Dell EMC iDRAC Service Module 4.1.0.0

Guide de l'utilisateur

Décembre 2021
Rév. A04

DELL Technologies

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Table des matières

1

Introduction

L'iDRAC Service Module (iSM) est un module logiciel léger que vous pouvez installer sur les serveurs PowerEdge yx2x ou versions ultérieures. L'iSM complète les interfaces de l'iDRAC suivantes avec des données de surveillance supplémentaires : interface utilisateur (UI), interface de ligne de commande RACADM, Redfish et Web Services-Management (WS-Man). Vous pouvez configurer les fonctionnalités de l'iSM depuis le système d'exploitation pris en charge selon les fonctionnalités que vous installez et des besoins d'intégration uniques de votre environnement.

Sujets :

Nouveautés de cette version

Derniers systèmes d'exploitation pris en charge

L'iDRAC Service Module 4.1.0.0 prend en charge les systèmes d'exploitation suivants :

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8.5
- Red Hat Enterprise Linux 8.4
- SUSE Linux Enterprise Server 15 SP3
- Ubuntu Server 20.04.2 LTS
- VMware vSphere ESXi 7.0 U3

L'iDRAC Service Module 4.1.0.0 prend en charge les nouveaux systèmes d'exploitation clients suivants sur Dell EMC Precision R7920 :

- Red Hat Enterprise Linux 8
- Microsoft Windows 10
- Microsoft Windows 11 Professionnel
- Ubuntu Desktop 20.04 LTS

Fonctionnalités nouvelles et améliorées

Vous trouverez ci-dessous les nouvelles fonctionnalités et améliorations de l'iDRAC Service Module 4.1.0.0 :

- Mappage des alertes SNMP OMSA : l'iSM peut désormais envoyer des traps SNMP depuis le système d'exploitation hôte au format OMSA lorsque cette fonctionnalité est activée.
- Yellowdog Updater, Modified (YUM) : les administrateurs système peuvent déployer l'iSM à l'aide de l'outil YUM pour les systèmes d'exploitation Red Hat Enterprise Linux. Le référentiel YUM de Dell est mis à jour avec de nouveaux artefacts lorsqu'une nouvelle version est publiée.
- Mise à jour améliorée des règles de pare-feu de l'iDRAC Service Module sur les systèmes d'exploitation Linux : des règles de pare-feu supplémentaires concernant l'iSM ont été ajoutées pour faciliter la communication ininterrompue entre l'iSM et l'iDRAC.
- Amélioration de l'opération iDRACHardReset sur les systèmes d'exploitation VMware ESXi : l'opération iDRACHardReset est prise en charge lorsque l'option Secure Boot est activée dans le BIOS.
- Support enhanced du mode de verrouillage normal sur les systèmes d'exploitation VMware ESXi 7.x avec des privilèges d'administration.

Pour plus d'informations, reportez-vous à la section Mode de verrouillage VMware ESXi.

- Amélioration des performances pour l'établissement de la communication iSM avec l'iDRAC sur les systèmes d'exploitation VMware ESXi.

Matrice des fonctionnalités prises en charge par le système d'exploitation

Les fonctionnalités suivantes sont prises en charge sur les serveurs PowerEdge yx2x, yx3x, yx4x et yx5x :

Tableau 1. Fonctionnalités prises en charge par chaque système d'exploitation pris en charge

Fonctionnalités	Serveurs	Systèmes d'exploitation		
	Séries PowerEdge prises en charge	Microsoft Windows (notamment les systèmes HyperV)	Linux	Virtualisation (VMware ESXi)
Partage des informations sur le système d'exploitation	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Réplication du journal Lifecycle Controller	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Récupération automatique du système/surveillance	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Fournisseurs WMI (Windows Management Instrumentation)	yx2x, yx3x, yx4x, yx5x	Oui	S/O	S/O
Préparation au retrait du périphérique NVMe par le biais de l'iDRAC.	yx3x, yx4x, yx5x	Oui	Oui	Oui
Collecte SupportAssist à partir d'un système d'exploitation hôte	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Données de système d'exploitation et d'application	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui (uniquement pour les serveurs PowerEdge yx4x et versions ultérieures)
Réinitialisation matérielle d'iDRAC à distance	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui (l'utilitaire de ligne de commande est pris en charge uniquement sur VMware ESXi 7.x)
l'accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte	yx2x, yx3x, yx4x, yx5x	Oui	Oui	S/O
Prise en charge intrabande des alertes SNMP de l'iDRAC	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Prise en charge de la surveillance de l'interface réseau par l'intermédiaire du client Redfish	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui

Tableau 1. Fonctionnalités prises en charge par chaque système d'exploitation pris en charge (suite)

Fonctionnalités	Serveurs	Systèmes d'exploitation		
	Séries PowerEdge prises en charge	Microsoft Windows (notamment les systèmes HyperV)	Linux	Virtualisation (VMware ESXi)
Activation à distance de WS-Man.	yx2x, yx3x, yx4x, yx5x	Oui	S/O	S/O
Cycle d'alimentation complet (FullPowerCycle)	yx4x, yx5x	Oui	Oui	VMware ESXi 7.x : oui
SNMP intrabande Get	yx2x, yx3x, yx4x, yx5x	Oui	Oui	S/O
Installation Live VIB	yx3x, yx4x, yx5x	S/O	S/O	Oui
SupportAssist : rapport de collecte anonyme	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Lanceur de l'interface utilisateur de l'iDRAC	yx3x, yx4x, yx5x	Oui	Oui	S/O
Prise en charge d'IPv6	yx3x, yx4x, yx5x	Oui	Oui	S/O
Envoi automatique pour événements sélectifs	yx4x, yx5x	Oui	Oui	Oui
Collecte SupportAssist avec informations identifiables publiquement (PII) sélectives	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui
Authentification unique (SSO, Single Sign-On)	yx4x, yx5x	Oui	Oui	S/O
Mise à jour automatique de l'installation d'iSM	yx4x, yx5x	Oui	Oui	S/O
Corrélation entre les serveurs de stockage (S2D)	yx3x, yx4x, yx5x	Oui	S/O	S/O
Surveillance S.M.A.R.T en mode AHCI	yx3x, yx4x, yx5x	Oui	Oui	Oui
Surveillance S.M.A.R.T en mode RAID logiciel	yx3x, yx4x, yx5x	Oui	S/O	S/O
Mappage des alertes SNMP OMSA	yx2x, yx3x, yx4x, yx5x	Oui	Oui	Oui

N/A - Non applicable

Plateformes prises en charge

iDRAC Service Module 4.1.0.0 prend en charge les serveurs PowerEdge de génération yx2x à yx5x. Pour en savoir plus, voir le document Identification de la série de vos serveurs Dell EMC PowerEdge.

Tableau 2. Plates-formes prises en charge par l'iDRAC Service Module 4.1.0.0.

Serveurs Dell EMC PowerEdge pris en charge			
Serveurs PowerEdge yx5x	**Serveurs PowerEdge yx4x**	**Serveurs PowerEdge yx3x**	**Serveurs PowerEdge yx2x**
PowerEdge C6520	PowerEdge C6420	PowerEdge C4130	PowerEdge FM120
PowerEdge C6525	PowerEdge FC640	PowerEdge C6320	PowerEdge M420
PowerEdge MX750c	PowerEdge FD332	PowerEdge FC430	PowerEdge M520
PowerEdge R250	PowerEdge M640	PowerEdge FC630	PowerEdge M620
PowerEdge R350	PowerEdge M640-VRTX	PowerEdge FC830	PowerEdge M820
PowerEdge R450	PowerEdge MX740c	PowerEdge M630	PowerEdge R220
PowerEdge R550	PowerEdge MX840c	PowerEdge M630-VRTX	PowerEdge R320
PowerEdge R650	PowerEdge R240	PowerEdge M830	PowerEdge R420
PowerEdge R650XS	PowerEdge R340	PowerEdge R230	PowerEdge R620
PowerEdge R6515	PowerEdge R440	PowerEdge R330	PowerEdge R720
PowerEdge R6525	PowerEdge R540	PowerEdge R430	PowerEdge R720XD
PowerEdge R750	PowerEdge R640	PowerEdge R530	PowerEdge R820
PowerEdge R750xa	PowerEdge R6415	PowerEdge R630	PowerEdge R920
PowerEdge R750XS	PowerEdge R740	PowerEdge R730	PowerEdge T320
PowerEdge R7515	PowerEdge R740xd	PowerEdge R730xd	PowerEdge T420
PowerEdge R7525	PowerEdge R740xd2	PowerEdge R830	PowerEdge T620
PowerEdge T150	PowerEdge R7415	PowerEdge R930	
PowerEdge T350	PowerEdge R7425	PowerEdge T130	
PowerEdge T550	PowerEdge R840	PowerEdge T330	
PowerEdge XR11	PowerEdge R940	PowerEdge T430	
PowerEdge XR12	PowerEdge R940xa	PowerEdge T630	
PowerEdge XE8545	PowerEdge T140		
	PowerEdge T340		
	PowerEdge T440		
	PowerEdge T640		
	PowerEdge XE7420		
	PowerEdge XE7440		

Coexistence d'OpenManage Server Administrator et de l'iDRAC Service Module

OpenManage Server Administrator (OMSA) et l'iDRAC Service Module (iSM) peuvent coexister sur un seul système. Si vous activez les fonctionnalités de surveillance lors de l'installation de l'iSM et, une fois l'installation terminée, si l'iSM détecte la présence d'OMSA, l'iSM désactive les fonctionnalités de réplication du journal Lifecycle et de récupération automatique du système qui se chevauchent. Si le service OMSA s'arrête, les fonctionnalités de l'iSM qui avaient été désactivées sont activées.

REMARQUE : Les fonctions qui se chevauchent sont la **Récupération automatique du système** et la **Réplication du journal Lifecycle**.

Disponibilité du logiciel

Le logiciel iDRAC Service Module est disponible aux emplacements suivants :

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

Téléchargement de l'iSM

Pour télécharger l'iSM :

1. Rendez-vous sur Dell.com/support.
2. Sur le site de support, cliquez sur **Parcourir tous les produits** > **Logiciel** > **Gestion des systèmes Enterprise** > **Gestion des systèmes Enterprise à distance** > **iDRAC Service Module** > **iDRAC Service Module - versions actuelles** > **Pilotes et téléchargements**.

Accès au contenu de support à partir du site de support Dell EMC

Accédez au contenu de support lié à un ensemble d'outils de gestion de systèmes à l'aide de liens directs, en accédant au site de support Dell EMC, ou à l'aide d'un moteur de recherche.

- Liens directs :
  - Pour la gestion des systèmes Dell EMC Enterprise et la gestion à distance des systèmes Dell EMC Enterprise à distance :https://www.dell.com/esmmanuals
  - Pour les solutions de virtualisation Dell EMC :www.dell.com/virtualizationsolutions
  - Pour Dell EMC OpenManage :https://www.dell.com/openmanagemanuals
  - Pour iDRAC :https://www.dell.com/idracmanuals
  - Pour la gestion des systèmes Dell EMC OpenManage Connections Enterprise :https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les outils facilitant la maintenance Dell EMC :https://www.dell.com/serviceabilitytools
- Site de support Dell EMC :
  1. Rendez-vous sur https://www.dell.com/support.
  2. Cliquez sur **Parcourir tous les produits**.
  3. Sur la page **Tous les produits**, cliquez sur **Logiciel** et cliquez sur le lien requis.
  4. Cliquez sur le produit requis, puis sur la version requise.

À l'aide des moteurs de recherche, saisissez le nom et la version du document dans la zone de recherche.

Autres documents utiles

Vous trouverez des informations sur la configuration de la sécurité de l'iSM ainsi que des informations sur l'utilisation de l'iDRAC, de RACADM, de DUP, des messages d'événement et des services Web Dell Lifecycle Controller 2 sur le site Dell.com/support.

- Le *Guide de configuration de la sécurité de l'iDRAC Service Module* fournit les configurations de sécurité relatives à l'iDRAC Service Module (iSM).
- Le document *Guide de l'utilisateur de l'iDRAC* fournit des informations détaillées sur la configuration et l'utilisation de l'iDRAC.
- Le document *Guide de l'utilisateur de l'utilitaire RACADM de l'iDRAC* fournit des informations sur l'utilisation de l'utilitaire de ligne de commande RACADM.
- Le manuel *Guide de l'utilisateur Dell Update Package* fournit des informations sur l'obtention et l'utilisation des packages DUP dans le cadre de la stratégie de mise à jour de votre système.
- Le document *Guide de référence des messages d'événement Dell* fournit des informations sur les événements et les erreurs générés par le firmware et d'autres agents qui surveillent les composants du système.
- Le document *Guide de l'interface des services Web Dell Lifecycle Controller 2* fournit des informations et des exemples d'utilisation du protocole Web Services for Management (WS-Man).

Contrat de licence du logiciel

La licence logicielle des versions prises en charge du système d'exploitation de l'iSM se trouve dans le programme d'installation. Consultez le fichier `license_agreement.txt`. En installant ou en copiant un ou plusieurs fichiers du support, vous acceptez les conditions du fichier `license_agreement.txt`.

2

Configuration de préinstallation

Avant d'installer iDRAC Service Module (iSM) :

- Accédez aux serveurs PowerEdge yx2x ou versions ultérieures. Pour obtenir la liste des plateformes prises en charge, voir Plateformes prises en charge.
- Vérifiez que vous disposez de privilèges d'administration.
- Lisez les instructions d'installation du système d'exploitation.
- Lisez les notes de mise à jour applicables et *la matrice de support logiciel des systèmes*.
- Consultez la configuration requise pour l'installation afin de vous assurer que votre système satisfait la configuration minimale requise.
- Fermez toutes les applications qui s'exécutent sur le système avant d'installer l'application iSM.

Sujets :

Configuration requise pour l'installation

Pour accéder à la liste des systèmes d'exploitation pris en charge sur l'iDRAC Service Module (iSM), voir Systèmes d'exploitation pris en charge.

Les conditions préalables spécifiques à un système d'exploitation sont répertoriées dans le cadre des procédures d'installation. L'iSM peut être installé à l'aide de l'interface utilisateur. Le programme d'installation prend également en charge l'installation silencieuse.

Systèmes d'exploitation et hyperviseurs pris en charge

L'iDRAC Service Module 4.1.0.0 est pris en charge pour les systèmes d'exploitation 64 bits suivants :

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.5
- Red Hat Enterprise Linux 8.4
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP3
- Ubuntu Server 20.04.02 LTS
- VMware vSphere (ESXi) 7.0 U3 pris en charge sur les serveurs PowerEdge yx3x, yx4x et yx5x.
- VMware vSphere (ESXi) 7.0 U2 pris en charge sur les serveurs PowerEdge yx3x, yx4x et yx5x.
- VMware vSphere (ESXi) 6.7 U3 pris en charge sur les serveurs PowerEdge yx3x, yx4x et yx5x.

Plateformes prises en charge

L'iDRAC Service Module 4.1.0.0 prend en charge les serveurs PowerEdge yx2x, yx3x, yx4x et yx5x.

Plates-formes prises en charge sur les systèmes d'exploitation Linux

Le tableau répertorie les plates-formes prises en charge par iDRAC Service Module 4.1.0.0 sur les systèmes d'exploitation Linux.

Tableau 3. Plates-formes prises en charge sur les systèmes d'exploitation Linux

Appareils Dell EMC	Ubuntu Server 20.04.02	SUSE Linux Enterprise Server 15 SP3	Red Hat Enterprise Linux 8.5 et 8.4	Red Hat Enterprise Linux 7.9
Serveurs PowerEdge yx5x	Oui	Oui	Oui	Oui
Serveurs PowerEdge yx4x	Oui	Oui	Oui	Oui
Serveurs PowerEdge yx3x	Non	Oui	Oui	Oui
Serveurs PowerEdge yx2x	Non	Non	Non	Non

REMARQUE : Seuls quelques serveurs PowerEdge yx3x prennent en charge le système d'exploitation Red Hat Enterprise Linux 8.x. Pour obtenir la liste des serveurs Dell EMC PowerEdge pris en charge, consultez la matrice de certification Red Hat Enterprise Linux pour les serveurs Dell EMC PowerEdge.

Plates-formes prises en charge sur les systèmes d'exploitation Microsoft Windows

Le tableau répertorie les plates-formes prises en charge par iDRAC Service Module 4.1.0.0 sur les systèmes d'exploitation Microsoft Windows.

