie sicher sind, dass das Laufwerk noch zur Verfügung steht, kann diese Fehlerbedingung gelöscht werden, indem die Laufwerksintegrität mit der Befehlszeile oder der UI zurückgesetzt wird und anschließend können Sie das Laufwerk erneut seinem Storage-Pool zuordnen. Rückgabecode: %2	**Meldungs-ID** : SDS0004
StorageSpaces – Treiber – 203	Ein I/O-Fehler ist auf dem physischen Laufwerk %1 aufgetreten. Rückgabecode: %2	**Meldungs-ID** : SDS0005
StorageSpaces – Treiber – 300	Die Konfiguration konnte vom physischen Laufwerk %1 nicht gelesen werden, oder es wurden beschädigte Daten für den Speicherplatz %2 zurückgegeben. Daher ist die Konfiguration im Arbeitsspeicher möglicherweise eine veraltete Kopie der Konfiguration. Rückgabecode: %3	**Meldungs-ID** : SDS0006
StorageSpaces – Treiber – 301	Die Konfiguration konnte von allen Pool-Laufwerken nicht gelesen werden, oder es wurden beschädigte Daten für den Speicherplatz %1 zurückgegeben. Aus diesem Grund wird der Speicherplatz nicht angefügt. Rückgabecode: %2	**Meldungs-ID** : SDS0007
StorageSpaces – Treiber – 302	Für die meisten der Pool-Laufwerke, die Speichermetadaten für den Speicherplatz %1 hosten, ist bei einem Update der Speichermetadaten ein Fehler aufgetreten, wodurch der Storage-Pool in einen Fehlerstatus gewechselt ist. Rückgabecode: %2	**Meldungs-ID** : SDS0008
StorageSpaces – Treiber – 303	Laufwerke, die Daten für den Speicherplatz hosten, sind fehlerhaft oder fehlen. Daher ist keine Kopie der Daten verfügbar. Rückgabecode: %2	**Meldungs-ID** : SDS0009
StorageSpaces – Treiber – 304	Mindestens ein Laufwerk, das Daten für den Speicherplatz %1 hostet, ist fehlerhaft oder fehlt. Daher ist mindestens eine Kopie der Daten nicht verfügbar. Mindestens eine	**Meldungs-ID** : SDS0010

Tabelle 14. Windows Ereignismeldung, die unter LC-Protokollen zugeordnet ist, die unter der S2D-Ereigniskorrelation überwacht werden (fortgesetzt)

Windows-Ereignisquelle: Quell-ID	Windows-Ereignismeldung	Zugeordnet auf iDRAC-LC-Protokoll
	Kopie der Daten ist jedoch immer noch verfügbar. Rückgabecode: %2	
StorageSpaces – Treiber – 306	Fehler beim Versuch, den Speicherplatz %1 zuzuordnen oder mehr Speicher für ihn zu reservieren. Der Grund hierfür liegt darin, dass ein Schreibfehler beim Aktualisieren der Speicherplatzmetadaten aufgetreten ist. Rückgabecode: %2	**Meldungs-ID** : SDS0011
StorageSpaces – Treiber – 307	Fehler beim Versuch, die Zuordnung von Speicherplatz %1 aufzuheben bzw. diesen zu kürzen. Rückgabecode: %2	**Meldungs-ID** : SDS0012

ANMERKUNG: Im *Referenzhandbuch zu Ereignis- und Fehlermeldungen* finden Sie Informationen zu den Ereignis- und Fehlermeldungen, die von der Firmware und anderen Agenten, die die Systemkomponenten überwachen, generiert werden.

ANMERKUNG: Das PPID-Feld wird nicht für Warnmeldungen aufgezeichnet, die einem Storage-Pool entsprechen. iSM repliziert diese Warnmeldungen in die Lifecycle-Controller-Protokolle im iDRAC mit der PPID „NA“.

S2D-Protokollerfassung (Storage Spaces Direct) mit SupportAssist-Erfassung

Die SAC-Anforderung (SupportAssist-Erfassung) erfasst und verpackt die Protokolldateien von Storage Spaces Direct (S2D). Diese Funktion steht nur auf Microsoft Windows-Betriebssystemen zur Verfügung. Die SDS-Ereigniskorrelationsfunktion muss für SAC aktiviert werden, damit dieser Protokollerfassungsbericht aufgenommen werden kann.

S.M.A.R.T.-Protokolle für Datenträger und Chipsatz im Bericht der SupportAssist-Erfassung

iDRAC-Servicemodul (iSM) erfasst die S.M.A.R.T-Protokolldaten vom SATA-Chipsatz-Treiber, wenn die SupportAssist-Erfassung (SAC) in Echtzeit angefordert wird.

Diese Funktion erfordert, dass die Funktion **S.M.A.R.T.-Überwachung** im iSM aktiviert wird und **Speicherprotokolle** unter den SupportAssist Collection-Einstellungen auf dem iDRAC aktiviert sind.

S.M.A.R.T-Verlaufsprotokoll

S.M.A.R.T-Verlaufsprotokolldateien werden alle 24 Stunden von einem SATA-Controller-Treiber-Chipsatz oder einem Windows Software-RAID-Controller-Gerät erfasst, wenn diese Funktion aktiviert ist. Die S.M.A.R.T-Verlaufsprotokolldateien werden in einem geplanten Intervall in iSM erfasst und an iDRAC gesendet. iDRAC bündelt diese S.M.A.R.T-Verlaufsprotokolldateien als Teil der von Ihnen konfigurierten SupportAssist-Erfassung. S.M.A.R.T-Verlaufsprotokolldateien werden mithilfe des iSM-Installationsprogramms oder der dcismcfg-CLI aktiviert oder deaktiviert.

ANMERKUNG: Diese Funktion erfordert die iDRAC9-Firmware 4.40.00.00 und höher.

In der SupportAssist-Erfassung sind diese Protokolldateien hier verfügbar: `\tsr\storagelog\Smartlogs-nightly.zip`.

Die Dateinamen früherer S.M.A.R.T.- Protokolldateien, die vom iDRAC-Servicemodul bereitgestellt werden, bestehen aus dem Hostnamen als Präfix, gefolgt von einem alphanumerischen Wert. Beispiel: HostRD20200414.json.

CLI-Tool des iDRAC-Servicemoduls – dcismcfg

Das Dienstprogramm dcismcfg wird verwendet, um die Funktion zur S.M.A.R.T-Verlaufsprotokollerfassung zu aktivieren oder zu deaktivieren. Dieses Dienstprogramm wird auf allen Betriebssystemen unterstützt. Sobald das Dienstprogramm verwendet wird, um die Funktion zur S.M.A.R.T-Verlaufsprotokollerfassung zu aktivieren oder zu deaktivieren, erfüllt der nächste Abfragezyklus des S.M.A.R.T-Monitorings die Anfrage.