Tableau 4. Plates-formes prises en charge sur les systèmes d'exploitation Microsoft Windows

Appareils Dell EMC	Microsoft Windows Server 2019	Microsoft Windows Server 2016	Microsoft Windows Server 2022
Serveurs PowerEdge yx5x	Oui	Oui	Oui
Serveurs PowerEdge yx4x	Oui	Oui	Oui
Serveurs PowerEdge yx3x	Oui	Oui	Oui
Serveurs PowerEdge yx2x	Non	Oui	Oui

REMARQUE : Seuls quelques serveurs PowerEdge yx4x prennent en charge le système d'exploitation Microsoft Windows Server 2022. Pour obtenir la liste des serveurs Dell EMC PowerEdge pris en charge, voir le document Matrice de prise en charge Microsoft Windows Server pour les serveurs Dell EMC PowerEdge.

Plates-formes prises en charge sur l'hyperviseur de virtualisation

Le tableau répertorie les plates-formes prises en charge par l'iDRAC Service Module 4.1.0.0 sur les systèmes d'exploitation de virtualisation.

Tableau 5. Plates-formes prises en charge sur l'hyperviseur de virtualisation

Serveurs Dell EMC PowerEdge	VMware ESXi		
	vSphere 7.0 U3	vSphere 7.0 U2	vSphere 6.7 U3
Serveurs PowerEdge yx5x	Oui	Oui	Oui
Serveurs PowerEdge yx4x	Oui	Oui	Oui
Serveurs PowerEdge yx3x	Oui	Oui	Oui
Serveurs PowerEdge yx2x	Non	Non	Non

REMARQUE : Seuls quelques serveurs PowerEdge yx3x prennent en charge VMware ESXi 7.0 U2. Pour connaître la liste des serveurs PowerEdge yx3x pris en charge, reportez-vous à VMware vSphere 7.x sur la matrice de compatibilité des serveurs Dell EMC PowerEdge.

Systèmes d’exploitation pris en charge sur les systèmes Dell EMC Precision Rack

Tableau 6. Systèmes d’exploitation pris en charge sur les systèmes Dell EMC Precision Rack

Appareils Dell EMC	Systèmes d'exploitation pris en charge
R7920	Microsoft Windows 10 RS5 Microsoft Windows 10 Microsoft Windows 11 Professionnel Red Hat Enterprise Linux 8 Ubuntu Desktop 20.04 LTS

Configurations matérielles requises

Vous trouverez ci-dessous la liste des configurations matérielles requises :

- Un des systèmes d'exploitation pris en charge. Pour en savoir plus sur les systèmes d’exploitation pris en charge, voir la section Systèmes d’exploitation pris en charge.
- Minimum 2 Go de RAM.
- Minimum 512 Mo d’espace disque dur.
- Droits d'administrateur.
- La capacité Remote Network Driver Interface Specification (RNDIS) (spécification d’interface de pilote réseau à distance) pour trouver des périphériques réseau sur USB.

3

Installation de l'iDRAC Service Module

L'iDRAC Service Module (iSM) peut être installé sur tous les systèmes d'exploitation suivants :

- Microsoft Windows
- Linux
- VMware ESXi

Pour accéder à la liste des systèmes d'exploitation pris en charge sur l'iSM, voir Systèmes d'exploitation pris en charge.

REMARQUE : À partir de l'iDRAC Service Module version 4.x.x.x, l'adresse IP par défaut de la carte NIC USB définie par l'iDRAC Service Module est 169.254.1.1.

Sujets :

Installation initiale de l'iDRAC Service Module via l'iDRAC Enterprise ou Datacenter ou l'iDRAC Express sous Microsoft Windows et Linux

Vous pouvez installer l'iDRAC Service Module (iSM) à partir de l'iDRAC Entreprise ou Datacenter ou d'une interface iDRAC Express. La procédure d'installation est la même pour l'installation de l'iSM via l'iDRAC ou l'iDRAC Express sous les systèmes d'exploitation Microsoft Windows et Linux. Avec un simple clic à l'aide du package du programme d'installation de l'iDRAC sur le système d'exploitation hôte. À l'aide de cette méthode plutôt que de télécharger le programme d'installation à partir du site de support Dell EMC ou du DVD OpenManage, vous pouvez installer une version de l'iSM compatible avec le firmware de l'iDRAC.

L'iSM doit être installé sur le système d'exploitation hôte. Par conséquent, un système d'exploitation doit obligatoirement être installé et en cours d'exécution sur le périphérique hôte.

1. Démarrez la console virtuelle.
2. Connectez-vous au système d'exploitation hôte en tant qu'administrateur.
3. Dans la liste des périphériques, sélectionnez le volume monté qui est identifié par SMINST, puis cliquez sur le script correspondant pour démarrer l'installation. Pour installer l'iSM, exécutez la commande appropriée pour votre système :

   Pour Windows : `ISM_Win.bat`

   Pour Linux : `sh ISM_Lx.sh` ou `. ISM_Lx.sh`

   Pour Ubuntu : `bash ism_Lx.sh`

   Une fois l'installation terminée, l'iDRAC indique que l'iSM est installé et précise la date de dernière installation.

   REMARQUE : Le programme d'installation est accessible par le système d'exploitation hôte pendant 30 minutes, au cours desquelles vous devez démarrer l'opération d'installation. Sinon, vous devez redémarrer le programme d'installation de l'iDRAC Service Module.

Installation de l'iDRAC Service Module sur les systèmes d'exploitation Microsoft Windows

Le programme d'installation de l'iDRAC Service Module (iSM) pour les systèmes d'exploitation pris en charge est disponible sur le DVD *Documentation et outils de gestion des systèmes*. Vous pouvez également télécharger le programme d'installation de l'iSM depuis le site Dell.com/support.

Vous pouvez effectuer une installation manuelle ou automatique avec les commutateurs de ligne de commande appropriés. Vous pouvez installer l'iSM via le mécanisme de **poussée** à l'aide de consoles comme OpenManage Essentials (OME).

REMARQUE : Procédez comme suit uniquement si le chemin du module PowerShell tiers est absent dans l'environnement du système d'exploitation :

1. Naviguez vers **SYSMGMT** > **iSM** > **Windows**, puis exécutez `iDRACSvcMod.msi`.
   Le **module de service iDRAC - Assistant InstallShield** s'affiche.
2. Cliquez sur **Suivant**.
   Le **contrat de licence** s'affiche.
3. Lisez le Contrat de licence logicielle, sélectionnez l'option **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.
4. Sélectionnez le **Type d'installation** parmi les options suivantes, puis cliquez sur **Suivant** :
   - **Typique** : toutes les fonctionnalités du programme sont installées (nécessite la plus grande quantité d'espace disque).
   - **Personnalisé** : permet de personnaliser l'installation en choisissant les fonctionnalités du programme à installer, ainsi que l'emplacement (recommandé aux utilisateurs expérimentés).

   REMARQUE : les étapes suivantes s'appliquent uniquement si vous sélectionnez l'option **Personnalisé** dans la fenêtre **Type d'installation** :

   REMARQUE : Par défaut, les fonctionnalités **Traps SNMP intrabande, Accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte, SNMP Get via le système d'exploitation hôte, Alertes SNMP via le système d'exploitation hôte, Activer WSMAN** ne sont pas activées.

   a. Choisissez les fonctions du programme à installer, puis cliquez sur **Suivant**.
      La fenêtre **Réplication du journal Lifecycle Controller** s'affiche.
   b. Indiquez l'emplacement où les journaux Lifecycle Controller doivent être répliqués. Par défaut, l'option **Par défaut (Journaux/Système Windows)** est sélectionnée et les journaux Lifecycle Controller sont répliqués dans le groupe **Système** du dossier **Journaux Windows** dans l'**Observateur d'événements**. Cliquez sur **Suivant**.

      REMARQUE : vous pouvez également créer un groupe personnalisé dans le dossier **Journal d'application et des services** en sélectionnant l'option **Personnalisé** dans la fenêtre **Réplication du journal Lifecycle Controller**.

   c. Sélectionnez le mode d'authentification pour activer WS-Man à distance et installez un certificat auto-signé si le certificat d'authentification est introuvable. Fournissez un numéro de port WINRM pour établir la communication. Par défaut, le numéro de port doit être 5986.
5. Pour activer la fonctionnalité d'**Accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte**, fournissez un numéro de port unique allant de 1024 à 65535.

   REMARQUE : Si le numéro de port n'est pas fourni, 1266, sauf si un numéro de port a été configuré précédemment, sera attribué par défaut.

   La fenêtre **Prêt à installer le programme** s'affiche.
6. Cliquez sur **Installer** pour continuer l'installation.
   Vous pouvez aussi cliquer sur **Précédent** pour modifier vos préférences.

   Parfois, même si l'iSM est installé, le message suivant s'affiche dans le fichier journal de l'hôte : **La communication entre l'iDRAC Service Module et l'iDRAC n'a pas pu être établie. Reportez-vous au Guide d'installation d'iDRAC Service Module le plus récent.** Pour en savoir plus sur le dépannage, voir la section Questions fréquentes.

   Parfois, lors de l'installation d'iSM, un message d'alerte s'affiche : **L'objet iDRAC Service Module a expiré. Veuillez vérifier que les services iDRAC Service Module ont démarré normalement.** Ce message d'avertissement est dû au délai d'activation d'une carte NIC USB et du démarrage du service iSM. Il est recommandé à l'utilisateur de vérifier l'état du service iSM une fois l'installation terminée.

   L'iSM est installé.
7. Cliquez sur **Terminer**.

Sous le système d'exploitation Microsoft Windows 2016 et Windows 2019, la description de l'appareil de la carte NIC USB de l'iDRAC indique qu'il s'agit d'un **Appareil compatible NDIS distant**.

Installation silencieuse de l'iDRAC Service Module sous Microsoft Windows

Vous pouvez installer l'iDRAC Service Module (iSM) à l'aide de l'installation silencieuse, sans console interactive.

- Pour installer l'iDRAC Service Module à l'aide de l'installation silencieuse (installation sans assistance), saisissez la commande `msiexec /i iDRACSvcMod.msi /qn` lorsque vous y êtes invité.
- Pour générer les fichiers log d'installation, saisissez `msiexec /i iDRACSvcMod.msi /L*V <logname with the path>`
- Pour répliquer les journaux Lifecycle Controller dans un groupe existant ou un dossier personnalisé, saisissez `msiexec /i iDRACSvcMod.msi CP_LCLOG_VIEW="<existing group name or custom folder name>"`
- Pour installer la fonctionnalité suivante à l'aide de l'installation silencieuse, saisissez `msiexec /i <location of the installer file>/iDRACSvcMod.msi /qn ADDLOCAL=<xxxx>`

  REMARQUE : `<XXXX>` peut être n'importe quelle fonctionnalité mentionnée dans le tableau suivant. Vous pouvez installer plusieurs fonctionnalités en utilisant une virgule. Par exemple :

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

Tableau 7. Paramètres et fonctionnalités

Paramètres	Fonctionnalités
`OSInfo`	Informations sur le système d'exploitation
`Watchdog`	Récupération automatique du système
`LCLog`	Réplication du journal Lifecycle
`IBIA2`	Accès à l'iDRAC via le système d'exploitation hôte
`WMIPOP`	Fournisseurs WMI (Windows Management Instrumentation)
`iDRACHardReset`	Réinitialisation matérielle de l'iDRAC
`SupportAssist`	SupportAssist
`iDRAC_GUI_Launcher`	Lanceur de l'interface utilisateur de l'iDRAC
`FullPowerCycle`	Cycle d'alimentation complet
`SDSEventCorrelation`	Corrélation des événements SDS
`SM`	Surveillance S.M.A.R.T
`OmsaSNMPTraps`	Traps SNMP OMSA

- Pour installer WS-Man, saisissez `msiexec.exe /i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2" CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1" /qn`
- Pour afficher l'interface utilisateur dans les langues prises en charge, saisissez `msiexec /i iDRACSvcMod.msi TRANSFORMS=<locale number>.mst`, où « locale number » possède la valeur suivante :

Tableau 8. Numéro des paramètres régionaux et leurs langues prises en charge

Numéro des paramètres régionaux	Langue
1031	Allemand
1033	Anglais (US)
1034	Espagnol
1036	Français
1041	Japonais

Tableau 8. Numéro des paramètres régionaux et leurs langues prises en charge (suite)

Numéro des paramètres régionaux	Langue
2052	Chinois simplifié

Modification des composants de l'iDRAC Service Module sous les systèmes d'exploitation Microsoft Windows

Pour modifier les composants de l'iDRAC Service Module :

1. Naviguez vers **SYSMGMT** > **iSM** > **Windows**, puis exécutez `iDRACSvcMod.msi`.
   Le **module de service iDRAC - Assistant InstallShield** s'affiche.
2. Cliquez sur **Suivant**.
3. Sélectionnez **Modifier**.
4. Activez ou désactivez les fonctionnalités selon les besoins, puis cliquez sur **Suivant**.
   La fenêtre **Réplication du journal Lifecycle Controller** s'affiche.
5. Indiquez l'emplacement où répliquer les fichiers log LC. Par défaut, l'option **Typique/Par défaut (Journaux/Système Windows)** est sélectionnée et les journaux LC sont répliqués dans le groupe **Système** du dossier **Journaux Windows** dans l'**Observateur d'événements**.
6. Cliquez sur **Suivant**.

   REMARQUE : vous pouvez également créer un groupe personnalisé dans le dossier **Journal d'application et des services** en sélectionnant l'option **Personnalisé** dans la fenêtre **Réplication du journal Lifecycle Controller**.

   REMARQUE : Vous devez redémarrer le système dans les cas de figure suivants :
   - Si vous basculez entre les options **Typique/Par défaut (Journaux/Système Windows)** et **Personnalisé**.
   - Si vous passez d'un dossier personnalisé à un autre dossier.

   L'écran **Prêt à installer** apparaît.
7. Pour accéder à l'iDRAC via la fonctionnalité du système d'exploitation hôte, fournissez un numéro de port unique allant de 1024 à 65535.

   REMARQUE : Si le numéro de port n'est pas fourni, 1266, sauf si un port a été configuré précédemment, sera attribué par défaut.
8. Cliquez sur **Installer** pour continuer le processus.
   Vous pouvez aussi cliquer sur **Précédent** pour modifier vos préférences.
   L'iDRAC Service Module a été modifié avec succès.
9. Cliquez sur **Terminer**.

Réparation de l'iDRAC Service Module exécuté sur les systèmes d'exploitation Microsoft Windows

Pour réparer un composant de l'iDRAC Service Module (iSM) défaillant ou non fonctionnel :

1. Naviguez vers **SYSMGMT** > **iSM** > **Windows**, puis exécutez `iDRACSvcMod.msi`.
   L'écran **iDRAC Service Module - Assistant InstallShield** s'affiche.
2. Cliquez sur **Suivant**.
3. Sélectionnez **Réparer**, puis cliquez sur **Suivant**.
   Le message **Prêt à installer** apparaît.
4. Cliquez sur **Réparer** pour continuer le processus.
   Vous pouvez aussi cliquer sur **Précédent** pour modifier vos préférences.
   Le composant de l'iDRAC Service Module est réparé avec succès.
5. Cliquez sur **Terminer**.

Désinstallation de l'iDRAC Service Module exécuté sur les systèmes d'exploitation Microsoft Windows

Vous avez le choix entre deux méthodes de désinstallation de l'iDRAC Service Module (iSM) :

- Désinstallation automatique avec l'ID de produit
- Désinstallation en utilisant la fonction Ajout/Suppression

Désinstallation sans assistance de l'iDRAC Service Module à l'aide de l'ID de produit

Saisissez `msiexec /x {D2C8B8C2-7AB8-4B64-8936-079341A389AB} /qn` pour désinstaller l'iDRAC Service Module à l'aide de l'ID de produit.

Désinstallation de l'iDRAC Service Module à l'aide de la fonctionnalité Ajouter ou Supprimer

Pour désinstaller l'iSM à l'aide de l'option Ajouter ou Supprimer à partir du panneau de configuration, accédez à **Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités** .

REMARQUE : Vous pouvez également effectuer une désinstallation en sélectionnant **Désinstaller** après avoir exécuté la commande `iDRACSvcMod.msi`.

REMARQUE : Vous pouvez afficher les fichiers log de l'iSM dans le groupe **Application** du dossier **Journaux Windows** dans l'**Observateur d'événements** Windows.

Installation de l'iDRAC Service Module sous VMware ESXi

VMware ESXi est installé en usine sur certains systèmes. Pour obtenir la liste de ces systèmes, voir le document *Matrice de support logiciel des systèmes* le plus récent, disponible sur **dell.com/support**.

L'iSM est disponible sous forme de fichier ZIP pour une installation sur les systèmes exécutant VMware ESXi. Le fichier ZIP respecte la convention d'affectation de noms **ISM-Dell-Web-4.1.0.0-<bldno>.VIB-<version>i-Live.zip**, où <version> correspond à la version ESXi prise en charge.

Les fichiers ZIP pour les versions ESXi prises en charge sont les suivants :

- Pour VMware ESXi 7.x : `ISM-Dell-Web-4.1.0.0-<bldno>.VIB-ESX7i-Live.zip`
- Pour VMware ESXi 6.x : `ISM-Dell-Web-4.1.0.0-<bldno>.VIB-ESX6i-Live.zip`

Si VMware ESXi n'est pas installé sur votre système, suivez ces étapes pour installer l'iSM sur VMware ESXi :

1. Copiez le fichier ZIP du lot hors ligne iSM à l'emplacement `/var/log/vmware` sur le système d'exploitation hôte.
2. Exécutez la commande suivante :
   - Pour VMware ESXi 7.x : `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`
   - Pour VMware ESXi 6.x : `esxcli software vib install -d /var/log/vmware/<iDRAC Service Module file>`

Pour mettre à niveau l'iSM sur VMware ESXi, procédez comme suit :

1. Copiez le fichier ZIP du lot hors ligne iSM à l'emplacement `/var/log/vmware` sur le système d'exploitation hôte.
2. Exécutez la commande suivante :
   - Pour VMware ESXi 7.x : `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`
   - Pour VMware ESXi 6.x : `esxcli software vib update -d /var/log/vmware/<iDRAC Service Module file>`

La configuration des fonctionnalités de l'iDRAC Service Module n'est pas conservée après un redémarrage forcé ou inapproprié. Une sauvegarde des fichiers de configuration est créée par l'hyperviseur ESXi par le biais du script `script /sbin/auto-backup.sh` qui

s'exécute périodiquement toutes les 60 minutes. Si vous souhaitez conserver la configuration, exécutez manuellement le script backup.sh avant de redémarrer le système.

REMARQUE : Aucun redémarrage du système d'exploitation hôte n'est requis après l'installation ou la désinstallation du package de l'iDRAC Service Module Live VIB.

REMARQUE : Dans les installations reposant sur un espace de stockage, comme VMware Update Manager (VUM) et apt-repository, toutes les fonctionnalités ne sont pas activées par défaut.

Utilisation de la CLI vSphere

Pour installer le logiciel de l'iSM sous VMware ESXi dans l'interface de ligne de commande (CLI) vSphere :

1. Copiez le fichier `ISM-Dell-Web-4.1.0.0-<bldno>.VIB-<version>i-Live.zip` dans un répertoire du système.
2. Éteignez tous les systèmes d'exploitation invités sur l'hôte ESXi et mettez l'hôte ESXi en mode de maintenance.
3. Si vous utilisez l'interface CLI vSphere sous Windows, naviguez vers le répertoire où vous avez installé les utilitaires CLI vSphere. Si vous utilisez l'interface CLI vSphere sur Linux, vous pouvez exécuter la commande suivante depuis n'importe quel répertoire :

   Pour VMware ESXi 7.x :

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

   Pour VMware ESXi 6.x :

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

   REMARQUE : l'extension PL n'est pas obligatoire si vous utilisez la CLI vSphere sous Linux.

4. À l'invite, saisissez le nom d'utilisateur racine (root) et le mot de passe de l'hôte ESXi.
   Le résultat de la commande affiche une mise à jour réussie ou ayant échoué.

Installation de l'iDRAC Service Module à l'aide de VMware Update Manager

Pour installer l'iSM à l'aide de VMware Update Manager (VUM) :

1. Installez VMware vSphere 6.5 ou versions ultérieures, vCenter Server, vSphere Client et VMware vSphere Update Manager, sur un système d'exploitation Microsoft Windows pris en charge.
2. Sur le bureau, double-cliquez sur **Client VMware vSphere** et connectez-vous au vCenter Server.
3. Cliquez avec le bouton droit sur **Hôte du client vSphere**, puis sélectionnez **Nouveau centre de données**.
4. Cliquez avec le bouton droit sur **Nouveau centre de données**, puis cliquez sur **Ajouter un hôte**. Fournissez les informations relatives au serveur ESXi demandées.
5. Cliquez avec le bouton droit sur l'**hôte ESXi** ajouté à l'**étape 4**, puis cliquez sur **Mode maintenance**.
6. Depuis **Plug-ins**, sélectionnez **Gérer les plug-ins** > **Télécharger VMware Update Manager**. Le statut est activé si le téléchargement a réussi. Suivez les instructions pour installer le client VUM.
7. Sélectionnez l'**hôte ESXi**. Cliquez sur **Update Manager** > **Vue Admin** > **Logithèque de correctifs** > **Importer des correctifs** et suivez les instructions qui s'affichent à l'écran pour charger convenablement le correctif.
   Le lot hors ligne est affiché.
8. Cliquez sur **Lignes de base et groupes**.
9. Cliquez sur l'onglet **Créer à partir des lignes de base**, saisissez le nom de la ligne de base, sélectionnez **Extension d'hôte** comme type de ligne de base, puis fournissez les informations demandées.
10. Cliquez sur **Vue Admin**.
11. Cliquez sur **Ajouter à la ligne de base**, en regard du nom du correctif chargé, et sélectionnez le nom de la ligne de base créée à l'étape 8.
12. Cliquez sur **Vue Conformité**.
13. Sélectionnez l'onglet **Update Manager**.

14. Cliquez sur **Joindre**, puis sélectionnez la **ligne d'extension de base** créée à l'étape 8 et suivez les instructions.
15. Cliquez sur **Balayer**, sélectionnez **Correctifs et extensions**, si l'option n'est pas sélectionnée par défaut, puis cliquez sur **Balayer**.
16. Cliquez sur **Préparer**, sélectionnez l'**extension d'hôte** créée et suivez les instructions.
17. Cliquez sur **Corriger** et suivez les instructions une fois la préparation terminée.
    L'installation de l'iSM est terminée.

    Pour plus d'informations sur VMWare Update Manager, reportez-vous au site Web de VMWare.

    REMARQUE : Vous pouvez installer l'iSM à partir du référentiel VUM, vmwaredepot.dell.com/.

Mise à niveau de l'iDRAC Service Module sur VMware ESXi

Pour mettre à niveau l'iDRAC Service Module à l'aide de VMware Update Manager (VUM) :

1. Installez VMware vSphere 6.5 ou versions ultérieures (vCenter Server, vSphere Client et VMware vSphere Update Manager) sur un système d'exploitation Microsoft Windows pris en charge.
2. Sur le bureau, double-cliquez sur **Client VMware vSphere** et connectez-vous au serveur vCenter.
3. Cliquez avec le bouton droit sur **Hôte du client vSphere**, puis sélectionnez **Nouveau centre de données**.
4. Cliquez avec le bouton droit sur **Nouveau centre de données**, puis cliquez sur **Ajouter un hôte**. Suivez les instructions affichées à l'écran pour fournir les informations relatives au serveur ESXi.
5. Cliquez avec le bouton droit sur l'**hôte ESXi** ajouté à l'**étape 4**, puis cliquez sur **Mode maintenance**.
6. Depuis **Plug-ins**, sélectionnez **Gérer les plug-ins** > **Télécharger VMware Update Manager**. (Le statut est activé si le téléchargement est réussi.) Suivez les instructions pour installer le client VUM.
7. Sélectionnez l'hôte ESXi. Cliquez sur **Update Manager** > **Vue Admin** > **Logithèque de correctifs** > **Importer des correctifs** et suivez les instructions qui s'affichent à l'écran pour charger convenablement le correctif.

   Le lot hors ligne est affiché.
8. Cliquez sur **Lignes de base et groupes**.
9. Cliquez sur l'onglet **Créer à partir des lignes de base**, entrez le nom de la ligne de base, puis sélectionnez **Extension d'hôte** comme type de ligne de base.

   REMARQUE : Sélectionnez la dernière version de l'iDRAC Service Module pour créer la ligne de base.

   Remplissez le reste des champs en suivant les instructions.
10. Cliquez sur **Vue Admin**.
11. Cliquez sur **Ajouter à la ligne de base** (en regard du nom du correctif chargé) et sélectionnez le nom de la ligne de base créée à l'étape 8.
12. Cliquez sur **Vue Conformité**. Sélectionnez l'onglet **Update Manager**. Cliquez sur **Joindre**, puis sélectionnez la **ligne d'extension de base** créée à l'étape 8 et suivez les instructions.
13. Cliquez sur **Balayer**, sélectionnez **Correctifs et extensions** (si l'option n'est pas sélectionnée par défaut), puis cliquez sur **Balayer**.
14. Cliquez sur **Préparer**, sélectionnez l'**extension d'hôte** créée et suivez les instructions.
15. Cliquez sur **Corriger** et suivez les instructions une fois la préparation terminée.

    La mise à niveau de l'iDRAC Service Module est terminée.

    REMARQUE : Le système d'exploitation hôte redémarre pendant la mise à niveau de l'iSM à l'aide de VMware Update Manager. Pour plus d'informations sur VMware Update Manager, reportez-vous au site Web officiel de VMware.

    REMARQUE : Vous pouvez mettre à jour l'iDRAC Service Module à partir du référentiel VMware Update Manager, disponible à l'adresse vmwaredepot.dell.com.

Installation d'iDRAC Service Module à l'aide de vSphere Lifecycle Manager dans Client vSphere

REMARQUE : Avant de procéder à l'installation, assurez-vous que la version de l'iSM que vous avez téléchargée est compatible avec VMware ESXi 7.x.

Pour installer l'iSM à l'aide de vSphere Lifecycle Manager (vLCM) dans Client vSphere (VC), procédez comme suit :

1. Installez Client vSphere (VCSA) sur un système d'exploitation Microsoft Windows pris en charge.
2. Connectez-vous à Client vSphere à l'aide d'un navigateur Web.

3. Cliquez avec le bouton droit de la souris sur **Hôte de Client vSphere**, puis sélectionnez **Nouveau datacenter**.
4. Cliquez avec le bouton droit de la souris sur **Nouveau datadenter**, puis sur **Ajouter un hôte**. Suivez les instructions affichées à l'écran pour fournir les informations sur le serveur ESXi.
5. Cliquez sur **Menu** > **Lifecycle Manager** > **Paramètres** > **Configuration des correctifs** > **NOUVEAU**, et activez le référentiel en ligne.
6. Cliquez sur **ACTIONS** > **Mises à jour de synchronisation**.

   L'iSM VIB est téléchargé dans VC.
7. Sélectionnez l'hôte ESXi. Cliquez sur **Lignes de base** > **Lignes de base jointes** > **JOINDRE** > **Créer** > **Joindre une ligne de base**, puis suivez les instructions qui s'affichent à l'écran pour télécharger le correctif.
8. Cliquez sur **PRÉPARER** et suivez les instructions.
9. Une fois la préparation terminée, cliquez sur **CORRIGER** et suivez les instructions.

   L'installation de l'iSM est terminée.

Utilisation de l'interface de ligne de commande (PowerCLI)

Pour installer l'iSM à l'aide de l'interface PowerCLI :

1. Installez l'interface PowerCLI d'ESXi prise en charge sur le système d'exploitation Microsoft Windows pris en charge.
2. Copiez le fichier OM-SrvAdmin-Dell-Web-<version>-<bldno>.VIB-ESX<version>i_<bld-revno>.zip sur l'hôte ESXi.
3. Naviguez vers le répertoire bin.
4. Exécutez Connect-VIServer, et entrez les références du serveur ou autres informations d'identification nécessaires.
5. Connectez-vous à l'hôte ESXi à l'aide de la CLI vSphere d'ESXi 6.x U3 ou ESXi 7.x prise en charge et créez un magasin de données.
6. Créez un dossier **ISM-Dell-Web-4.1.0,0-<bldno>.VIB-<version>I** sur l'hôte ESXi 6.x U3 ou ESXi 7.x sous le répertoire **/vmfs/volumes/<datastore_name>**.
7. Copiez le fichier ZIP ESXi sur l'hôte ESXi 6.x U3 ou ESXi 7.x dans le répertoire **/vmfs/volumes/<datastore_name>ISM-Dell-Web-4.1.0,0-<bldno>.VIB-<version>I**.
8. Décompressez le fichier ZIP dans le dossier indiqué ci-dessus.
9. Exécutez la commande suivante dans l'interface PowerCLI :

   Pour ESXi 7.x :

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-4.1.0.0-<bldno>.VIB-<version>i/metadata.zip
   ```

   Pour ESXi 6.x :

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-4.1.0.0-<bldno>.VIB-<version>i/metadata.zip
   ```
10. Exécutez la commande suivante pour vérifier si l'iSM est correctement installé sur l'hôte :

    Pour ESXi 7.x : `esxcli software component get -n DEL-dcism`.

    Pour ESXi 6.x : `esxcli software vib get -n dcism`.

    L'iSM s'affiche.
11. Redémarrez le système d'exploitation hôte après l'installation de l'iSM à l'aide de la commande Power CLI ci-dessus.

    Pour plus d'informations sur Power CLI, reportez-vous au site Web de VMWare.

Désinstallation de l'iDRAC Service Module sur VMware ESXi

Pour désinstaller l'iSM sur VMware ESXi, utilisez la commande suivante :

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

Installation de l'iDRAC Service Module sous les systèmes d'exploitation Linux pris en charge

L'ensemble de l'iSM est stocké dans un package RPM (Red Hat Package Manager) unique. Le package, qui est accompagné d'un script shell, permet d'installer, de désinstaller, d'activer ou de désactiver les fonctionnalités disponibles.

Avant d'installer l'iSM, vous devez installer le collecteur du package OSC à l'aide de `rpm -ivh dcism-osc*.rpm`.

Comme le programme d'installation sous Linux est constitué d'un seul RPM, l'installation granulaire n'est pas prise en charge. Vous ne pouvez activer ou désactiver des fonctionnalités que lors d'une installation par script.

REMARQUE : Le programme d'installation est disponible pour toutes les versions 64 bits des systèmes d'exploitation Linux prises en charge par l'iSM.

Configuration avant installation requise pour les systèmes d'exploitation Linux

Pour installer l'iSM sur des systèmes dotés d'un système d'exploitation Linux pris en charge, exécutez `setup.sh`.

Assurez-vous que la configuration requise de base pour le fonctionnement est bien respectée, notamment :

- La **connexion directe entre le système d'exploitation et l'iDRAC** est activée automatiquement après l'installation de l'iSM
- La pile réseau IPv4 est activée dans le système d'exploitation hôte
- Le sous-système USB est activé
- `udev` est activé ; obligatoire pour démarrer iSM automatiquement

Pour plus d'informations sur l'iDRAC, consultez la dernière version du *Guide d'utilisation d'Integrated Dell Remote Access Controller* sur Dell.com/support.

Dépendances d'installation Linux

Vous trouverez ci-dessous la liste des packages dépendants et exécutables qui doivent être installés pour terminer l'installation.

Tableau 9. Dépendances d'installation Linux

Commandes d'exécutable	Nom de package
/sys	fileSystem
grep	grep
cut, cat, echo, pwd,	coreutils
lsusb	usbutils
find	findutils
commandes de script shell	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

Tableau 9. Dépendances d'installation Linux (suite)

Commandes d'exécutable	Nom de package
curl	libcurl
openssl	libssl

Installation de l'iDRAC Service Module sous les systèmes d'exploitation Linux

1. Ouvrez l'application et passez en revue les fonctionnalités affichées à l'écran :

```
[x] 1. Watchdog Instrumentation Service
[x] 2. LifeCycle Log Information
[x] 3. Operating System Information
[ ] 4. iDRAC access via Host OS
        [ ] a. Access via GUI, WS-man, Redfish, Remote Racadm
        [ ] b. In-band SNMP Traps
        [ ] c. SNMP OMSA Traps
        [ ] d. Access via SNMP Get
[x] 5. iDRAC SSO Launcher
        [x] a. Read only
        [ ] b. Administrator
[ ] 6. Chipset S.M.A.R.T Monitoring
    7. iDRAC Hard Reset
    8. Support Assist
    9. Full Power Cycle
[ ] 10. All Features
```

2. Installez la fonctionnalité requise en saisissant le numéro de la fonctionnalité en question. séparez les différentes fonctions à installer par une virgule. Par exemple, pour installer les sous-fonctionnalités, saisissez **4.a, 4.b ou 4.c**.
3. Installez les fonctionnalités sélectionnées en saisissant **I**. Si vous ne souhaitez pas poursuivre l'installation, saisissez **q** pour quitter cet écran.

   REMARQUE : Après avoir installé différentes fonctionnalités, vous pouvez également les modifier.