Führen Sie die folgenden Befehle aus, um die S.M.A.R.T-Verlaufsprotokollerfassung zu aktivieren oder zu deaktivieren:

Unter Windows führen Sie einen der folgenden Befehle aus:

- `<iSM install path>/shared/bin/dcismcfg.exe --collectperiodicsmartlog true/false`
- `<iSM install path>/shared/bin/dcismcfg.exe -c true/false`

Unter Linux führen Sie einen der folgenden Befehle aus:

- `<iSM install path>/bin/dcismcfg --collectperiodicsmartlog true/false`
- `<iSM install path>/bin/dcismcfg -c true/false`

Das Dienstprogramm dcismcfg muss als Administrator oder als root-Nutzer ausgeführt werden und wird ab iDRAC-Firmware-Version 4.40.00.00 und höher unterstützt.

ANMERKUNG: Die S.M.A.R.T-Verlaufsprotokollerfassung ist eine Unterfunktion der S.M.A.R.T-Monitoring-Funktion. Wenn Sie jedoch die S.M.A.R.T-Verlaufsprotokollerfassung aktivieren und die S.M.A.R.T-Monitoring-Funktion nicht aktiviert ist, werden Sie dazu aufgefordert, das S.M.A.R.T-Monitoring zu aktivieren, um die Verlaufsprotokollerfassung zu aktivieren.

SupportAssist-Erfassungseinstellungen

Gehen Sie zum Öffnen der Einstellungenseite für die SupportAssist-Erfassung zum SupportAssist-Dashboard im iDRAC und wählen Sie aus dem Drop-Down-Menü die Option **Einstellungen** aus.

iSM 3.4.0 oder höher unterstützt die gefilterte und nicht gefilterte **OSApp-Erfassung** (Erhebung von Betriebssystem- und Anwendungsdaten) auf ESXi. Diese Auswahl kann über die **Erfassungseinstellungen** getroffen werden.

Eine nicht gefilterte ausgewählte Erfassung enthält **vmsupport**-Protokolldateien für **Protokolle**, **Netzwerk**, **Storage**, **Konfiguration**, **Installationsprogramm**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines** und **hostProfiles**.

Die gefilterte ausgewählte Erfassung enthält **vmsupport**-Protokolle für **Storage**, **Konfiguration**, **Installationsprogramm**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines** und **hostProfiles**.

Archivverzeichnis einrichten

Sie können die Kopien der von SupportAssist durchgeführten Erfassungen in ein Verzeichnis speichern. Klicken Sie auf die Schaltfläche **Archivverzeichnis einrichten** klicken, um den Speicherort festzulegen.

Identifizierungsinformationen

Sie können die Identifizierungsinformationen in die gesendeten Daten aufnehmen, indem Sie auf das Drop-Down-Menü klicken und **Nein** oder **Ja** auswählen.

E-Mail-Benachrichtigungen

Sie können die E-Mail-Benachrichtigungseinstellungen festlegen, wenn eine neue Supportanfrage geöffnet oder eine neue SupportAssist-Erfassung hochgeladen wird. Wählen Sie aus dem Drop-Down-Menü **E-Mail-Benachrichtigungen empfangen** die Option **Nein** oder **Ja** aus.

Sie können die Spracheinstellung auswählen. Die verfügbaren Sprachen sind:

- **Englisch**
- **Deutsch**
- **Französisch**
- **Japanisch**
- **Spanisch**
- **Chinesisch (vereinfacht)**

Automatische Erfassung

Standardmäßig ist die automatische Erfassungsfunktion aktiviert. Um diese Funktion zu deaktivieren, verwenden Sie das Drop-Down-Menü, um entweder **aktivieren** oder **deaktivieren** auszuwählen.

Sie können auch die Uhrzeit für eine geplante Erfassung festlegen oder einstellen, indem Sie eine der folgenden Optionen aus dem Dropdown-Menü **Automatische Erfassungen planen** auswählen:

- **Wöchentlich**
- **Monatlich**
- **Vierteljährlich**
- **Nie**

Sie können die automatische Erfassung auch als wiederkehrend festlegen.

Um den ProSupport Plus-Empfehlungsbericht anzuzeigen, wählen Sie **Ja** aus dem Dropdown-Menü **ProSupport Plus Empfehlungsbericht senden**.

Nach dem Auswählen der Einstellungen klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

iDRAC-Servicemodul – Automatisches Versenden von Festplatten durch SupportAssist

Wenn der Server auf **PDR16 und PDR63** stößt, sendet der Dell EMC Support Ihnen E-Mails, die Sie über den vorhersehbaren Fehler oder einen ungültigen Festplattenblock auf einer SSD informieren, wenn dies durch die geltenden Lizenzbedingungen abgedeckt ist. Sobald Sie die E-Mail erhalten haben, müssen Sie dem Dell EMC Support eine Serviceadresse mitteilen, damit die versandten Teile geliefert werden können.

Aktivieren der In-Band-Funktion SNMP Get – Linux

Installieren und konfigurieren Sie das **net-snmp**-Paket, um SNMP-Anfragen von Remote-Systemen anzunehmen. Diese Funktion ist standardmäßig deaktiviert.

Zur Installation der In-Band-Funktion SNMP Get über das Installationsprogramm setup.sh führen Sie folgende Tasks aus:

1. Starten Sie die iSM-Installation über das Skript setup.sh, indem Sie `./setup.sh` in der Befehlszeile ausführen.
2. Lesen und akzeptieren Sie die Lizenzvereinbarung, um mit der Installation fortzufahren.
3. Auf der nächsten Seite wird eine Liste der Funktionen angezeigt. Wählen Sie die Option **Zugriff über SNMP Get** unter **iDRAC Zugriff per Host-BS** aus, geben Sie **4.c** ein und bestätigen Sie mit **Enter**.
4. Wenn diese Funktion aktiviert ist, starten Sie den Installationsablauf der ausgewählten Funktionen durch Eingabe von **I** und **Enter**.
5. Nachdem die Installation abgeschlossen ist, starten Sie den iDRAC-Servicemodul-Prozess.
   Wenn der SNMP-Agent nicht auf dem iDRAC aktiviert ist, konfiguriert und aktiviert iSM den SNMP-Agent.
6. Die Einstellungen für den SNMP-Agenten auf der iDRAC GUI finden Sie unter **Einstellungen**.
7. Klicken Sie auf **iDRAC-Servicemodul-Einrichtung**.
8. Unter **Monitoring** können Sie prüfen, ob die Option **SNMP Get über Hostbetriebssystem** aktiviert ist.
9. Öffnen Sie ein neues **PuTTY Konfiguration** Fenster, geben Sie Ihre Hostnamen-IP-Adresse ein und klicken Sie auf **Öffnen**.
10. Klicken Sie für **PuTTY Sicherheitshinweis** auf **Ja**.
11. Melden Sie sich mit den iDRAC-Anmeldeinformationen an.
12. Geben Sie `racadm get iDRAC.ServiceModule.HostSNMPGet` ein und drücken Sie die Eingabetaste.
    Stellen Sie sicher, dass **HostSNMPGet** aktiviert ist.