   Pour vérifier l'état du service iSM, exécutez la commande : `systemctl status dcismeng.service`. Si l'iSM est installé et en cours d'exécution, l'état **Exécution** s'affiche.

   vous devez fournir un numéro de port unique compris dans la plage 1 024 à 65 535 si vous avez choisi d'installer l'accès à l'iDRAC par l'intermédiaire de la fonctionnalité du système d'exploitation hôte. Si vous n'indiquez aucun numéro de port, le *numéro de port 1266* ou un port configuré précédemment (le cas échéant) est attribué par défaut. Si OpenManage Server Administrator est déjà installé sur le port 1311, le même port ne peut pas être utilisé pour l'iSM.

   Lorsqu'iSM 3.4.0 ou version ultérieure est installé sur les systèmes d'exploitation Linux, un avertissement gnome s'affiche, semblable à : « *failed to rescan: Failed to parse /usr/share/applications/iDRACGUILauncher.desktop file: cannot process file of type application/x-desktop* ».

Installation silencieuse de l'iDRAC Service Module sous Linux

Vous pouvez installer l'iSM discrètement en arrière-plan, sans console utilisateur. Pour ce faire, il convient d'utiliser `setup.sh` avec des paramètres spécifiques.

Les paramètres qui peuvent être transmis pour utiliser `setup.sh` sont les suivants :

Tableau 10. Paramètres d'installation silencieuse

Paramètre	Description
-h	Aide : affiche l'aide
-i	Installation : installe et active les fonctionnalités sélectionnées
-x	Express : installe et active toutes les fonctions disponibles

Tableau 10. Paramètres d'installation silencieuse (suite)

Paramètre	Description
-d	Suppression : désinstalle l'iSM
w	Surveillance : active le Service d'instrumentation de surveillance
-l	Journal Lifecycle Controller : active les informations du journal Lifecycle
-o	Informations sur le système d'exploitation : permet d'obtenir des informations sur le système d'exploitation
-a	Démarrage automatique : démarre le service après l'installation du composant de l'iSM
-o	Accès à l'iDRAC via le système d'exploitation hôte : active l'accès à l'interface utilisateur de l'iDRAC, WS-Man, Redfish et RACADM à distance
-s	Active les interruptions SNMP intrabandes
-So	Active les traps SNMP OMSA
-g	Permet l'accès via SNMP Get
-Sr	Active la connexion à l'iDRAC par authentification unique (SSO) en tant qu'utilisateur en lecture seule
-Sa	Active la connexion à l'iDRAC par authentification unique (SSO) en tant qu'administrateur
-Sm	Permet la surveillance S.M.A.R.T du chipset
-Sp	Active la collecte périodique des journaux S.M.A.R.T

REMARQUE : Sous les systèmes d'exploitation Linux, si une opération modifiant une fonctionnalité dotée d'une option d'installation silencieuse est activée à partir du pack Web Linux à l'aide de setup.sh, les états de fonctionnalités précédemment activées seront écrasés par les nouvelles fonctionnalités sélectionnées pendant l'opération de modification.

Désinstallation de l'iDRAC Service Module sous les systèmes d'exploitation Linux

Vous avez le choix entre deux méthodes de désinstallation de l'iSM :

- Utilisation du script de désinstallation
- Utilisation de la commande RPM

Désinstallation de l'iDRAC Service Module à l'aide du script de désinstallation

La commande utilisée pour la désinstallation de l'iSM est `dcism-setup.sh`. Exécutez la commande shell et sélectionnez *d* pour désinstaller l'iSM.

Pour désinstaller l'iSM en mode silencieux, exécutez `./setup.sh -d`.

Désinstallation de l'iDRAC Service Module avec la commande RPM

L'iSM peut être désinstallé à l'aide de la commande RPM `rpm -e dcism` sur la ligne de commande.

REMARQUE : La désinstallation de l'iSM à l'aide de la commande `rpm -e dcism` n'entraine pas la désinstallation du package OSC installé par l'iSM. Vous pouvez désinstaller le package OSC à l'aide de la commande `rpm -e dcism-osc`.

Désinstallation de l'iDRAC Service Module avec la commande dpkg

Dans le système d'exploitation Ubuntu, l'iSM peut être désinstallé à l'aide de la commande dpkg dans la ligne de commande `dpkg --remove dcism`.

Vous pouvez désinstaller le package OSC à l'aide de la commande `dpkg --purge dcism-osc`.

Installation de l'iDRAC Service Module lorsque le mode de verrouillage de la configuration du système est activé dans l'iDRAC

Lorsque la fonctionnalité du mode de verrouillage de la configuration du système est activée par l'intermédiaire de l'iDRAC, aucune opération de configuration ne peut être effectuée pour l'iSM. Toutes les fonctionnalités activées avant l'activation de la fonctionnalité du mode de verrouillage de la configuration du système restent activées. Si OMSA est installé après l'activation de la fonctionnalité du mode de verrouillage de la configuration du système, seules les fonctionnalités de l'iSM qui étaient activées auparavant restent disponibles pour les utilisateurs. Dès que la fonctionnalité du mode de verrouillage de la configuration du système est désactivée dans l'iDRAC, toutes les opérations de configuration peuvent être effectuées.

Prise en charge des URI de l'iDRAC pour l'obtention du programme d'installation de l'iDRAC Service Module

Vous pouvez télécharger les packages Web de l'iSM depuis l'URL suivante : **https:// <iDRACIP>/software/ism/package.xml**. Vous pouvez télécharger les packages uniquement lorsque le package de mise à jour Dell du LC de l'iSM est chargé et disponible dans l'iDRAC. Vous pouvez également les charger dans l'iDRAC en activant la mise à jour automatique du LC de l'iDRAC.

Vous trouverez ci-dessous un exemple de code XML avec un nom de fichier image mentionné pour télécharger le package.

```
<PayloadConfiguration>
<Image filename="OM-iSM-Dell-Web-LX-4.1.0.0.tar.gz" id="5DD5A8BA-1958-4673-BE77-40B69680AF5D"
skip="false" type="APAC" version="4.1.0.0"/>
<Image filename="OM-iSM-Dell-Web-LX-4.1.0.0.tar.gz.sign" id="E166C545-82A9-4D5D-8493-
B834850F9C7A" skip="false" type="APAC" version="4.1.0.0"/>
<Image filename="OM-iSM-Dell-Web-X64-4.1.0.0.exe" id="5015744F-F938-40A8-B695-5456E9055504"
skip="false" type="APAC" version="4.1.0.0"/>
<Image filename="ISM-Dell-Web-4.1.0.0-VIB-ESX6i-Live.zip" id="1F3A165D-7380-4691-
A182-9D9EE0D55233" skip="false" type="APAC" version="4.1.0.0"/>
<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>
```

Pour télécharger les packages, utilisez le nom de fichier image présent dans le code XML à ajouter à l'URL. Par exemple :

- Les packages Web Microsoft Windows peuvent être téléchargés depuis l'URL **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-X64–4.1.0.0.exe**.

Le package VMware ESXi Live VIB depuis Lifecycle Controller peut être téléchargé depuis l'URL**https://<iDRACIP>/software/ism/ISM-Dell-Web-4.1.0,0-VIB-ESX6i-Live.zip**.

Le package Web Red Hat Enterprise Linux peut être téléchargé depuis l'URL **https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-LX-4.1.0.0.tar.gz**.

Prise en charge d'idrac.local et de drac.local en tant que FQDN de l'iDRAC

Vous pouvez connecter l'iSM à l'interface utilisateur de l'iDRAC à partir du système d'exploitation hôte en saisissant `drac.local` ou `idrac.local` dans le navigateur Web, que le système d'exploitation hôte prenne en charge le protocole mDNS (multicast Domain Name System) ou non.

REMARQUE : Cette fonctionnalité est uniquement prise en charge sur les adresses IPv4.

4

Configuration de l'iDRAC Service Module

Les fonctionnalités de l'iDRAC Service Module peuvent être configurées à distance à l'aide de différentes interfaces de l'iDRAC, telles que l'interface utilisateur, l'interface de ligne de commande et WS-Man.

Sujets :

Configuration de l'iDRAC Service Module à partir de l'interface Web de l'iDRAC

Connectez-vous à l'interface utilisateur de l'iDRAC à l'aide de l'adresse IP de l'iDRAC en tant qu'utilisateur root ou administrateur.

Pour utiliser l'iSM à partir de l'interface Web de l'iDRAC pour les serveurs PowerEdge yx2x et yx3x, accédez à **Présentation** > **Serveur** > **Service Module**.

Pour utiliser l'iSM à partir de l'interface Web de l'iDRAC pour les serveurs PowerEdge yx4x et yx5x, accédez à **Paramètres de l'iDRAC** > **Paramètres** > **Configuration de l'iDRAC Service Module**.

Configuration de l'iDRAC Service Module à partir de RACADM

Vous pouvez accéder à l'iSM et le configurer via les commandes de l'interface de ligne de commande RACADM. Pour vérifier l'état des fonctionnalités fournies par l'iSM, utilisez la commande `racadm get idrac.servicemodule`. Ces fonctionnalités sont les suivantes :

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

Pour définir ou configurer les fonctionnalités, utilisez la commande `racadm set idrac.servicemodule. <feature name> <enabled or disabled>`.

REMARQUE : Les noms des fonctionnalités et les attributs commençant par un symbole # ne peuvent pas être modifiés.

Pour utiliser l'iSM à partir de RACADM, reportez-vous aux objets du groupe **Service Module** dans le manuel *Guide de référence de la ligne de commande RACADM pour iDRAC8, iDRAC9 et CMC* ( ) disponible à l'adresse Dell.com/support.

Configuration de l'iDRAC Service Module à partir de WS-Man

Vous pouvez accéder à l'iSM et le configurer via WS-Man à l'aide de la commande suivante :

```
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:{username} -p:{password} -r:https://<Host
IP address>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic
@{Target="iDRAC.Embedded.1";AttributeName="AgentLite.1#<feature>";AttributeValue="1"}
```

Pour utiliser l'iSM à partir de WS-Man, reportez-vous au *Guide de l'interface des services Web Dell Lifecycle Controller 2*. Ce guide fournit des informations et des exemples d'utilisation de WS-Man, et est disponible sur Dell.com/support.

5

Configurations de sécurité et compatibilité

L'iDRAC Service Module (iSM) est déployé avec la configuration de sécurité par défaut pour vous protéger contre certains incidents, comme le piratage de DLL, l'altération de DLL et la divulgation d'informations. Cette section présente la configuration de la sécurité avec laquelle l'iSM est installé.

Sujets :

Sécurité de communication renforcée entre l'iSM et l'iDRAC à l'aide du protocole TLS

La communication de données entre l'iSM et l'iDRAC utilise des supports USBNIC INET protégés par TLS. Cela assure la protection de toutes les données transmises de l'iDRAC vers l'iSM via USBNIC. L'iDRAC et l'iSM utilisent des certificats auto-signés pour contrôler l'authentification. Les certificats auto-signés sont valables 10 ans. De nouveaux certificats auto-signés sont générés chaque fois que vous effectuez une nouvelle installation de l'iSM. Réinstallez ou mettez à niveau l'SM lorsque les certificats expirent.

REMARQUE : La réinstallation de l'iSM (réparation) ne fonctionne pas sur les systèmes d'exploitation Linux. Vous devez désinstaller, puis installer l'iSM sur les systèmes d'exploitation Linux.

REMARQUE : Lorsque le certificat TLS-client de l'iSM expire, la communication entre l'iSM et l'iDRAC échoue et un journal d'audit du système d'exploitation est généré. Vous devez alors réinstaller l'iSM sur le système d'exploitation hôte.

La version du TLS de l'iDRAC et de l'hôte doit être 1.1 ou supérieure. La communication entre l'iSM et l'iDRAC échoue si la négociation de la version du protocole TLS échoue. Si une version de l'iSM compatible avec la fonctionnalité TLS est installée sur un firmware de l'iDRAC qui ne prend pas en charge la communication TLS via USBNIC, elle fonctionnera avec le canal non-TLS comme dans les nouvelles versions d'iSM.

Si l'iSM est installé ou mis à niveau vers la version 3.4.0 ou ultérieure avant que l'iDRAC soit mis à niveau vers la version 3.30.30.30 ou ultérieure, vous devez désinstaller et réinstaller l'iSM pour établir un nouveau certificat TLS. L'iSM avec fonctionnalité TLS est pris en charge sur les versions de firmware de l'iDRAC 3.30.30.30 et ultérieures.

L'iSM sans fonctionnalité TLS ne fonctionne pas sur une version du firmware iDRAC prenant en charge le TLS. Par exemple : les versions iSM 3.3 et antérieures qui ne sont pas compatibles avec TLS ne sont pas prises en charge par le firmware de l'iDRAC 3.30.30.30 et versions ultérieures. Si l'iSM 3.3.0 est installé sur le firmware 3.30.30.30 de l'iDRAC, plusieurs événements avec ISM0050 sont observés dans le fichier log Lifecycle Controller.

REMARQUE : Lorsque le mode FIPS (Federal Information Processing Standards) est activé sur le système d'exploitation hôte ou l'iDRAC, la communication entre l'iSM et l'iDRAC n'est pas établie.