    ANMERKUNG: Wenn die In-Band-SNMP-Funktion während der iDRAC-Servicemodulinstallation nicht aktiviert wird, kann sie später über die iDRAC-Benutzeroberfläche oder den RACADM-Befehl aktiviert werden.

    - Über iDRAC-GUI: **iDRAC-Einstellungen ->Einstellungen ->iDRAC-Servicemodul einrichten ->Aktivieren von SNMP-Get über Hostbetriebssystem ->Aktivieren oder Deaktivieren**
    - Über RACADM: **racadm set idrac.servicemodule.HostSnmpGet "Enabled"oder "Disabled"**

    ANMERKUNG: iDRAC-Benutzeroberfläche oder RACADM-Befehle für die In-Band-SNMP-Funktion sind nur für PowerEdge-Server yx4x und yx5x verfügbar. Für yx3x-PowerEdge-Server müssen Sie den iSM-Installer verwenden, um die Funktion zu aktivieren und zu deaktivieren.

ANMERKUNG: Wenn die SNMP-Get-Funktion aktiviert ist, wird ein iDRAC-Konto **iSMSnmpUser** erstellt, sodass SNMPv3 intern unterstützt wird. Wenn das Konto bereits vorhanden ist, protokolliert iSM die Fehlermeldung **"iSMSnmpUser" kann nicht auf dem iDRAC erstellt werden, weil der Nutzername bereits existiert**. **Dann wird die Funktion SnmpGet über Hostbetriebssystem deaktiviert** und die Funktion wird deaktiviert. In solchen Fällen müssen Sie „iSMSnmpUser“ aus iDRAC entfernen und die Funktion zum **Aktivieren von SNMP-Get über Hostbetriebssystem** auf der iDRAC UI deaktivieren und erneut aktivieren. Das von iSM erstellte Konto „iSMSnmpUser“ wird gelöscht, sobald die Funktion deaktiviert ist oder iSM deinstalliert wird. Die Funktion „SNMP Get“ funktioniert nicht, wenn die maximale Anzahl von iDRAC-Konten (16) erstellt wurde und keine weiteren Plätze vorhanden sind.

Aktivieren der In-Band-SNMP-Get-Funktion – Windows

Durch die In-Band-SNMP-Get-Funktion können Sie die Systemmanagementdaten über den SNMP-Dienst auf dem Hostbetriebssystem abfragen. Als Voraussetzung für diese Funktion müssen die Host-SNMP-Dienste aktiviert und konfiguriert werden.

Der SNMP-Dienst auf dem iDRAC muss aktiviert werden. Falls er nicht aktiviert ist, aktiviert und konfiguriert das iDRAC-Servicemodul den SNMP-Dienst auf iDRAC. Diese Funktion kann von allen iDRAC Schnittstellen oder dem Installer aktiviert oder deaktiviert werden.

Diese Funktion unterstützt SNMP Version 1 und 2 für Microsoft Windows-Betriebssysteme und SNMP Version 1, 2 und 3 für Linux-Betriebssysteme.

ANMERKUNG: iDRAC-UI oder RACADM-Befehle für In-Band-SNMP-Get-Funktion gelten nur für PowerEdge-Server yx4x und höher.

ANMERKUNG: Das iDRAC-Servicemodul unterstützt nur iDRAC SNMP OID 1.3. 6.1. 4.1.674.10892.5.

iDRAC GUI Launcher

Wenn Sie iDRAC Servicemodul 3.1 oder höher verwenden, können Sie die iDRAC UI vom lokalen System aus starten. Doppelklicken Sie auf das Symbol für das **iDRAC GUI-Startprogramm**. Die iDRAC-UI-Anmeldeseite wird im Standardbrowser geöffnet. Verwenden Sie die iDRAC-Anmeldeinformationen für die Anmeldung auf der iDRAC-Startseite. Diese Funktion wird nur von Betriebssystemen von Microsoft Windows ausgeführt. Diese Tastenkombination ist nach der erfolgreichen Installation von iSM 3.1 oder höher im Startmenü verfügbar.

ANMERKUNG: Wenn das iSM deaktiviert ist, ist das Symbol für das iDRAC-GUI-Startprogramm ebenfalls deaktiviert.

ANMERKUNG: Wenn der Standard-Browserproxy so eingestellt ist, dass er den Systemproxy verwendet, wird ein Fehler beim Starten der iDRAC-GUI angezeigt. Sie müssen die IP-Adresse aus der Adressleiste kopieren und in die Ausnahmeliste der Proxyeinstellungen eintragen.

SSO (Single Sign-on) zur iDRAC-Benutzeroberfläche vom Administrator-Desktop des Hostbetriebssystems

Übersicht

Die Host-Administratoren können iDRAC über das Hostbetriebssystem über IPv6 starten. Das **iDRAC SSO-Startprogramm** erfordert eine Desktop-Umgebung des Hostbetriebssystems.

ANMERKUNG: Nicht-Administratoren können auf diese Funktion nicht auf dem Hostbetriebssystem zugreifen.

Die SSO-Funktion (Single Sign-On) ermöglicht es einem authentifizierten Betriebssystemadministrator, direkt auf die iDRAC-Webschnittstelle zuzugreifen, ohne dass eine Anmeldung über separate iDRAC-Administrator-Anmeldeinformationen erforderlich ist. Bei der Installation dieser Funktion wird auf Microsoft Windows-Betriebssystemen eine Verknüpfung in **Programme** mit dem Namen **Invoke-iDRACLauncher** erstellt. Auf Linux-Betriebssystemen erstellt iSM unter **Anwendungen** eine Verknüpfung, auf die der Nutzer doppelklicken und damit das iDRAC-Dashboard starten kann. iSM stellt auf Microsoft Windows-Betriebssystemen eine Befehlszeilenschnittstelle namens **Invoke-iDRACLauncher** und auf Linux-Betriebssystemen namens **Invoke-iDRACLauncher.sh** bereit.

Sie können das iDRAC-Servicemodul über die IPv6-Adresse konfigurieren. Standardmäßig erfolgt die Kommunikation über IPv4. Bei einem Ausfall wird ein Neustart der Kommunikation über IPv6 versucht. Eine Fehlermeldung wird geprüft, wenn die Kommunikation fehlschlägt.

Der Nutzer kann die IPv6-Adresse mit **RACADM-Passthrough-**Befehlen aktualisieren. Die Single-Sign-On-Funktion über IPv6 ist nur gültig, wenn IPv6 mit einer gültigen eindeutigen lokalen Adresse (ULA) konfiguriert ist. Beispiel:

```
fde1:53ba:e9a0:de12::/64
fde1:53ba:e9a0:de13::/64
fde1:53ba:e9a0:de14::/64
fde1:53ba:e9a0:de15::/64
fde1:53ba:e9a0:de16::/64
```

Nutzer können zwischen zwei Arten von Berechtigungen für die Anmeldung am iDRAC wählen.

- Konto **ohne Schreibzugriff**: Eine Express- oder Standardinstallation von iSM installiert das **iDRAC SSO-Startprogramm**, über das sich der Administrator als Konto **ohne Schreibzugriff** am iDRAC anmelden kann. Neben der Möglichkeit, den Zustand von Komponenten, Protokolle und Bestand anzuzeigen, ermöglicht dies auch einige zusätzliche **SupportAssist**-Operationen, die vom Servicepersonal benötigt werden.
- **Administratorkonto**: Die Installation dieser Funktion durch Auswahl der **Administratorberechtigung** ermöglicht es dem Administrator des Hostbetriebssystems, sich als Operator am iDRAC anzumelden. Mit diesem Konto können Sie alle Vorgänge durchführen, die ein iDRAC-Root-Nutzer durchführen kann, mit Ausnahme der Konfiguration und des Löschens von iDRAC-Nutzern und des Lifecycle-Protokolls.

ANMERKUNG: Hostbetriebssystemnutzer ohne Administratorrechte können das iDRAC-GUI-Startprogramm nicht aufrufen, wenn die iDRAC-Firmware-Version 4.00.00.00 oder höher ist und die Kommunikation zwischen iDRAC und iSM nicht über IPv4 erfolgt.

ANMERKUNG: Im *iDRAC 9-Benutzerhandbuch* finden Sie spezifische Berechtigungen, die einem Nutzerkonto *ohne Schreibzugriff* bzw. mit *Operatorrechten* gewährt werden.

Deaktivieren von Single Sign-On am iDRAC vom Hostbetriebssystem aus: Sie können diese Funktion auch vollständig **deaktivieren**. Wenn iSM durch Deaktivieren dieser Funktion installiert wird, ruft das **iDRAC GUI-Startprogramm** die iDRAC-Anmeldeseite mit dem Standardbrowser auf.

Invoke-iDRACLauncher ist vom iSM-Dienst unabhängig und kann auch aufgerufen werden, wenn iSM-Dienst angehalten wurde.

Wenn auf dem Hostbetriebssystem kein Browser installiert ist oder **Invoke-iDRACLauncher** den iDRAC aufgrund von Browserproblemen nicht starten kann, wird dennoch im iDRAC eine Sitzung erstellt. Mithilfe eines iDRAC-Administratorkontos können Sie sich beim iDRAC anmelden und die Sitzungen löschen.

Nachstehend finden Sie das Verhalten des iDRAC GUI-Startprogramms mit verschiedenen **Betriebssystem-zu-iDRAC-Passthrough**-Statusmeldungen:

- Wenn die Einstellung für **Betriebssystem-zu-iDRAC-Passthrough** im iDRAC deaktiviert ist, fragt **Invoke-iDRACLauncher**, ob Sie OSBMC-Passthrough im USBNIC-Modus aktivieren möchten.
- Wenn die Einstellung für **Betriebssystem-zu-iDRAC-Passthrough** bereits im LOM-Modus konfiguriert ist, startet das iDRAC-Startprogramm die iDRAC-GUI nicht.
- Wenn die Einstellung **Betriebssystem-zu-iDRAC-Passthrough** im iDRAC deaktiviert ist und **Lokale iDRAC-Konfiguration über Einstellungen deaktivieren** ebenfalls deaktiviert ist oder der Sperrmodus im iDRAC aktiviert ist, wird die iDRAC-GUI nicht gestartet.

  ANMERKUNG: Wenn **Lokale Konfiguration über Einstellungen** oder **Lokale Konfiguration über RACADM** auf dem iDRAC deaktiviert ist, wird der iDRAC-Anmeldebildschirm angezeigt.

Wenn eine iDRAC SSO-Sitzung auf dem Hostbetriebssystem aktiv ist, wird mit dem Schließen des zugehörigen Terminals auch der Browser mit der SSO-Sitzung geschlossen.

ANMERKUNG: Stellen Sie sicher, dass Sie das **iDRAC GUI-Startprogramm** über eine von der Benutzeroberfläche unterstützte und UI-fähige Oberfläche aufrufen. SSO über IPv4 funktioniert nicht, wenn Sie das dritte Oktett in der USB NIC IP-Adresse ändern. Diese Funktion mit IPv6 erfordert iDRAC9 Firmware 4.00.00.00 oder höher.

Voraussetzungen

Linux-Pakete:

1. Browser wie z. B. Mozilla Firefox
2. Sudo
3. PowerEdge-Server der yx4x Serie und höher
4. iDRAC-Firmware-Versionen 3.30.30.30 und höher

   ANMERKUNG: Die einmalige Anmeldung über IPv6 wird auf iDRAC Firmware-Version 4.00.00.00 und höher unterstützt.

Einschränkungen für Linux-Betriebssysteme

Es bestehen Einschränkungen des **iDRAC SSO-Startprogramms** auf Linux-Betriebssystemen, die Folgendes nicht unterstützen:

1. Desktop-Dienstprogramme außer GNOME
2. Browser außer Mozilla Firefox

ANMERKUNG: Wenn die lokale Konfiguration über KC oder RACADM in iDRAC deaktiviert ist, wird der iDRAC-Anmeldebildschirm angezeigt.

IPv6-Kommunikation zwischen iSM und iDRAC über Betriebssystem-BMC-Passthrough

Das iSM unterstützt sowohl IPv4 als auch IPv6 als Kommunikationsmodi. Nachdem Sie iSM installiert haben, versucht der iSM-Dienst, eine Verbindung zum iDRAC über die lokale IPv4-Link-Adresse herzustellen. Wenn die USBNIC-Schnittstelle des Hosts über keine IP-Adresse verfügt, versucht das iSM, die IPv4-Adresse hostseitig zu konfigurieren. Diese USBNIC-Schnittstellenkonfiguration auf dem Hostbetriebssystem wird von iSM nur einmal durchgeführt. iSM bleibt vom iDRAC getrennt, wenn die Konfiguration von USBNIC auf dem Hostbetriebssystem in weiterer Folge unvollständig ist. Falls die Verbindung auch nach Konfiguration der IPv4-Adresse fehlschlägt, versucht das iSM, sich über IPv6 mit dem iDRAC zu verbinden.