Paramètres de stratégie pour la connexion directe OS-BMC sur VMware ESXi

Vous trouverez ci-dessous les commandes et les paramètres affectés des paramètres de stratégie pour l'interface de connexion directe OS-BMC sur VMware ESXi :

```
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

Authentification des DLL et des objets partagés avant le chargement

Le chargement sécurisé des bibliothèques dans l'iSM permet d'éviter les attaques, telles que le piratage de DLL, le préchargement de DLL et la plantation binaire. Pour préserver l'iSM de ces attaques, cette fonctionnalité empêchera :

- le chargement des bibliothèques dynamiques à partir de n'importe quel chemin arbitraire,
- le chargement de toutes les bibliothèques non signées.

Cette fonctionnalité effectue la vérification du chemin d'accès et la vérification de la signature Authenticode pour les DLL et les objets partagés. Un événement d'échec est déclenché en cas d'échec de l'authentification des DLL et des objets partagés. En cas d'échec de la validation de l'authentification, la bibliothèque correspondante n'est pas chargée et est vérifiée dans le fichier log du système d'exploitation.

6

Fonctionnalités de surveillance de l'iSM

À l'aide de l'iSM, vous pouvez surveiller et gérer les aspects des performances du serveur, notamment le cycle d'alimentation, la sécurité, les alertes, ainsi que la gestion des périphériques pour optimiser et préserver l'intégrité et la disponibilité du système.

REMARQUE : **FullPowerCycle** et **SupportAssist on the Box** sont pris en charge uniquement sur les serveurs PowerEdge yx4x et yx5x.

Sujets :

Surveillance S.M.A.R.T

La fonctionnalité de surveillance S.M.A.R.T prend en charge les disques durs SATA activés avec SATA en mode AHCI et en mode RAID. Elle dispose d'une fonctionnalité intégrée pour surveiller les alertes S.M.A.R.T via les méthodes d'audit prises en charge par l'iDRAC pour les disques durs sous le contrôleur du chipset SATA. Auparavant, les alertes étaient surveillées par n'importe quel utilitaire Open source pour surveiller les disques durs définis en mode RAID.

Tableau 11. Valeurs d'attribut et description

Valeurs d'attribut	Description
Activé	Les contrôleurs de chipset SATA sont surveillés pour les événements S.M.A.R.T en temps réel.
Désactivé	La surveillance S.M.A.R.T est désactivée.
S/O	Le contrôleur du chipset SATA n'est pas disponible.

REMARQUE : Par défaut, l'attribut S.M.A.R.T est défini sur **Activé** ou **NA** lorsque la configuration ne prend pas en charge le chipset SATA.

La surveillance S.M.A.R.T est une fonctionnalité installée via le programme d'installation d'iSM. Vous pouvez installer ou modifier le package du programme d'installation d'iSM pour désactiver la fonctionnalité de surveillance S.M.A.R.T. Cette fonctionnalité est disponible sur un disque SATA pris en charge par Dell EMC avec des fonctionnalités S.M.A.R.T.

Si le disque est compatible avec la fonctionnalité S.M.A.R.T et que cette dernière est activée, l'iSM surveille les disques et génère des événements en conséquence. La période de surveillance par défaut est de 24 h et ne peut pas être configurée manuellement. Seuls les événements PDR16 (panne prédictive) et PDR22 (seuil de température dépassé) sont surveillés.

Si une erreur du système d'exploitation se produit suite à une erreur S.M.A.R.T du disque, l'événement n'est pas détecté par le système d'exploitation. Si les disques durs font partie d'un pool de stockage, l'iSM ne surveille pas les disques pour les échecs S.M.A.R.T.

Sur les serveurs PowerEdge yx3x, la surveillance S.M.A.R.T à l'aide du RAID logiciel est applicable uniquement pour l'événement PDR22.

REMARQUE : S.M.A.R.T nécessite également l'installation du firmware de l'iDRAC9 4.00.00.00 ou version ultérieure.

Informations sur le système d'exploitation

OpenManage Server Administrator partage actuellement les informations sur le système d'exploitation et le nom de l'hôte avec l'iDRAC. L'iDRAC Service Module (iSM) fournit les mêmes informations, telles que le nom du système d'exploitation hôte, l'adresse IP de l'hôte serveur, la version du système d'exploitation et le nom de domaine complet (FQDN) avec l'iDRAC. Les interfaces réseau sur le système d'exploitation hôte s'affichent également. Par défaut, la fonctionnalité de surveillance est activée. Cette fonctionnalité est disponible y compris lorsqu'OpenManage Server Administrator est installé sur le système d'exploitation hôte.

Vous pouvez également afficher les détails de l'interface réseau du système d'exploitation hôte par l'intermédiaire du plug-in client Redfish pour les navigateurs.

REMARQUE : La version minimale du firmware de l'iDRAC requise pour afficher des informations à l'aide du client Redfish est 3.00.00.00.

REMARQUE : L'iSM prend désormais en charge les clients DHCP dhclient, dhcpd, wicked, netplan et internes avec Network Manager. Si la configuration réseau sur le système d'exploitation hôte est configurée à l'aide d'un autre client DHCP, l'iSM ne peut pas surveiller les changements d'état de l'interface réseau, par exemple la configuration DHCP d'une interface. Par conséquent, il se peut que vous ne puissiez pas afficher la modification des informations de l'interface réseau du système d'exploitation hôte, comme l'état DHCP, le serveur DHCP, la passerelle par défaut et le serveur DNS dans les interfaces de l'iDRAC.

Réplication du journal du Lifecycle Controller dans le système d'exploitation

La réplication du journal Lifecycle Controller réplique les fichiers log Lifecycle Controller (LC) dans les fichiers log du système d'exploitation. Les événements, dont l'option Journal du système d'exploitation est sélectionnée comme cible dans la page Alertes ou dans les interfaces équivalentes RACADM ou WS-Man, sont répliqués dans les fichiers log du système d'exploitation. Ce processus est similaire à la réplication du journal des événements système (SEL) effectuée par OpenManage Server Administrator.

Le jeu par défaut des fichiers log à inclure dans les fichiers log du système d'exploitation est le même que les fichiers log configurés pour les alertes ou interruptions SNMP. Toutefois, les événements consignés dans le fichier log Lifecycle Controller après l'installation de l'iSM sont répliqués dans le fichier log du système d'exploitation. Si OpenManage Server Administrator est installé, cette fonctionnalité de surveillance est désactivée pour éviter les doublons d'entrées du journal SEL dans le fichier log du système d'exploitation.

Dans l'iSM, vous pouvez personnaliser l'emplacement de réplication des fichiers log Lifecycle Controller. Par défaut, les fichiers log Lifecycle Controller sont répliqués dans le groupe **Système** du dossier **Journaux Windows** dans l'**Observateur d'événements** Windows. Vous pouvez répliquer les journaux Lifecycle Controller vers un groupe existant ou créer un dossier dans le dossier **Journaux des applications et des services** dans l'**Observateur d'événements** Windows. Lorsque l'iSM est déjà installé et que le système d'exploitation hôte subit un redémarrage ou que l'iSM est redémarré et que l'iDRAC dispose de certains fichiers log Lifecycle Controller générés pendant cette période d'interruption de service de l'hôte, alors les fichiers log de l'iSM considèrent ces fichiers log Lifecycle Controller comme des événements passés dans le journal du système d'exploitation lorsque le service démarre.

REMARQUE : Vous pouvez choisir l'emplacement de réplication des fichiers log Lifecycle Controller uniquement lors de l'installation personnalisée de l'iSM ou de la modification de l'iSM.

REMARQUE : Le nom de la source des fichiers log Lifecycle Controller de l'iSM a été modifié de **iDRAC Service Module** à **Journal Lifecycle Controller**.

Récupération automatique du système

La fonctionnalité de récupération automatique du système est une horloge matérielle utilisée pour réinitialiser le serveur en cas de défaillance matérielle. Vous pouvez effectuer des opérations de récupération automatique du système, comme le redémarrage, le cycle d'alimentation ou la mise hors tension du serveur après l'intervalle de temps spécifié. Cette fonctionnalité s'active uniquement lorsque le minuteur de surveillance du système d'exploitation est désactivé. Si OpenManage Server Administrator est installé, cette fonctionnalité de surveillance est désactivée pour éviter les doublons d'entrées de l'horloge de surveillance.

Vous pouvez configurer trois paramètres dans cette fonction depuis les interfaces de l'iDRAC :

1. **État de la surveillance** : l'état par défaut est activé lorsque OMSA n'est pas présent et lorsque l'horloge de surveillance du BIOS ou du système d'exploitation est désactivée.
2. **Délai d'expiration de la surveillance** : la valeur par défaut est de 480 secondes. La valeur minimale est de 60 secondes et la valeur maximale est de 720 secondes.
3. **Délai d'expiration de la surveillance, Action de récupération ou Action de récupération automatique** : les actions peuvent être **Cycle d'alimentation**, **Mettre hors tension**, **Redémarrer** ou **Aucun**.

REMARQUE : Sous Windows, lorsque l'événement d'échec d'authentification DLL (SEC0704) est déclenché, l'action de récupération automatique du système définie sur la page des paramètres de l'iSM est exécutée. L'iSM doit être réparé ou réinstallé pour rétablir l'état par défaut.

Fournisseurs WMI (Windows Management Instrumentation)

Les fournisseurs Windows Management Instrumentation (WMI) disponibles avec l'iSM présentent les données matérielles par le biais de WMI (Windows Management Instrumentation). WMI est un ensemble d'extensions du modèle de pilotes Windows offrant une interface de système d'exploitation par laquelle les composants instrumentés fournissent des informations et des notifications. WMI est l'implémentation par Microsoft des normes Web-Based Enterprise Management (WBEM) et Common Information Model (CIM) publiées par le consortium DMTF (Distributed Management Task Force) pour gérer le matériel, les systèmes d'exploitation et les applications des serveurs. Les fournisseurs WMI participent à l'intégration avec les consoles de gestion des systèmes telles que Microsoft System Center et activent la rédaction de scripts de gestion des serveurs Microsoft Windows.

L'espace de nommage utilisé est `\\root\cimv2\dcim`. Les requêtes prises en charge sont **Énumération** et **Obtenir**. Vous pouvez utiliser toute interface client WMI telle que **WinRM**, **PowerShell**, **WMIC** ou **WBEMTEST** pour interroger les profils iDRAC pris en charge via le système d'exploitation hôte.

REMARQUE : Lorsque plusieurs classes WMI sont énumérées simultanément, l'iSM peut redémarrer la communication avec l'iDRAC. Aucune action requise.

Préparation au retrait d'un périphérique SSD PCIe NVMe

Vous pouvez supprimer un périphérique SSD (Solid State Device) PCIe (Peripheral Component Interconnect Express) NVMe (Non-Volatile Memory Express) sans arrêter ou redémarrer le système. Lorsque vous supprimez un périphérique, toutes les activités associées au périphérique doivent être arrêtées pour éviter une perte de données. Arrêtez toute activité manuellement avant d'effectuer la tâche de préparation au retrait. Pour éviter la perte des données, utilisez l'option **Préparation au retrait** pour pouvoir ensuite physiquement retirer le périphérique SSD PCIe NVMe. L'opération de préparation au retrait effectue la validation et vérifie si l'appareil est occupé par une activité ou non. Si l'appareil est occupé par une activité, l'opération de préparation au retrait s'arrête.

REMARQUE : L'opération **Préparation au retrait** NVMe n'est pas prise en charge sur le système d'exploitation VMware ESXi, lorsque l'appareil NVMe est configuré comme un appareil de transfert.

Suivez les conditions préalables documentées dans VMware avant d'exécuter une opération de préparation au retrait dans VMware ESXi.

Réinitialisation matérielle d'iDRAC à distance

L'iDRAC peut ne pas répondre pour plusieurs raisons. L'iSM peut réinitialiser entièrement un contrôleur iDRAC8 ou iDRAC9 qui ne répond pas en interrompant temporairement l'alimentation du contrôleur iDRAC sans affecter la production du système d'exploitation. Cette fonctionnalité ne peut être désactivée qu'à partir de la page de l'iSM à l'aide de l'interface de l'iDRAC.

Pour réinitialiser l'iDRAC, utilisez la commande shell suivante pour Windows PowerShell ou Linux :

```
./Invoke-iDRACHardReset
```

REMARQUE : La commande shell est prise en charge uniquement sur VMware ESXi 7.x.

Dans tous les systèmes d'exploitation ESXi, vous pouvez exécuter la réinitialisation de l'iDRAC à distance à l'aide de la commande à distance WinRM suivante :