ANMERKUNG: Diese Funktion wird nur auf Linux-Betriebssystemen unterstützt.

ANMERKUNG: Wenn der IPv6-Netzwerkstapel auf dem Hostbetriebssystem deaktiviert ist, versucht iSM erneut, über IPv4 mit dem iDRAC zu kommunizieren.

Wenn eines der beiden Protokolle deaktiviert ist, versucht das iSM nicht, über das deaktivierte Protokoll eine Verbindung zum iDRAC herzustellen.

ANMERKUNG: Wenn die iDRAC-Firmware-Version IPv6 auf USBNIC nicht unterstützt, wird die Verbindung zwischen iSM und iDRAC über IPv4 hergestellt.

Entsprechende Überprüfungsmeldungen werden vom iSM protokolliert und geben die Protokollversion an, über die das iSM mit dem iDRAC verbunden ist.

ANMERKUNG: Wenn die iDRAC-USBNIC bereits nur mit IPv6-Adresse auf dem Hostbetriebssystem konfiguriert ist und iSM auf dem Host installiert ist, erfolgt die iSM-Kommunikation mit dem iDRAC sofort über das IPv4-Protokoll.

Nicht unterstützte Funktionen mit IPv6-Protokoll

Folgende Funktionen werden nicht unterstützt, wenn das iSM mit dem IPv6-Protokoll konfiguriert ist und die IPv4-Konfiguration auf der USBNIC-Schnittstelle nicht verfügbar ist:

- In-Band-iDRAC-Zugriff
- In-Band-SNMP-Get
- idrac.local und drac.local
- AutoUpdate von iSM

7

Häufig gestellte Fragen

In diesem Abschnitt werden einige häufig gestellte Fragen zum iDRAC-Servicemodul (iSM) beantwortet.

iSM-Kommunikation mit iDRAC-Switches von IPv4-Protokoll zu IPv6-Protokoll

Die iSM-Kommunikation mit iDRAC-Switches wechselt vom IPv4- zum IPv6-Protokoll, wenn Sie `ifconfig iDRAC down` ausführen und die iSM-Kommunikation mit dem iDRAC über IPv4 erfolgt.

Tabelle 15. Änderung des Protokolls, wenn Sie den Befehl ausführen

Funktion/Protokoll	IPv4 auf Linux	IPv4 auf Windows	IPv6 auf Linux	IPv6 auf Windows
BS-Informationen	Ja	Ja	Ja	Ja
WMI	k. A.	Ja	k. A.	Ja
SupportAssist	Ja	Ja	Ja	Ja
Invoke-iDRACLauncher	Ja	Ja	Ja	Ja
Invoke-iDRACHardReset	Ja	Ja	Ja	Ja
Invoke-VirtualPowerCycle	Ja	Ja	Ja	Ja
Host SNMP Get	Ja	Ja	Nein	Nein
In-Band SNMP-Traps	Ja	Ja	Ja	Ja
iDRAC SSO Launcher	Ja	Ja	Ja (ULA)	Ja (ULA)
Automatische Systemwiederherstellung	Ja	Ja	Ja	Ja
In-Band-iDRAC-Zugriff	Ja	Ja	Nein	Nein
iSM Auto-Update	Ja	Ja	Nein	Nein
NVMe-Vorbereitung zum Entfernen	Ja	Ja	Ja	Ja
Server-Speicher-Korrelation	Ja	Ja	Ja	Ja
S.M.A.R.T-Protokolle auf AHCI	Ja	Ja	Ja	Ja

Mehrere iDRAC-SSO-Sitzungen sind sowohl über IPv4- als auch über ULA-Adresse aktiv

Wenn der Nutzer die IPv4- oder ULA-Adresse im iSM ändert, werden mehrere Sitzungen erstellt. Die alte IP-Adresse wird schließlich gelöscht.

Problemumgehung: Löschen Sie die alte IP-Adresse manuell.

Muss ich vor der Installation oder Ausführung von iSM OpenManage Server Administrator deinstallieren?

Nein. Stellen Sie jedoch vor der Installation oder Ausführung des iSM sicher, dass Sie die Funktionen von OpenManage Server Administrator, die das iSM bereitstellt, gestoppt haben.

ANMERKUNG: Die Deinstallation von OpenManage Server Administrator ist nicht erforderlich.

Wie erkenne ich, ob das iSM auf meinem System ausgeführt wird?

So überprüfen Sie, ob das iSM auf Ihrem System installiert ist:

- Unter Windows:

  Führen Sie den Befehl `service.msc` aus. Suchen Sie in der Liste der Dienste den Dienst mit der Bezeichnung **DSM iDRAC-Servicemodul**.

- Unter Linux:

  Führen Sie den Befehl `/etc/init.d/dcismeng status` aus. Wenn iSM installiert ist und ausgeführt wird, wird der Status **wird ausgeführt** angezeigt.

ANMERKUNG: Verwenden Sie den Befehl `systemctl status dcismeng.service` anstelle des Befehls `init.d`, um zu überprüfen, ob das iSM auf den Betriebssystemen Red Hat Enterprise Linux oder SUSE Linux installiert ist.

Wie kann ich feststellen, welche Version des iSM auf meinem System installiert ist?

Um die im System vorhandene Version des iSM herauszufinden, klicken Sie auf **Start** > **Systemsteuerung** > **Programme und Funktionen**. Die Version des installierten iSM wird auf der Registerkarte **Version** angegeben. Sie können die Version auch überprüfen, indem Sie **Arbeitsplatz** > **Programm deinstallieren oder ändern** aufrufen.

Führen Sie auf dem Betriebssystem Linux den folgenden Befehl aus:

```
rpm -qa | grep dcism
```

Führen Sie auf dem Betriebssystem VMware ESXi den folgenden Befehl aus:

```
esxcli software vib list --vibname=dcism
```

Welche Berechtigungsebene muss ein Nutzer mindestens haben, um das iSM zu installieren?

Zum Installieren des iSM müssen Sie über Administratorrechte im Betriebssystem verfügen.

Wenn ich versuche, das iSM zu installieren, wird folgende Fehlermeldung angezeigt: Dies ist kein unterstützter Server. Was soll ich tun?

Stellen Sie vor der Installation des iSM sicher, dass der Server oder das System, auf dem das iSM installiert werden soll, ein PowerEdge-Server yx2x oder höher ist. Stellen Sie außerdem sicher, dass Sie über ein 64-Bit-System verfügen.

Die Meldung Das iSM kann nicht mit iDRAC über den Betriebssystem-zu-iDRAC-Passthrough-Kanal kommunizieren ist in der Betriebssystem-Protokolldatei, selbst wenn das Betriebssystem-zu-iDRAC-Passthrough über USBNIC ordnungsgemäß konfiguriert ist. Warum erhalte ich diese Meldung?

iSM nutzt das Betriebssystem zum iDRAC-Passthrough über USBNIC, um die Kommunikation mit dem iDRAC herzustellen. Gelegentlich kann es vorkommen, dass die Kommunikation nicht hergestellt werden kann, obwohl die USBNIC-Endpunkte mit korrekter IP-Schnittstelle konfiguriert sind. Dies kann eintreten, wenn die Routing-Tabelle des Host-Betriebssystems mehrere Einträge für dieselbe Zielmaske aufweist und das USBNIC-Ziel nicht als erstes Ziel in der Routing-Reihenfolge aufgelistet ist.

Tabelle 16. Details zur Routing-Reihenfolge

Ziel	Gateway	Genmask	Flags	Metrik	Ref.	Iface verwenden
Standardeinstellung	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	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 enp0s20u12u3

In diesem Beispiel ist **enp0s20u12u3** die USBNIC-Schnittstelle. Die Link-Local-Zielmaske wird wiederholt und der USBNIC ist nicht der erste auf der Liste. Dies führt zu dem Konnektivitätsproblem zwischen dem iSM und iDRAC über Betriebssystem-zu-iDRAC-Passthrough. Um das Konnektivitätsproblem zu beheben, stellen Sie sicher, dass die iDRAC-USBNIC-IPv4-Adresse (die Standardeinstellung lautet 169.254.1.1) über das Hostbetriebssystem erreichbar ist. Wenn sie vom Hostbetriebssystem aus nicht erreichbar ist, führen Sie einen der folgenden Schritte aus:

- Ändern Sie die iDRAC-USBNIC-Adresse auf einer eindeutigen Ziel-Maske.
- Löschen Sie die ungewünschten Einträge aus der Routing-Tabelle, um sicherzustellen, dass USBNIC als die Route ausgewählt wird, sobald der Host die iDRAC-USBNIC-IPv4-Adresse erreichen möchte.

Wenn ich versuche, das iSM zu installieren, wird die folgende Fehlermeldung angezeigt: Dieses Betriebssystem wird nicht unterstützt.

iSM kann nur auf unterstützten Betriebssystemen installiert werden. Informationen zu den unterstützten Betriebssystemen finden Sie unter Unterstützte Betriebssysteme.

Ich habe die Remote-iDRAC-Hardware-Reset-Funktion verwendet, um den iDRAC zurückzusetzen. Das IPMI reagiert jedoch nicht, und ich bin nicht in der Lage, das Problem zu beheben.

Wenn Sie versuchen, die Remote-iDRAC-Hardware-Reset-Funktion auf dem **Betriebssystem VMware ESXi** anzuwenden, reagieren die IPMI-Treiber nicht mehr und daher wird die iSM-Kommunikation angehalten. Möglicherweise müssen Sie den Server neu starten und den IPMI-Treiber erneut laden, um das Problem zu beheben.

Wo finde ich das replizierte Lifecycle-Protokoll auf meinem Betriebssystem?

So zeigen Sie die replizierten Lifecycle-Protokolldateien an:

Tabelle 17. Betriebssystem und Standort

Betriebssystem	Speicherort
Microsoft Windows	**Ereignisanzeige** > **Windows-Protokolle** > ***<Bestehenden Gruppe oder Benutzerdefinierter Ordner>***. Alle iSM-Lifecycle-Protokolle werden unter dem Quellnamen **iDRAC-Servicemodul** repliziert.
Red Hat Enterprise Linux und SUSE Linux	**/var/log/messages**
VMware ESXi	**/var/log/syslog.log**
Ubuntu	**/var/log/syslog**

Was ist das Standard-SNMP-Protokoll, das im iSM für das Versenden von Warnmeldungen in Linux-Betriebssystemen konfiguriert ist?

Standardmäßig ist das SNMP-Multiplexing-Protokoll (SMUX) im iSM zum Senden von Warnmeldungen konfiguriert.

SMUX wird auf meinem System nicht unterstützt. Welches Protokoll sollte ich für das Versenden von Warnmeldungen konfigurieren?

Wenn SMUX auf dem System nicht unterstützt wird, wird Agent-x als Standard-Protokoll verwendet.

Wie konfiguriere ich das iSM zur Verwendung des Agent-x-Protokolls zum standardmäßigen Senden von Warnmeldungen?

Sie können Agent-x als Standardprotokoll konfigurieren, indem Sie den Befehl `./Enable-iDRACSNMPTrap.sh 1/agentx –force` verwenden. Wenn –force nicht angegeben ist, stellen Sie sicher, dass die net-SNMP konfiguriert ist und starten den snmpd-Dienst neu.

Welche abhängigen Linux-Pakete oder ausführbaren Dateien sollte ich im Rahmen der Linux-Installation ebenfalls installieren?

Eine Liste der abhängigen Linux-Pakete finden Sie unter Linux-Abhängigkeiten.

Ich habe einen benutzerdefinierten Ordner in der Windows-Ereignisanzeige erstellt, die Lifecycle-Protokolldateien werden jedoch nicht in meinem benutzerdefinierten Ordner repliziert. Was muss ich tun, damit die Lifecycle-Protokolldateien repliziert werden?

Stellen Sie sicher, dass Sie die Windows-**Ereignisanzeige** nach der Erstellung des benutzerdefinierten Ordners schließen. Öffnen Sie die Windows-**Ereignisanzeige** erneut, um die replizierten Lifecycle-Protokolldateien anzuzeigen.

Ich habe mich für die benutzerdefinierte Installationsoption über die grafische Benutzeroberfläche im Rahmen der Installation des iSM entschieden und habe eine Funktion deaktiviert, aber ich bin nicht in der Lage, diese Funktion über die anderen Oberflächen zu aktivieren. Wie kann ich diese Funktion erneut aktivieren?

Bei Systemen mit Microsoft Windows kann eine Funktion, die Sie über das Installationsprogramm aktiviert und über eine andere Oberfläche als das Installationsprogramm deaktiviert haben, nur über die gleiche Oberfläche oder das Installationsprogramm im Modus der grafischen Benutzeroberfläche aktiviert werden.