```
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
```

REMARQUE : La fonctionnalité de réinitialisation matérielle de l'iDRAC à distance fonctionne uniquement avec l'iDRAC8 sur les serveurs PowerEdge yx3x ou ultérieurs et si elle est connectée au système d'exploitation en tant qu'administrateur.

l'accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte

À l'aide de serveurs PowerEdge, vous pouvez gérer le matériel ou le firmware d'un périphérique par l'intermédiaire de l'iDRAC en configurant un réseau iDRAC dédié. Par le biais du port réseau dédié, vous pouvez accéder aux interfaces UI, WS-Man et RACADM de l'iDRAC, ainsi qu'au client Redfish.

Les conditions préalables pour gérer le matériel ou le firmware, il convient en premier lieu de disposer d'une connexion dédiée entre un périphérique et l'interface de l'iDRAC prise en charge. À l'aide de l'accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte, vous pouvez vous connecter à une interface de l'iDRAC à partir d'un hôte ou d'une adresse IP de système d'exploitation, indépendamment de la connexion établie entre un périphérique et un réseau iDRAC dédié. Grâce à cette fonctionnalité, vous pouvez surveiller le matériel ou le firmware y compris lorsque l'iDRAC n'est pas connecté au réseau.

Vous pouvez sélectionner l'une des sous-fonctionnalités suivantes pour activer l'accès à l'iDRAC via le système d'exploitation hôte :

- **Accès par le biais de l'interface GUI, de WS-Man, de Redfish, de l'utilitaire RACADM à distance**
- **Interruptions SNMP intrabande**
- **Traps SNMP OMSA**
- **Accès via SNMP Get**

Si vous sélectionnez **Accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte**, toutes les sous-fonctionnalités sont sélectionnées par défaut. Si vous souhaitez sélectionner l'une des sous-fonctionnalités individuelles, vous pouvez sélectionner une fonctionnalité en particulier et l'activer.

Pour plus d'informations, reportez-vous à Accès à l'iDRAC par l'intermédiaire du système d'exploitation hôte.

Accès à l'iDRAC par le biais de l'interface GUI, de WS-Man, de Redfish et de l'utilitaire RACADM à distance

La fonctionnalité **Accès à l'iDRAC par le biais de l'interface GUI, de WS-Man, de Redfish et de l'utilitaire RACADM à distance** permet à un administrateur du système d'exploitation hôte d'accéder à distance aux interfaces iDRAC par le biais du système d'exploitation hôte. Saisissez l'URL `https:// <Host OS IP Address>: <ListenPortNumber>` dans le navigateur de la station de gestion à distance pour accéder à l'interface UI de l'iDRAC.

REMARQUE : ListenPortNumber est le numéro de port configuré lors de l'activation de la fonctionnalité iDRACAccessviaHostOS dans l'iSM.

Prise en charge intrabande des alertes SNMP de l'iDRAC

Tous les événements dont la cible est l'option **Trap SNMP** dans la page Alertes, ou dans les interfaces RACADM ou WS-Man équivalentes, peuvent être reçus sous la forme d'un trap SNMP par l'intermédiaire du système d'exploitation en utilisant l'iSM. Pour la version 3.0.0 (ou ultérieure) du firmware de l'iDRAC, cette fonctionnalité n'a pas besoin que la fonctionnalité de réplication LCL de l'iSM soit activée. Seuls les événements consignés dans le fichier log Lifecycle Controller après l'installation de l'iSM sont envoyés en tant qu'interruptions SNMP.

À l'aide de l'iSM, vous pouvez recevoir des alertes SNMP du système d'exploitation hôte similaires aux alertes générées par l'iDRAC.

Cette fonctionnalité est désactivée par défaut. Bien que le mécanisme d'alerte SNMP intrabande puisse coexister avec le mécanisme d'alerte SNMP de l'iDRAC, les journaux enregistrés peuvent présenter des alertes SNMP redondantes issues des deux sources. Il est recommandé d'utiliser l'option intrabande ou hors bande, mais pas les deux.

REMARQUE : Vous pouvez utiliser la fonctionnalité SNMP intrabande sur des serveurs PowerEdge yx3x ou versions ultérieures avec une version du firmware de l'iDRAC qui est au moins la version 2.30.30.30.

Pour plus d'informations, reportez-vous au livre blanc Alertes SNMP iDRAC intrabande

Mappage des journaux Lifecycle de l'iDRAC sur les alertes SNMP OMSA et OMSS

Le mappage des journaux Lifecycle de l'iDRAC sur les alertes SNMP OMSA et OMSS est désactivé par défaut et ne peut être activé que lorsque la fonctionnalité existante d'alertes SNMP de l'hôte est activée. Configurez la fonctionnalité à l'aide de l'interface RACADM de l'iDRAC ou de l'option **Modifier** du programme d'installation de l'iSM. Lorsqu'elle est activée, cette fonctionnalité convertit les enregistrements des journaux Lifecycle de l'iDRAC sélectionnés en alertes SNMP OMSA et OMSS correspondantes. L'ID d'objet (OID) de l'alerte OMSA ou OMSS qui en résulte correspond au produit OMSA ou OMSS, et le reste des varbinds d'alerte sont celles de l'iDRAC.

Le sous-agent SNMP iSM transmet les alertes mappées à la destination d'interruption SNMP configurée sur le système d'exploitation hôte. L'iSM n'ajoute ni ne modifie aucune destination d'interruption configurée par l'administrateur, et ne crée aucune règle de pare-feu sortant pour ouvrir les ports UDP (User Datagram Protocol) correspondants aux traps SNMP.

Lorsque la fonctionnalité d'alertes SNMP OMSA de l'hôte est désactivée, la fonctionnalité existante de transfert des journaux Lifecycle de l'iDRAC sous forme de traps SNMP est active. Le tableau suivant indique les différents états des fonctionnalités :

Tableau 12. États des fonctionnalités d'alerte SNMP OMSA et OMSS

iDRAC.ServiceModule. HostSNMPAlert	iDRAC.ServiceModule. HostSNMPOMSAAlert	Remarques
Oui	Oui	Le mappage SNMP de l'iDRAC vers OMSA est piégé et envoyé à la destination.
Oui	Non	Seules les alertes de l'iDRAC sont envoyées à la destination (condition par défaut).
Non	Oui	S/O
Non	Non	Aucune alerte n'est mappée ni envoyée à une quelconque destination.

L'iSM désactive automatiquement cette nouvelle fonctionnalité lorsqu'il détecte le service OMSA en cours d'exécution sur le système d'exploitation hôte, afin d'éviter la duplication des interruptions à la destination d'interruption.

Selon la configuration de la fonctionnalité ci-dessus, l'iSM transmet l'alerte iDRAC reçue à la destination d'interruption ayant l'un des ID d'objet suivants :

- ID d'objet iDRAC Enterprise (fonctionnalité existante)
- ID d'objet OMSA/OMSS Enterprise (introduit à partir d'iSM 4.1.0.0 et versions ultérieures)

REMARQUE : Si l'iSM 4.1.0.0 est installé avec la version 4.40.10 du firmware de l'iDRAC ou une version antérieure, où le mappage des alertes OMSA et OMSS n'est pas pris en charge par les interfaces de l'iDRAC (RACADM, interface utilisateur iDRAC), cette fonctionnalité peut être activée ou désactivée uniquement à l'aide du programme d'installation de l'iSM.

Activation à distance de WS-Man

Avec la fonctionnalité d'informations WMI, vous pouvez vous connecter à l'espace de nommage Microsoft Windows WMI hôte pour surveiller le matériel du système. L'interface WMI sur l'hôte est activée par défaut, et vous pouvez y accéder à distance. Cependant, si vous souhaitez accéder aux interfaces WMI à l'aide de l'adaptateur WMI de WINRM, vous devez l'activer manuellement, car il n'est pas activé par défaut. Cette fonction vous permet d'accéder à distance aux espaces de noms WMI de WINRM. Pour ce faire, activez-la au cours de l'installation.

Cette fonction est accessible à l'aide des commandes PowerShell. Les commandes utilisées sont les suivantes :

Tableau 13. Activation à distance de WS-Man

Commande	Description
`Enable-iSMWSMANRemote –Status enable – Forcereconfigure yes –Createselfsigncert yes – IPAddress <IP address> –Authmode Basic, Kerberos, Certificate`	Activation et configuration de la fonctionnalité WS-Man à distance
`Enable-iSMWSMANRemote –Status get`	Affichage de l'état de la fonctionnalité WS-Man à distance
`Enable-iSMWSMANRemote –Status disable`	Désactivation de la fonctionnalité WS-Man à distance
`Enable-iSMWSMANRemote –Status enable – Forcereconfigure yes –Createselfsigncert yes – IPAddress <IP address>`	Reconfiguration de la fonctionnalité WS-Man à distance

REMARQUE : Vous devez disposer d'un certificat d'authentification serveur et d'un protocole HTTPS pour utiliser cette fonctionnalité.

Mise à jour automatique de l'iSM

Vous pouvez mettre à jour l'iSM par l'intermédiaire du processus de mise à jour automatique de l'iDRAC.

REMARQUE : Si la mise à jour automatique de l'iSM est activée, la dernière version de l'iSM LC DUP doit être installée depuis la page Dell.com/support.

REMARQUE : Vous n'avez pas besoin de télécharger les mises à jour sur le site support.dell.com. Le package de l'iSM mis à jour est disponible localement dans l'iDRAC.

REMARQUE : L'iSM LC DUP dans l'iDRAC est supprimé lorsque l'option de suppression de l'iDRAC LC est utilisée. Vous devez télécharger l'iSM LC DUP à partir de la page Dell.com/support.

Tableau 14. Commandes d'installation et de mise à jour de l'iSM

Commandes à exécuter dans l'invite de commande	Descriptions
`dcism-sync.exe`	Pour installer ou mettre à jour l'iSM. Suivez la procédure de l'Assistant Installation.
`--help/-h`	Pour afficher le contenu de l'aide.
`--silent/-s`	Pour effectuer une mise à jour ou une installation silencieuse.
`--force/-f`	Pour désinstaller la version actuelle et installer le package de mise à jour disponible dans Lifecycle Controller. **REMARQUE :** cette option écrase la configuration précédente.
`--get–version/-v`	Pour obtenir des informations sur la version de la mise à jour et la version installée de l'iSM.
`--get–update/-g`	Pour télécharger les packages de mise à jour de l'iSM dans le répertoire spécifié par l'utilisateur

Tableau 14. Commandes d'installation et de mise à jour de l'iSM (suite)

Commandes à exécuter dans l'invite de commande	Descriptions
`dcism-sync.exe –p "feature"`	Pour installer des fonctionnalités spécifiques, identiques aux arguments de la CLI utilisés avec `msiexec.exe`. Par exemple, pour installer la fonctionnalité d'accès à l'iDRAC par l'intermédiaire de l'iDRAC du système d'exploitation de l'hôte sous Windows, saisissez `dcism-sync.exe -p "ADDLOCAL=IBIA"`.

Cycle d'alimentation complet (FullPowerCycle)

Le cycle d'alimentation complet (FullPowerCycle) est une fonctionnalité d'interface d'appel permettant de réinitialiser l'alimentation auxiliaire du serveur. Une quantité croissante de matériel de serveur s'exécute sur l'alimentation auxiliaire du serveur. Le dépannage de certains problèmes de serveur nécessite de débrancher physiquement le câble d'alimentation du serveur pour réinitialiser le matériel fonctionnant sur l'alimentation auxiliaire.

La fonctionnalité FullPowerCycle permet à l'administrateur de connecter ou de déconnecter l'alimentation auxiliaire à distance sans passer par le datacenter. Cette fonction est prise en charge sur les serveurs PowerEdge yx5x.

L'alimentation du système n'est pas affectée immédiatement après l'émission d'une **demande** FullPowerCycle. Au lieu de cela, une balise est définie pour l'émission d'une requête lors du passage du système à l'état S5. Pour que la fonctionnalité FullPowerCycle prenne effet, après l'exécution de la commande request, vous devez également exécuter la commande system shutdown. Si la balise est définie sur l'entrée S5, un état d'alimentation inférieure est forcé sur le système. Cette opération s'apparente au retrait et au remplacement de l'adaptateur secteur. Cette balise peut être supprimée à l'aide de la fonction **Annuler** tant que l'état S0 est défini sur le système avant que ce dernier ne passe à l'état S5.

Vous pouvez bénéficier des différentes options de FullPowerCycle sur votre système. Vous pouvez utiliser les commandes suivantes pour demander/annuler FullPowerCycle, ou en obtenir l'état, sur votre système :

Pour les systèmes d'exploitation Windows, des menus contextuels sont disponibles pour les options FullPowerCycle Activate (request), FullPowerCycle Cancel et FullPowerCycle get status.

Tableau 15. Commandes FullPowercycle pour le système d'exploitation Windows

Commandes à exécuter dans la console Power Shell	Descriptions
`Invoke-FullPowerCycle – request`	Pour demander FullPowerCycle sur votre système. **REMARQUE :** un message s'affiche pour indiquer que l'opération de cycle d'alimentation VirtualAC est déclenchée par le système d'exploitation du serveur.
`Invoke-FullPowerCycle - get status`	Pour obtenir l'état de FullPowerCycle sur votre système. **REMARQUE :** un message s'affiche pour indiquer que le système va être mis hors tension à la date et à l'heure indiquées.
`Invoke-FullPowerCycle - cancel`	Pour annuler FullPowerCycle sur le système.

Pour les systèmes d'exploitation Linux et VMware ESXi, des menus contextuels sont disponibles pour les options FullPowerCycle Activate (request), FullPowerCycle Cancel et FullPowerCycle get status.

Tableau 16. Commandes FullPowercycle pour le système d'exploitation Linux et Vmware ESXi

Commandes à exécuter dans la console Power Shell	Descriptions
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle request`	Pour demander FullPowerCycle sur votre système.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle cancel`	Pour annuler FullPowerCycle sur le système.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle get-status`	Pour obtenir FullPowerCycle sur votre système.

Les messages suivants sont affichés après chaque opération réussie de FullPowerCycle sur les fichiers log du système d'exploitation et LCL :

Message de demande :"`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`".

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

REMARQUE : La fonctionnalité FullPowerCycle est disponible pour le système d'exploitation ESXi 7.x, mais pas pour les systèmes d'exploitation ESXi 6.x.

REMARQUE : La fonctionnalité FullPowerCycle peut être utilisée uniquement avec un administrateur local ou de domaine ou des utilisateurs root ou sudo.

SupportAssist on the Box

SupportAssist permet de gagner du temps en rationalisant les tickets de support technique. Une collecte basée sur un événement crée une demande de service ouverte avec SupportAssist. Les collectes planifiées vous aident à surveiller et à entretenir votre environnement. Ces collectes comprennent les données d'informations sur le matériel, les fichiers log du contrôleur RAID, le système d'exploitation et les données d'application. Les fonctionnalités prises en charge sont les suivantes :

- **Enregistrement de SupportAssist** : l'iSM prend en charge l'enregistrement de SupportAssist. Il s'agit d'une activité ponctuelle. Vous pouvez saisir les informations requises, comme le nom, l'adresse e-mail et le nombre afin de terminer l'enregistrement.
- **Collecte SupportAssist** : la fonctionnalité de collecte SupportAssist dans l'iDRAC recueille des informations sur le matériel, le système d'exploitation et les données d'application pertinentes, pour ensuite les compresser.

SupportAssist procure également les avantages suivants :

- Identification proactive des problèmes
- Création de tickets automatisée
- Initiation de contacts d'assistance par un agent du support technique Dell

REMARQUE : Vous devez terminer l'enregistrement pour bénéficier de SupportAssist.

Vous pouvez visualiser les éléments suivants dans le tableau de bord SupportAssist.

Résumé de demande de service

Dans la session Résumé de demande de service, vous pouvez afficher des informations détaillées sur les demandes suivantes :

- Ouvert
- Fermé
- Soumis

Présentation de SupportAssist

Dans cette session, vous pouvez afficher des informations sur le **contrat de service**, notamment son type, sa date d'expiration et des détails relatifs aux paramètres **Collecte automatique** .

Dans l'onglet **Demandes de service**, vous pouvez également afficher la liste des demandes créées, ainsi que leur état, leur description, leur source, leur ID, leur date d'ouverture, leur date de clôture, etc.

En cliquant sur l'onglet **Journal de collecte**, vous pouvez afficher l'heure des collectes, l'ID de tâche, le type de collecte, les données recueillies, l'état des collectes, l'heure d'envoi, etc.

REMARQUE : Lorsque vous initiez manuellement une collecte SupportAssist depuis l'iDRAC, le périphérique de stockage de masse USB n'est pas exposé au système d'exploitation hôte. Le transfert des fichiers du contrôleur du système d'exploitation et des fichiers log collectés est traité en interne entre l'iDRAC et l'iSM.

REMARQUE : La collecte de données du système d'exploitation et d'application sur ESXi est prise en charge uniquement par les serveurs PowerEdge yx4x et versions ultérieures.

Enregistrement de SupportAssist

Avant de commencer le processus d'enregistrement, assurez-vous que l'iSM est installé et en cours d'exécution sur le système d'exploitation hôte et qu'une connexion Internet fonctionnelle est disponible.

1. Connectez-vous à l'iDRAC.

2. Dans le menu déroulant **Maintenance**, sélectionnez la fonctionnalité **SupportAssist**.
   L'Assistant **Enregistrement de SupportAssist** s'affiche.
3. Dans l'onglet **Bienvenue**, cliquez sur **Suivant**.
4. Dans l'onglet **Informations de contact et d'expédition**, indiquez vos coordonnées principales, dont votre **prénom**, votre **nom**, votre **numéro de téléphone**, votre **numéro secondaire**, votre **adresse e-mail**, le **nom de votre société**, la **ligne 1 de votre adresse**, la **ligne 2 de votre adresse**, votre **ville**, votre **État**, votre **code postal** et votre **pays**.

   REMARQUE : Vous pouvez ajouter vos coordonnées secondaires en cliquant sur l'option **Ajouter les coordonnées d'un contact secondaire**.

   REMARQUE : Pour poursuivre l'enregistrement, vous devez d'abord remplir toutes les informations requises.

5. Une fois les informations de contact et d'expédition remplies, cliquez sur **Suivant**.
6. Lisez le contrat de licence logicielle, sélectionnez l'option **J'accepte les termes du contrat de licence**, puis cliquez sur **Enregistrer**.

   REMARQUE : Le processus d'enregistrement peut prendre plusieurs minutes. Une fois l'enregistrement effectué, vous recevrez un e-mail de bienvenue de la part de SupportAssist à l'adresse e-mail spécifiée.

7. Dans l'onglet **Résumé**, affichez l'**ID d'enregistrement** et les paramètres actuels des **fonctionnalités automatiques**.
8. Pour fermer l'Assistant **Enregistrement de SupportAssist**, cliquez sur **Fermer**.
   Les informations de contact s'affichent au bas de la page SupportAssist.
9. Cliquez sur l'option **Modifier** pour apporter des modifications aux informations de contact principales ou secondaires.
10. Cliquez sur **Enregistrer** pour appliquer les modifications.

Collecte SupportAssist

La fonctionnalité Collecte SupportAssist dans l'iDRAC recueille des informations sur le matériel, le système d'exploitation et les données d'application pertinentes, pour ensuite les compresser. Exécutez l'outil Collector du système d'exploitation manuellement pour générer le rapport de collecte SupportAssist. À l'aide de l'iDRAC Service Module, l'outil Collector du système d'exploitation recueille automatiquement des informations pertinentes sur le système d'exploitation et le matériel. Les journaux de support sont collectés automatiquement, avec notamment des informations sur le système d'exploitation et les applications.

L'utilisation de l'iDRAC Service Module permet de réduire le nombre d'étapes manuelles nécessaires pour obtenir le rapport de support technique de Dell puisque le processus de collecte est automatisé.

Données à collecter

SupportAssist crée automatiquement et envoie une collecte au support technique de Dell en cas de déclenchement basé sur un événement ou là où vous avez configuré un rythme planifié. Vous pouvez collecter les types d'informations suivantes :

- **Informations sur le système**
- **Journaux de stockage**
- **Données de système d'exploitation et d'applications**
- **Journaux de débogage**

Vous pouvez également effectuer la collecte SupportAssist à partir d'un shell de système d'exploitation vers un chemin de fichier spécifié en utilisant :

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

REMARQUE : Cette commande shell est uniquement prise en charge sur l'iDRAC9 pour les serveurs PowerEdge yx4x et versions ultérieures ainsi que si vous êtes connecté au système d'exploitation en tant qu'administrateur.

REMARQUE : Sous un système d'exploitation Windows Core, vous devez accéder au chemin d'accès absolu pour exécuter la commande `Invoke-SupportAssistCollection.exe`.

Préférences de collecte

Vous pouvez sélectionner ou définir les préférences de collecte à l'aide de la fonctionnalité des préférences de collecte. Vous pouvez sélectionner l'un des types de préférences de collecte suivants pour l'enregistrement des rapports de collecte :

- **Envoyer maintenant** : vous recevez une notification vous signalant que **la tâche a bien été ajoutée à la liste d'attente des tâches** après avoir cliqué sur l'option **Collecter**.
- **Enregistrer localement**
- **Enregistrer sur le réseau** : si vous sélectionnez cette option, vous devez fournir des informations sur les **paramètres réseau**, notamment le **protocole**, l'**adresse IP**, le **nom de partage**, le **nom de domaine**, le **nom d'utilisateur** et le **mot de passe**.

Vous pouvez sélectionner les préférences de collecte de votre choix et cliquer sur **Collecter** pour recevoir les données.

REMARQUE : Cette fonctionnalité est disponible par défaut lors de l'installation de l'iDRAC Service Module 2.0 ou version ultérieure sur les systèmes exécutant les systèmes d'exploitation Microsoft ou Linux pris en charge. Vous ne pouvez pas désactiver cette fonction.

REMARQUE : La fonctionnalité de collecte des fichiers log du système d'exploitation de la collecte SupportAssist automatisée n'est pas prise en charge sur CentOS.

REMARQUE : La collecte de données du système d'exploitation et d'application sur ESXi est prise en charge uniquement par les serveurs PowerEdge yx4x et versions ultérieures.

Collecte de rapport anonyme

Vous pouvez effectuer des opérations de collecte et de chargement SupportAssist sans effectuer le processus d'enregistrement. Avant la version 3.0.2 de l'iDRAC Service Module, l'enregistrement était une condition préalable à l'exécution de la collecte SupportAssist.

Le firmware iDRAC pris en charge pour la collecte anonyme est l'iDRAC 3.15.15.15 dans les serveurs PowerEdge yx4x et yx5x. Pour l'iDRAC 2.60.60.60, la collecte se fait dans les serveurs PowerEdge yx3x.

REMARQUE : Vous pouvez effectuer un chargement de collecte SupportAssist anonyme en utilisant un nom d'utilisateur ou un mot de passe vide dans un environnement proxy sur les serveurs PowerEdge yx3x.

Corrélation des événements logiciels et pannes matérielles pour Microsoft SDS

Les fichiers du journal des événements pour les alertes ou les événements de pool de stockage matériel sont surveillés par l'iSM avec la fonctionnalité de corrélation de stockage de serveur. Le sous-système de stockage de serveur est surveillé lorsque les contrôleurs de stockage Dell EMC sont utilisés en mode RAID. Toutefois, dans les espaces de stockage (SS) ou les espaces de stockage direct (S2D), le sous-système de stockage de serveur est surveillé en mode transfert ou le chipset SATA est utilisé pour créer le pool de stockage. Avec cette fonctionnalité, les alertes définies par le matériel couvertes par le journal Lifecycle Controller (LC) et les alertes définies par le logiciel couvertes par les fichiers log du système d'exploitation sont fusionnées, et les alertes sont enregistrées dans les fichiers log Lifecycle de l'iDRAC.

Cette fonctionnalité est installée avec le package de l'iSM Service Module et est activée par défaut. Vous pouvez modifier les préférences dans les paramètres de l'iDRAC. Dans le cadre de la surveillance, l'iSM audite les fichiers log pour identifier les éventuels échecs et avertissements. L'iSM intégrera les événements de corrélation SS sur l'hôte à un événement Lifecycle Controller équivalent. Le SSLCMAP ne doit accéder qu'aux fichiers log Lifecycle et à l'alerte SupportAssist. Vous ne pouvez pas configurer le SSLCMAP sur une autre destination d'alerte dans l'iDRAC.

Vous trouverez ci-après les conditions préalables pour la collecte des journaux S2D :

- La fonctionnalité de corrélation d'événements SS doit être activée sur la page Service Module dans l'interface utilisateur de l'iDRAC.
- Le filtre PII doit être désactivé sur la page Service Module dans l'interface utilisateur de l'iDRAC.

Tableau 17. Messages d'événement Windows mappés sous les journaux LC surveillés sous la corrélation d'événements S2D

Source d'événement Windows : SourceID	Message d'événement Windows	Mappé sur le journal LC de l'iDRAC
Espaces de stockage : pilotes : 100	Le disque physique %1 n'a pas pu lire la configuration ou a renvoyé des données corrompues pour le pool de stockage %2. Par conséquent, il est possible que la configuration en mémoire ne soit pas la copie la plus récente de la configuration. Code de retour : %3	**ID de message** : SDS0001

Tableau 17. Messages d'événement Windows mappés sous les journaux LC surveillés sous la corrélation d'événements S2D (suite)

Source d'événement Windows : SourceID	Message d'événement Windows	Mappé sur le journal LC de l'iDRAC
Espaces de stockage : pilotes : 102	La majorité des disques physiques du pool de stockage %1 n'a pas réussi à effectuer la mise à jour de la configuration, ce qui a entraîné l'échec du pool. Code de retour : %2	**ID de message** : SDS0002
Espaces de stockage : pilotes : 103	La consommation de capacité du pool de stockage %1 a dépassé la limite de seuil définie sur le pool. Code de retour : %2	**ID de message** : SDS0003
Espaces de stockage : pilotes : 200	Windows n'a pas pu lire l'en-tête du disque physique %1. Si vous savez que le disque est toujours utilisable, réinitialiser l'intégrité du disque à l'aide de la ligne de commande ou de l'interface utilisateur peut résoudre cette condition d'échec et vous permettre de réaffecter le disque à son pool de stockage. Code de retour : %2	**ID de message** : SDS0004
Espaces de stockage : pilotes : 203	Une panne d'E/S s'est produite sur le disque physique %1. Code de retour : %2	**ID de message** : SDS0005
Espaces de stockage : pilotes : 300	Le disque physique %1 n'a pas pu lire la configuration ou a renvoyé des données corrompues pour l'espace de stockage %2. Par conséquent, il est possible que la configuration en mémoire ne soit pas la copie la plus récente de la configuration. Code de retour : %3	**ID de message** : SDS0006
Espaces de stockage : pilotes : 301	Les disques du pool n'ont pas pu lire la configuration ou ont renvoyé des données corrompues pour l'espace de stockage %1. Par conséquent, l'espace de stockage ne sera pas lié. Code de retour : %2	**ID de message** : SDS0007
Espaces de stockage : pilotes : 302	La plupart des lecteurs de pool hébergeant les métadonnées d'espace de l'espace de stockage %1 n'ont pas réussi la mise à jour des métadonnées d'espace, ce qui a entraîné l'échec de l'état du pool de stockage. Code de retour : %2	**ID de message** : SDS0008
Espaces de stockage : pilotes : 303	Les disques hébergeant des données de l'espace de stockage sont défaillants ou manquants. Par conséquent, aucune copie des données n'est disponible. Code de retour : %2	**ID de message** : SDS0009
Espaces de stockage : pilotes : 304	Un ou plusieurs disques hébergeant des données de l'espace de stockage %1 ont échoué ou sont manquants. Par conséquent, au moins une copie des données n'est pas disponible. Toutefois, au moins une copie des données est toujours disponible. Code de retour : %2	**ID de message** : SDS0010
Espaces de stockage : pilotes : 306	La tentative de mappage ou d'allocation de stockage supplémentaire pour l'espace de stockage %1 a échoué. Un échec d'écriture liée à la mise à jour des métadonnées de	**ID de message** : SDS0011

Tableau 17. Messages d'événement Windows mappés sous les journaux LC surveillés sous la corrélation d'événements S2D (suite)

Source d'événement Windows : SourceID	Message d'événement Windows	Mappé sur le journal LC de l'iDRAC
	l'espace de stockage en est la cause. Code de retour : %2	
Espaces de stockage : pilotes : 307	La tentative d'annulation d'adressage ou de suppression de l'espace de stockage %1 a échoué. Code de retour : %2	**ID de message** : SDS0012

REMARQUE : le document *Guide de référence des messages d'événement et d'erreur* fournit des informations sur les événements et les erreurs générés par le firmware et d'autres agents qui surveillent les composants du système.

REMARQUE : le champ PPID n'est pas enregistré pour les alertes correspondant à un pool de stockage. L'iSM réplique ces alertes dans les fichiers log Lifecycle Controller dans l'iDRAC avec le PPID « NA ».

Collecte des fichiers log des espaces de stockage direct avec la collecte SupportAssist

La demande de collecte SupportAssist (SAC) entraine la collecte et l'enregistrement des fichiers log des espaces de stockage direct (S2D). Cette fonctionnalité est disponible uniquement sur les systèmes d'exploitation Microsoft Windows. La fonctionnalité de corrélation des événements SDS doit être activée pour que la SAC inclue ce rapport de collecte de journal.

Fichiers log S.M.A.R.T pour les disques et chipset dans le rapport de collecte SupportAssist

L'iDRAC Service Module (iSM) collecte les données des fichiers log S.M.A.R.T à partir du pilote de chipset SATA lorsque la collecte de SupportAssist (SAC) est demandée en temps réel.

Cette fonctionnalité nécessite que la fonctionnalité **Surveillance S.M.A.R.T** soit activée dans iSM et que l'option **Journaux de stockage** soit activée dans les préférences de collecte SupportAssist dans l'iDRAC.

Journal S.M.A.R.T d'historique

Les fichiers log S.M.A.R.T d'historique sont collectés à partir d'un chipset de pilote de contrôleur SATA ou d'un périphérique de contrôleur RAID logiciel Windows toutes les 24 heures, si cette fonctionnalité est activée. Les fichiers log S.M.A.R.T d'historique sont collectés dans un intervalle planifié dans l'iSM et envoyés à l'iDRAC. L'iDRAC regroupe les fichiers log S.M.A.R.T d'historique dans le cadre de la collecte SupportAssist que vous configurez. Les fichiers log S.M.A.R.T d'historique sont activés ou désactivés à l'aide du programme d'installation de l'iSM ou de l'interface de ligne de commande dcismcfg.

REMARQUE : Cette fonctionnalité nécessite le firmware de l'iDRAC9 version 4.40.00.00 ou ultérieure.

Dans la collecte SupportAssist, ces fichiers log sont disponibles à l'adresse `\tsr\storagelog\Smartlogs-nightly.zip`.

Noms de fichier des S.M.A.R.T. précédents Les fichiers log fournis par l'iDRAC Service Module se composent du nom de l'hôte sous la forme d'un préfixe suivi d'une valeur alphanumérique. Par exemple : HostRD20200414.json.

Outil d'interface de ligne de commande de l'iDRAC Service Module : dcismcfg

L'utilitaire dcismcfg permet d'activer ou de désactiver la fonctionnalité de collecte de journaux S.M.A.R.T d'historique. Tous les systèmes d'exploitation prennent en charge cet utilitaire. Une fois que l'utilitaire est utilisé pour activer ou désactiver la fonctionnalité de collecte des journaux S.M.A.R.T d'historique, le cycle d'interrogation suivant de la surveillance S.M.A.R.T remplit la demande.

Exécutez les commandes suivantes pour activer ou désactiver la fonctionnalité de collecte des journaux S.M.A.R.T d'historique.

Pour Windows, exécutez l'une des commandes suivantes :

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

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

Pour Linux, exécutez l'une des commandes suivantes :

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

L'utilitaire dcismcfg doit être exécuté en tant qu'administrateur ou utilisateur root et est pris en charge par la version de firmware de l'iDRAC 4.40.00.00 et ultérieures.

REMARQUE : La collecte des journaux S.M.A.R.T d'historique est une sous-fonctionnalité de la fonctionnalité de surveillance S.M.A.R.T. Toutefois, tout en activant la collecte des journaux S.M.A.R.T, si la fonctionnalité de surveillance S.M.A.R.T. n'est pas activée, vous êtes invité à activer la surveillance S.M.A.R.T. afin d'activer la collecte des journaux d'historique.

Paramètres de collecte SupportAssist

Pour ouvrir la page des paramètres de collecte SupportAssist, accédez au tableau de bord SupportAssist dans l'iDRAC et sélectionnez **Paramètres** dans le menu déroulant.

iSM 3.4.0, ou versions ultérieures, prend en charge la collecte de données de système d'exploitation et d'application filtrée et non filtrée **Collecte OSApp** sur ESXi. Cette sélection peut être effectuée à partir des **Préférences de collecte**.

Une collecte sélectionnée non filtrée contient des fichiers log **Support machine virtuelle** pour **Journaux**, **Réseau**, **Stockage**, **Configuration**, **Programme d'installation**, **Machine virtuelle bloquée**, **Capture instantanée des performances**, **Machines virtuelle** et **Profils d'hôtes**.

Une collecte filtrée contient des fichiers log **Support machine virtuelle** pour **Stockage**, **Configuration**, **Programme d'installation**, **Machine virtuelle bloquée**, **Capture instantanée des performances**, **Machines virtuelles** et **Profils d'hôtes**.

Définition du répertoire d'archivage

Vous pouvez stocker les copies des collectes effectuées par SupportAssist dans un répertoire. Cliquez sur le bouton **Définir le répertoire d'archivage** pour spécifier l'emplacement.

Informations d'identification

Vous pouvez inclure les informations d'identification dans les données envoyées en cliquant sur le menu déroulant et en sélectionnant **Non** ou **Oui**.

Notifications d'e-mail

Vous pouvez paramétrer les notifications par e-mail lorsqu'un nouveau ticket de support est ouvert ou qu'une nouvelle collecte SupportAssist a été téléchargée. Dans le menu déroulant **Recevoir des notifications par e-mail**, sélectionnez **Non** ou **Oui**.

Vous pouvez également sélectionner la préférence linguistique. Les langues suivantes sont disponibles :

- **Anglais**
- **Allemand**
- **Français**
- **Japonais**
- **Espagnol**
- **Chinois simplifié**

Collecte automatique

La fonctionnalité de collecte automatique est activée par défaut. Pour désactiver cette fonctionnalité, utilisez le menu déroulant pour sélectionner **Activer** ou **Désactiver**.

Vous pouvez également planifier l'heure de la collecte en sélectionnant l'une des options suivantes dans le menu déroulant **Planifier la collecte automatique** :

- **Hebdomadaire**
- **Mensuelle**
- **Tous les trimestres**
- **Jamais**

Vous pouvez également rendre la collecte automatique récurrente.

Pour afficher le Rapport de recommandation ProSupport Plus, sélectionnez **Oui** dans le menu déroulant **Envoyer le Rapport de recommandation ProSupport Plus**.

Une fois vos préférences sélectionnées, cliquez sur **Appliquer** pour enregistrer les modifications.

Envoi automatique du disque SupportAssist de l'iDRAC Service Module

Si le serveur rencontre un **PDR16 et PDR63**, le support Dell EMC vous avertit par e-mail de l'échec prédictive ou de la défaillance d'un bloc de disque sur un SSD, sous réserve des conditions de licence en vigueur. Une fois l'e-mail reçu, vous devez effectuer un suivi et fournir l'adresse du service au support Dell EMC pour la livraison des pièces expédiées.

Configuration de la fonctionnalité SNMP intrabande Get-Linux

Installez et configurez le package **Net-SNMP** pour accepter les requêtes SNMP à partir de systèmes distants. Cette fonction est désactivée par défaut.

Pour installer la fonctionnalité SNMP intrabande Get via le programme d'installation setup.sh, procédez comme suit :

1. Pour démarrer l'installation de l'iSM, exécutez `./setup.sh` sur la ligne de commande.
2. Lisez et acceptez le contrat de licence pour poursuivre l'installation.
   La liste des fonctionnalités apparaît.
3. Pour sélectionner la sous-option **Accès via SNMP Get** sous la fonctionnalité **Accès à l'iDRAC via le système d'exploitation hôte**, saisissez **4.c**, puis appuyez sur **Entrée**.
4. Une fois la fonctionnalité activée, saisissez **I**, puis appuyez sur **Entrée** pour lancer le processus d'installation des fonctionnalités sélectionnées.
5. Une fois l'installation terminée, démarrez le processus de l'iDRAC Service Module.
   Si le service de l'agent SNMP n'est pas activé sur l'iDRAC, l'iSM configure et active l'agent SNMP.
6. Pour afficher les propriétés de l'agent SNMP, accédez à **Paramètres** dans l'interface utilisateur d'iDRAC.
7. Cliquez sur **Configuration de l'iDRAC Service Module**.
8. Sous la session **Surveillance**, vérifiez que l'option **SNMP Get via le système d'exploitation hôte** est activée.
9. Ouvrez une nouvelle fenêtre « **Configuration PuTTY** », indiquez votre adresse IP de nom de l'hôte, puis cliquez sur **Ouvrir**.
10. Cliquez sur **Oui** pour activer l'**alerte de sécurité PuTTY**.
11. Connectez-vous à l'iDRAC avec les informations d'identification correspondantes.
12. Saisissez `racadm get iDRAC.ServiceModule.HostSNMPGet` et appuyez sur Entrée.
    Assurez-vous que **HostSNMPGet** est activé.

    Si la fonctionnalité SNMP intrabande Get n'est pas active lors de l'installation de l'iDRAC Service Module, vous pouvez l'activer en utilisant les commandes iDRAC UI ou RACADM suivantes :

    - À l'aide de l'interface utilisateur de l'iDRAC : **Paramètres de l'iDRAC -> Paramètres -> Configuration de l'iDRAC Service Module -> Activer SNMP Get via le système d'exploitation hôte -> Activer ou Désactiver**
    - À l'aide de RACADM : **racadm set idrac.servicemodule.HostSnmpGet « Activé » ou « Désactivé »**

    REMARQUE : Les commandes de l'interface utilisateur de l'iDRAC ou RACADM pour la fonctionnalité SNMP Get intrabande sont uniquement applicables aux serveurs PowerEdge yx4x et yx5x. Sur les serveurs PowerEdge yx3x, vous devez utiliser le programme d'installation de l'iSM pour activer et désactiver cette fonctionnalité.

Lorsque la fonctionnalité SNMP Get est activée, cela crée un compte iDRAC **iSMSnmpUser** pour la prise en charge en interne de SNMPv3. Si le compte existe déjà, l'iSM génère le message d'erreur suivant et la fonctionnalité est désactivée.

```
Unable to create the user \"iSMSnmpUser"\ on iDRAC because the username already
exists. The SnmpGet via Host OS feature will be disabled.
```

Dans ce cas, vous devez supprimer « iSMSnmpUser » dans l'iDRAC, puis désactiver et activer à nouveau la fonctionnalité **Activer SNMP Get via le système d'exploitation hôte** sur l'interface utilisateur de l'iDRAC. Le compte « iSMSnmpUser » créé par l'iSM est supprimé lorsque la fonctionnalité est désactivée ou lorsque l'iSM est désinstallé. La fonctionnalité SNMP Get ne fonctionne pas lorsque le nombre maximal de comptes iDRAC créés (16) est atteint et qu'il n'y a aucun logement supplémentaire disponible.

Configuration de la fonctionnalité SNMP intrabande Get-Windows

La fonctionnalité SNMP intrabande Get vous permet d'interroger les données de gestion des systèmes via le service SNMP sur le système d'exploitation hôte. La configuration et l'activation des services SNMP hôtes sont une condition préalable pour cette fonctionnalité.

Le service SNMP de l'iDRAC doit être activé. S'il n'est pas activé, l'iDRAC Service Module activera et configurera le service SNMP sur l'iDRAC. Cette fonctionnalité peut être activée ou désactivée à l'aide de l'une des interfaces iDRAC ou du programme d'installation.

Cette fonctionnalité prend en charge SNMP v1 et v2 sur les systèmes d'exploitation Microsoft Windows et SNMP v1, v2 et v3 sur les systèmes d'exploitation Linux.

REMARQUE : Les commandes iDRAC UI ou RACADM pour la fonctionnalité SNMP Get intrabande sont uniquement applicables aux serveurs PowerEdge yx4x et versions ultérieures.

REMARQUE : l'iDRAC Service Module prend uniquement en charge l'iDRAC SNMP OID 1.3. 6.1. 4.1.674.10892.5.

Lanceur de l'interface utilisateur de l'iDRAC

À l'aide de l'iDRAC Service Module 3.1 ou version ultérieure, vous pouvez lancer l'interface utilisateur de l'iDRAC à partir de votre système local. Double-cliquez sur l'icône **Lanceur de l'interface utilisateur de l'iDRAC**. La page de connexion de l'interface utilisateur de l'iDRAC s'ouvre dans le navigateur par défaut. Utilisez vos informations d'identification iDRAC pour vous connecter à la page d'accueil de l'iDRAC. Cette action est prise en charge uniquement sur les systèmes d'exploitation Microsoft Windows. Le raccourci est disponible dans le menu Démarrer une fois l'iSM 3.1 ou version ultérieure installé.

REMARQUE : Lorsque l'iSM est désactivé, l'icône du lanceur de l'interface utilisateur de l'iDRAC est également désactivée.

REMARQUE : Si le proxy du navigateur par défaut est défini de manière à utiliser le proxy du système, le lancement de l'interface utilisateur de l'iDRAC échoue. Vous devez copier l'adresse IP depuis la barre d'adresse et l'entrer dans la liste des exceptions des « paramètres du proxy ».

Authentification unique à l'interface utilisateur de l'iDRAC à partir du bureau des administrateurs sur le système d'exploitation hôte

Présentation

Les administrateurs d'hôte peuvent lancer l'iDRAC à partir du système d'exploitation hôte à l'aide d'une IPv6. Le lanceur de l'authentification unique (SSO) de l'iDRAC nécessite un environnement de bureau tel que GNOME ou K Desktop Environment (KDE) sur le système d'exploitation hôte.

.

REMARQUE : Les administrateurs ne peuvent pas accéder à cette fonctionnalité sur le système d'exploitation hôte.

La fonctionnalité d'authentification unique (SSO, Single Sign-On) permet à un administrateur du système d'exploitation authentifié d'accéder directement à l'interface Web de l'iDRAC sans devoir se connecter séparément à l'aide des informations d'identification d'administrateur de l'iDRAC. Après l'installation de cette fonctionnalité, un raccourci appelé **Invoke-iDRACLauncher** sera créé dans le **menu Programmes** sur les systèmes d'exploitation Microsoft Windows. Sur les systèmes d'exploitation Linux, l'iSM crée un raccourci sous **Applications**, sur lequel vous pouvez double-cliquer pour lancer le tableau de bord de l'iDRAC. L'iSM fournit une interface de ligne de commande appelée **Invoke-iDRACLauncher** sur les systèmes d'exploitation Microsoft Windows et **Invoke-iDRACLauncher.sh** sur les systèmes d'exploitation Linux.

Vous pouvez configurer l'iDRAC Service Module via une adresse IPv6. Par défaut, la communication est établie via IPv4. En cas d'échec, une nouvelle tentative de communication est effectuée via IPv6. Un message d'erreur est audité en cas d'échec de la communication.

Vous pouvez mettre à jour l'adresse IPv6 à l'aide des commandes de **connexion directe RACADM**. La fonctionnalité d'authentification unique (SSO) sur IPv6 est valide uniquement lorsque IPv6 est configuré avec une adresse locale unique valide (ULA). Par exemple :