Beispielsweise können Sie eine Funktion, die während der iSM-Installation über die grafische Benutzeroberfläche deaktiviert wurde, nicht etwa mithilfe der RACADM CLI-Befehle aktivieren.

Ich kann über das Hostbetriebssystem als Active-Directory-Nutzer über LDAP nicht auf die iDRAC-Seite zugreifen. Ich habe versucht, über das Hostbetriebssystem auf die iDRAC-Seite zuzugreifen. Es wird jedoch eine Fehlermeldung angezeigt, dass die Seite nicht aufgerufen werden kann. Wie kann ich das Problem beheben?

Wenn Sie versuchen, über das Hostbetriebssystem auf die iDRAC-Seite zuzugreifen, wird ggf. eine Fehlermeldung angezeigt, dass die Seite nicht aufgerufen werden kann. Stellen Sie sicher, dass das iDRAC-Netzwerk so konfiguriert ist, dass die Authentifizierung als LDAP-Benutzer zulässig ist. Sie können sich entweder als lokaler Nutzer oder als Gast anmelden.

Ich erhalte keinen Zugriff auf die iDRAC-Seite über das Hostbetriebssystem, nachdem ich iDRAC auf die Werkseinstellungen zurückgesetzt habe, z. B. mit `racadm racresetcfg`. Wie kann ich das Problem beheben?

Stellen Sie sicher, dass der Betriebssystem-zu-iDRAC-Passthrough-Kanal aktiviert ist. Standardmäßig ist dies im Werksmodus deaktiviert. Wenn Sie den Betriebssystem-zu-iDRAC-Passthrough-Kanal aktivieren möchten, nutzen Sie dafür folgenden Befehl: `racadm set idrac.os-bmc.adminstate 1`.

Ich sehe 169.254.0.2 als die Quell-IP-Adresse in über das iSM empfangenen iDRAC-SNMP-Traps. Wie kann ich das Problem beheben?

Auf Linux-Betriebssystemen zeigen die über das Hostbetriebssystem empfangenen iDRAC-SNMP-Traps den Hostnamen oder die Quell-IP-Adresse als 169.254.0.2 statt des tatsächlichen Namens des Hostbetriebssystems oder der IP-Adresse an. Das Betriebssystem legt fest, wie der Eintrag vor der Trap-Ausgabe an den Nutzer befüllt wird.

Ich habe mein Betriebssystem für iDRAC-zu-LOM-Passthrough konfiguriert, und wenn ich versuche, dcism-sync auszuführen, schlägt der Updatevorgang fehl. Was kann ich tun?

Das Betriebssystem-zu-iDRAC-Passthrough muss für die Verwendung des USB-NIC-Modus konfiguriert sein. Dies ist eine Voraussetzung für Installation und Update des iSM.

Ich kann die Funktion WMIInfo des iSM auf den Betriebssystemen Linux und VMware ESXi mittels RACADM- und WSMan-Befehlen aktivieren oder deaktivieren. Hat das Auswirkungen auf meine iSM-Konfiguration auf dem Hostbetriebssystem?

Die Funktion WMIInfo des iSM ist nur für Microsoft Windows-Betriebssysteme verfügbar. Das Aktivieren bzw. Deaktivieren dieser Funktion von einer der iDRAC-Schnittstellen auf einem anderen Betriebssystem als Microsoft Windows hat keinen Einfluss auf die iSM-Konfiguration auf dem Host-Betriebssystem.

Wenn ich die IP-Adresse der USBNIC-Schnittstelle auf dem Hostbetriebssystem lösche, kann das iSM nicht mit dem iDRAC kommunizieren.

Der iSM konfiguriert die USBNIC-Schnittstelle des Hostbetriebssystems nur einmal. Wenn Sie später die USBNIC-Schnittstelle auf dem Hostbetriebssystem deaktivieren, indem Sie die IP-Adresse löschen, die Verbindung zur Schnittstelle unterbrechen oder die IPV4- oder IPV6-Adresse auf dieser Schnittstelle deaktivieren, behält das iSM die Nutzerkonfiguration bei und überschreibt die Schnittstelleneinstellungen nicht. Um die Kommunikation zwischen iSM und iDRAC wiederherzustellen, starten Sie den iSM-Dienst auf dem Hostbetriebssystem neu.

Nach der Installation von iSM mit der Stapeldatei ISM_Win.BAT von der vom iDRAC freigegebenen logischen Partition „SMINST“ unter dem Betriebssystem Microsoft Windows wird eine Konsolenmeldung angezeigt: „Das System kann die angegebene Datei nicht finden.“

Nach dem iSM erfolgreich installiert wurde, wird die Bereitstellung der logischen Partition **SMINST** vom Host-Betriebssystem aufgehoben. Diese Meldung wird angezeigt, wenn der BAT aus aufgerufen wird von der **SMINST** Partition liegen. Die Installation erfolgreich war. Es sind keine weiteren Schritte des Benutzers erforderlich.

Wenn unter dem Betriebssystem Ubuntu abhängige Pakete für iSM nicht vorhanden sind, wird bei der Installation über das Betriebssystem-DUP iSM im Zustand „installieren+entpacken“ installiert.

Sie können dies überprüfen Sie folgenden Befehl eingeben:

```
#dpkg -s dcism
```

```
Package: dcism
```

`Status: install ok unpacked`

Um dieses Problem zu beheben, führen Sie den Befehl `apt-get install -f`. Dies installiert abhängiger Pakete initialisiert.

Wenn ich iSM 3.4.0 oder höher auf Linux-Betriebssystemen wie Red Hat Enterprise Linux installiere, sehe ich einige Meldungen in Betriebssystemprotokollen wie *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*.

Die Meldungen beziehen sich auf den GNOME-Desktop-Manager. Verschiedene Betriebssystemgruppen verfügen über Bugzilla-Elemente, um diese Situation zu beheben. Zum Beispiel: https://bugzilla.redhat.com/show_bug.cgi?id=1594177. Es sind keine weiteren Schritte des Benutzers erforderlich.

Wenn ich auf die Verknüpfung *iDRAC GUI-Startprogramm* unter Menü > Zubehör klicke, wird auf dem Betriebssystem Red Hat Enterprise Linux ein leeres Terminal angezeigt.

Die Anzeige von Text auf dem Terminal hängt von der GNOME-Version auf dem installierten Betriebssystem ab. Eine Alternative ist das Ausführen des Startprogramms über eine UI-fähige Shell. Zum Beispiel: `bash#> sh /opt/dell/srvadmin/iSM/bin/iDRACLauncher.sh` als Sudo-Nutzer.

Falls der Betriebssystem-zu-iDRAC-Passthrough im iDRAC deaktiviert ist, sehen Sie ein leeres Terminal, wenn die iDRAC-Benutzeroberfläche von Linux-Betriebssystemen wie Red Hat Enterprise Linux 7.6 und Red Hat Enterprise Linux 8.0 aus gestartet wird. Geben Sie **j** oder **J** ein und drücken Sie die **Eingabetaste**, um die Konfiguration der USBNIC-Schnittstelle auf dem Hostbetriebssystem anzuzeigen.

Alternativ können Sie das Betriebssystem-zu-iDRAC-Passthrough im iDRAC im USBNIC-Modus aktivieren und das iDRAC-Startprogramm vom Hostbetriebssystem aus erneut ausführen.

8

Linux und Ubuntu Installationspakete

Nachfolgend finden Sie die Installationspakete für die unterstützten Linux- und Ubuntu-Betriebssysteme:

Tabelle 18. Linux-Installationspakete

Linux-Betriebssystem wird unterstützt.	Installationspaket
Red Hat Enterprise Linux 7	`SYSMGMT\iSM\linux\RHEL7\x86_64\dcism-3.6.0-<bldno>.el7.x86_64.rpm`
Red Hat Enterprise Linux 8	`SYSMGMT\iSM\linux\RHEL8\x86_64\dcism-3.6.0-<bldno>.el8.x86_64.rpm`
Ubuntu 20	`SYSMGMT\iSM\linux\Ubuntu18\x86_64\dcism-3.6.0-<bldno>.ubuntu20.deb`
SUSE Linux Enterprise Server 15	`SYSMGMT\iSM\linux\SLES15\x86_64\dcism-3.6.0-<bldno>.sles15.x86_64.rpm`

ANMERKUNG: Sie können alle aufgelisteten Red Hat Enterprise Linux-Installationspakete verwenden, um iSM auf CentOS zu installieren.

9

Ressourcen und Support

Weitere Informationen zu den Funktionen dieser Version finden Sie in der Dokumentation zum iSM 3.6.0.

Zuletzt veröffentlichte Dokumente

So greifen Sie auf die neueste Version der iSM-Dokumente zu:

1. Gehen Sie zu **www.dell.com/ismmanuals**.
2. Klicken Sie auf die Version des iDRAC-Servicemoduls.
3. Klicken Sie auf **Handbücher und Dokumente**.

Zugreifen auf Dokumente mithilfe von direkten Links

Tabelle 19. Direkte Links für Dokumente

URL	Produkt
Www.dell.com/idracmanuals	iDRAC und Lifecycle Controller
Www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
unter www.dell.com/esmmanuals	Unternehmens-Systemmanagement
www.dell.com/ServiceabilityTools	Betriebsfähigkeitstools
Www.dell.com/omconnectionsclient	Client-Systemmanagement

Zugriff auf Dokumente über die Produktsuche

1. Gehen Sie zu **www.dell.com/support**.
2. In der **Geben Sie eine Service-Tag -Nummer, Seriennummer ...** Suchfeld, geben Sie den Produktnamen an. Zum Beispiel PowerEdge oder iDRAC. Eine Liste von NAS-Clustern wird angezeigt.
3. Wählen Sie Ihr Produkt und klicken Sie auf das Suchsymbol oder drücken Sie die Eingabetaste.
4. Klicken Sie auf **Handbücher und Dokumente**.

Zugriff auf Dokumente über die Produktauswahl

Sie können auch Dokumente zugreifen indem Sie Ihr Produkt aus.

1. Gehen Sie zu **www.dell.com/support**.
2. Klicken Sie auf **Alle Produkte durchsuchen**.
3. Klicken Sie auf die gewünschte Produktkategorie, z. B. Server, Software, Storage usw.
4. Klicken Sie auf das gewünschte Produkt und anschließend auf die gewünschte Version, falls zutreffend.

   ANMERKUNG: Für einige Produkte müssen Sie durch die Unterkategorien navigieren.
5. Klicken Sie auf **Handbücher und Dokumente**.

Themen:

- Identifizieren der Serie Ihrer Dell EMC PowerEdge-Server

Identifizieren der Serie Ihrer Dell EMC PowerEdge-Server

Die PowerEdge-Serverserie von Dell EMC ist basierend auf ihrer Konfiguration in verschiedene Kategorien unterteilt. Sie werden bezeichnet als Serien YX2X, YX3X, YX4X, YX4XX oder YX5XX der Server bezeichnet. Die Struktur der Namenskonvention wird nachfolgend beschrieben:

Der Buchstabe Y steht für die Buchstaben in der Server-Modellnummer. Die Buchstaben geben den Formfaktor des Servers an. Die Formfaktoren werden nachfolgend beschrieben:

- C – Cloud
- F – Flexibel
- M oder MX – Modular
- R – Rack
- T – Tower

Der Buchstabe X steht für die Ziffern in der Server-Modellnummer. Die Ziffern kennzeichnen mehrere Eigenschaften des Servers. Sie sind wie folgt aufgeführt:

- Das erste Zeichen (X) gibt den Wertestrom oder die Klasse des Servers an.
  - 1–5 – iDRAC basic
  - 6–9 – iDRAC Express
- Die zweite Ziffer steht für die Generation des Servers. Sie wird in der Server-Namenskonvention beibehalten und nicht durch den Buchstaben X ersetzt.
  - 0 – Serie 10
  - 1 – Serie 11
  - 2 – Serie 12
  - 3 – Serie 13
  - 4 – Serie 14
  - 5 – Serie 15
- Das letzte Zeichen (X) steht immer für die Bauart des Prozessors, wie nachfolgend beschrieben:
  - 0 – Intel
  - 5 – AMD

ANMERKUNG: Bei Servern, die einen AMD-Prozessor verwenden, besteht die Modellnummer aus vier Zeichen statt drei. Das dritte Zeichen (X) gibt die Anzahl der Prozessorsockel an, die von einer Serverserie unterstützt wird.

- 1 Server mit einem Sockel
- 2 Server mit zwei Sockeln

Tabelle 20. Benennungskonvention für PowerEdge-Server und Beispiele

YX3X-Server	YX4X-Systeme	YX4XX Systeme	YX5XX
PowerEdge M630	PowerEdge M640	PowerEdge R6415	PowerEdge R6515
PowerEdge M830	PowerEdge R440	PowerEdge R7415	PowerEdge R7515
PowerEdge T130	PowerEdge R540	PowerEdge R7425	PowerEdge R6525

10

Kontaktaufnahme mit Dell EMC

Dell EMC bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. Informationen zur Kontaktaufnahme mit Dell EMC für den Verkauf, den technischen Support und den Kundendienst erhalten Sie unter www.dell.com/contact.

Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Produktkatalog.