```
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
```

Vous pouvez choisir entre deux types de privilèges pour se connecter à l'iDRAC.

- Compte en **Lecture seule** : une installation rapide ou classique d'iSM installe le **Lanceur de l'authentification unique (SSO) de l'iDRAC**, permettant à l'administrateur d'ouvrir une session dans l'iDRAC en tant que compte en **Lecture seule**. Outre la possibilité de consulter l'état d'intégrité des composants, les journaux et l'inventaire, d'autres opérations **SupportAssist** nécessaires au personnel de maintenance sont autorisées.
- Compte **Administrateur** : l'installation de cette fonctionnalité se fait en sélectionnant le privilège d' **administration** et permet à l'administrateur du système d'exploitation hôte d'ouvrir une session dans l'iDRAC en tant qu'opérateur. À l'aide de ce compte, vous pouvez effectuer toutes les opérations qu'un utilisateur root de l'iDRAC peut effectuer, à l'exception de la configuration ou de la suppression des utilisateurs de l'iDRAC ou de l'effacement du journal Lifecycle.

REMARQUE : Les comptes du système d'exploitation hôte sans droits d'administration ne peuvent pas initier le lanceur de l'interface utilisateur de l'iDRAC si la version du firmware de l'iDRAC est 4.00.00.00 ou ultérieure et si la communication entre l'iDRAC et iSM ne s'effectue pas via IPv4.

REMARQUE : Reportez-vous au *Guide de l'utilisateur iDRAC 9* pour consulter les détails relatifs aux privilèges attribués à un compte *Opérateur* ou en *Lecture seule*.

Désactiver l'authentification unique dans l'iDRAC à partir du système d'exploitation hôte : vous pouvez également choisir de **désactiver** complètement cette fonctionnalité. Lorsque l'iSM est installé en désactivant cette fonctionnalité, le **Lanceur de l'interface utilisateur de l'iDRAC** lance la page de connexion de l'iDRAC à l'aide du navigateur par défaut.

Invoke-iDRACLauncher est indépendant du service iSM et peut être appelé même si le service iSM est arrêté.

Lorsque les navigateurs ne sont pas installés sur le système d'exploitation hôte ou que **Invoke-iDRACLauncher** n'est pas en mesure de lancer l'iDRAC en raison de problèmes de navigateur, une session est néanmoins créée dans l'iDRAC. À l'aide d'un compte d'administrateur de l'iDRAC, vous pouvez vous connecter à l'iDRAC et supprimer les sessions.

Le lanceur de l'interface utilisateur de l'iDRAC se comporte différemment en fonction de l'état du paramètre de **connexion directe entre le système d'exploitation et l'iDRAC**.

- Lorsque le paramètre de **connexion directe entre le système d'exploitation et l'iDRAC** est désactivé dans l'iDRAC, **Invoke-iDRACLauncher** vous invite à activer la connexion directe OS-BMC en mode USBNIC.
- Lorsque le paramètre de **connexion directe entre le système d'exploitation et l'iDRAC** est déjà configuré en mode LOM, le programme de lancement de l'interface utilisateur de l'iDRAC ne lance pas l'interface utilisateur de l'IDRAC.
- Lorsque le paramètre de **connexion directe entre le système d'exploitation et l'iDRAC** est désactivé dans l'iDRAC et que l'option **Désactiver la configuration locale d'iDRAC à l'aide des paramètres** est également désactivée ou que le mode de verrouillage est activé dans l'iDRAC, l'interface utilisateur de l'iDRAC n'est pas lancée.

  REMARQUE : Lorsque les options **Configuration locale à l'aide des paramètres** ou **Configuration locale à l'aide de RACADM** sont désactivées dans l'iDRAC, l'écran de connexion de l'iDRAC s'affiche.

Lorsqu'une session iDRAC par authentification unique (SSO) est active sur le système d'exploitation hôte, la fermeture du terminal associé entraîne également la fermeture du navigateur où la session en authentification unique (SSO) a été établie.

REMARQUE : Assurez-vous que vous appelez le **lanceur de l'interface utilisateur de l'iDRAC** à partir d'une interface compatible avec l'interface utilisateur et prise en charge par l'interface utilisateur. L'authentification unique (SSO) sur IPv4 ne fonctionne pas lorsque vous modifiez le troisième octet de l'adresse IP de l'USB-NIC. L'utilisation de cette fonctionnalité avec IPv6 nécessite le firmware de l'iDRAC9 4.00.00.00 ou une version ultérieure.

Conditions préalables

Packages Linux :

1. Navigateur tel que Mozilla Firefox
2. Sudo
3. Serveurs PowerEdge yx4x et versions ultérieures
4. Versions de firmware de l'iDRAC 3.30.30.30 et ultérieures

   REMARQUE : L'authentification unique (SSO) sur IPv6 est prise en charge sur le firmware iDRAC 4.00.00.00 et versions ultérieures.

Limitations pour les systèmes d'exploitation Linux

Limitations du **lanceur de l'authentification unique (SSO) de l'iDRAC** sous les systèmes d'exploitation Linux ne prenant pas en charge les éléments suivants :

1. Utilitaires de bureau autres que GNOME
2. Navigateurs autres que Mozilla Firefox

REMARQUE : Lors de la désactivation de la configuration locale sur KC ou RACADM dans l'iDRAC, l'écran de connexion de l'iDRAC s'affiche.

Communications IPv6 entre l'iSM et l'iDRAC via une connexion directe entre le système d'exploitation et BMC

L'iSM prend en charge à la fois les modes de communication IPv4 et IPv6. Une fois l'iSM installé, le service de l'iSM tente de se connecter à l'iDRAC à l'aide d'une adresse IPv4 link-local. S'il n'y a pas d'adresse IP sur l'interface de la carte NIC USB de l'hôte, l'iSM tente de configurer l'adresse IPv4 du côté de l'hôte. Cette configuration de l'interface de la carte NIC USB sur le système d'exploitation hôte par l'iSM n'est effectuée qu'une seule fois. L'iSM reste déconnecté de l'iDRAC si des modifications ultérieures sont apportées à la configuration de l'interface de la carte NIC USB et peuvent rompre la communication entre l'iSM et l'iDRAC. Si la connexion échoue, même après configuration de l'adresse IPv4, l'iSM tente de se connecter à l'iDRAC à l'aide d'IPv6.

REMARQUE : Cette fonctionnalité est prise en charge uniquement sur les systèmes d'exploitation Linux.

REMARQUE : Si la pile réseau IPv6 est désactivée sur le système d'exploitation hôte, l'iSM tente à nouveau de communiquer avec l'iDRAC à l'aide d'IPv4.

Si l'un ou l'autre des protocoles est désactivé, l'iSM n'essaiera pas de se connecter à l'iDRAC à l'aide du protocole désactivé.

REMARQUE : Si la version du firmware de l'iDRAC ne prend pas en charge IPv6 sur la carte NIC USB, la connexion entre l'iSM et l'iDRAC est établie à l'aide d'IPv4.

Les messages d'audit respectifs sont enregistrés dans le journal par l'iSM, indiquant la version du protocole utilisé par l'iSM pour se connecter à l'iDRAC.

REMARQUE : Si la carte NIC USB de l'iDRAC est déjà configurée uniquement à l'aide d'une adresse IPv6 sur le système d'exploitation hôte, et que l'iSM est ensuite installé sur l'hôte, alors la communication entre l'iDRAC et l'iSM se met à utiliser le protocole IPv4.

Fonctionnalités non prises en charge avec le protocole IPv6

Les fonctionnalités qui ne sont pas prises en charge lorsque l'iSM est configuré avec le protocole IPv6 et que la configuration IPv4 n'est pas disponible sur l'interface de la carte NIC USB sont les suivantes :

- Accès à l'iDRAC intrabande
- SNMP intrabande Get

- idrac.local et drac.local
- Mise à jour automatique de l'iSM

7

Questions fréquentes

Cette section répertorie les questions fréquentes sur l'iDRAC Service Module (iSM).

Basculement du protocole IPv4 au protocole IPv6 pour la communication entre l'iSM et l'iDRAC

La communication entre l'iSM et l'iDRAC bascule du protocole IPv4 au protocole IPv6, lorsque vous exécutez `ifconfig iDRAC down`, lorsque l'iSM communique avec l'iDRAC via IPv4.

Tableau 18. Modification du protocole lors de l'exécution de la commande

Fonctionnalité/ Protocole	IPv4 sous Linux	IPv4 sous Windows	IPv6 sous Linux	IPv6 sous Windows
informations sur OS	Oui	Oui	Oui	Oui
WMI	S/O	Oui	S/O	Oui
SupportAssist	Oui	Oui	Oui	Oui
Invoke-iDRACLauncher	Oui	Oui	Oui	Oui
Invoke-iDRACHardReset	Oui	Oui	Oui	Oui
Invoke-VirtualPowerCycle	Oui	Oui	Oui	Oui
SNMP Get de l'hôte	Oui	Oui	Non	Non
Interruptions SNMP intrabande	Oui	Oui	Oui	Oui
Traps SNMP OMSA intrabande	Oui	Oui	Oui	Oui
Lanceur de l'authentification unique (SSO) de l'iDRAC	Oui	Oui	Oui (ULA)	Oui (ULA)
Récupération automatique du système	Oui	Oui	Oui	Oui
Accès intrabande iDRAC	Oui	Oui	Non	Non
Mise à jour automatique d'iSM	Oui	Oui	Non	Non
Préparation du retrait de NVMe	Oui	Oui	Oui	Oui
Corrélation entre les serveurs de stockage	Oui	Oui	Oui	Oui
Journaux S.M.A.R.T sur AHCI	Oui	Oui	Oui	Oui

Plusieurs sessions iDRAC par connexion à authentification unique (SSO) sont actives sur IPv4 et sur l'adresse ULA

Lorsque l'utilisateur modifie l'adresse IPv4 ou ULA dans l'iSM, plusieurs sessions sont créées. L'ancienne adresse IP est finalement supprimée.

Solution de contournement : supprimez manuellement l'ancienne adresse IP.

Dois-je désinstaller OpenManage Server Administrator avant d'installer ou d'exécuter l'iSM ?

Nombre Toutefois, avant d'installer ou d'exécuter l'iSM, assurez-vous que vous avez arrêté les fonctionnalités OpenManage Server Administrator fournies par l'iSM.

REMARQUE : La désinstallation d'OpenManage Server Administrator n'est pas obligatoire.

Comment savoir si l'iSM s'exécute sur mon système ?

Pour vérifier que l'iSM est installé sur votre système :

- Sous Windows :

  Exécutez la commande `service.msc`. Recherchez dans la liste des services un service nommé **DSM iDRAC Service Module**.

- Sous Linux :

  Exécutez la commande `/etc/init.d/dcismeng status`. Si l'iSM est installé et en cours d'exécution, l'état qui s'affiche est **en cours d'exécution**.

- Sur VMware ESXi :

  Exécutez la commande `/etc/init.d/dcism-netmon-watchdog status`. Si l'iSM est installé et en cours d'exécution, l'état qui s'affiche est **en cours d'exécution**.

REMARQUE : Utilisez la commande `systemctl status dcismeng.service` au lieu de la commande `init.d` pour déterminer si l'iSM est installé sur le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux.

Comment connaître la version de l'iSM installée sur mon système ?

Pour vérifier la version de l'iSM installée sur le système, cliquez sur **Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités**. La version d'iSM installée est indiquée dans l'onglet **Version**. Vous pouvez aussi vérifier la version via **Mon poste de travail** > **Désinstaller ou modifier un programme**

Sous le système d'exploitation Linux, exécutez la commande suivante :

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

Sous le système d'exploitation VMware ESXi, exécutez la commande suivante :

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

Quel est le niveau de permission minimum requis pour installer l'iSM ?

Pour installer l'iSM, vous devez disposer de privilèges Administrateur sur le système d'exploitation.

Je vois le message « L'iSM ne peut pas communiquer avec l'iDRAC à l'aide du canal d'intercommunication entre le système d'exploitation et l'iDRAC » dans le journal du système d'exploitation, alors que la connexion directe entre le système d'exploitation et l'iDRAC via USBNIC est configurée correctement. Pourquoi ce message s'affiche-t-il ?

L'iSM utilise la connexion directe entre le système d'exploitation et l'iDRAC via USBNIC afin d'établir la communication avec iDRAC. Parfois, la communication n'est pas établie bien que l'interface USBNIC soit configurée avec des points de terminaison IP appropriés. Ce problème peut survenir lorsque la table de routage du système d'exploitation hôte possède plusieurs entrées sous le même masque cible et que la destination USBNIC n'est pas la première dans la liste de l'ordre de routage.

Tableau 19. Détails de l'ordre de routage

Destination	Passerelle	Masque générique	Indicateurs	Mesure	Réf.	Utiliser Iface
Par défaut	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

Dans l'exemple, **enp0s20u12u3** est l'interface USBNIC. Le masque cible lien-local est répété et l'interface USBNIC n'est pas la première dans la liste. Cela entraîne un problème de connectivité entre l'iSM et iDRAC sur la connexion directe entre le système d'exploitation et iDRAC. Pour résoudre le problème de connectivité, assurez-vous que l'adresse IPv4 USBNIC de l'iDRAC (la valeur par défaut est 169.254.1.1) est accessible depuis le système d'exploitation hôte. Si elle n'est pas accessible depuis le système d'exploitation hôte, effectuez l'une des opérations suivantes :

- Modifiez l'adresse USBNIC iDRAC sur un masque cible unique.
- Supprimez les entrées indésirables de la table de routage pour garantir qu'USBNIC est l'itinéraire choisi quand l'hôte veut accéder à l'adresse IPv4 USBNIC de l'iDRAC.

Chaque fois que j'essaie d'installer l'iSM, le message d'erreur suivant s'affiche : Ce système d'exploitation n'est pas pris en charge.

L'iSM ne peut être installé que sur les systèmes d'exploitation pris en charge. Pour connaître les systèmes d'exploitation pris en charge, voir Systèmes d'exploitation pris en charge.

J’ai utilisé la fonctionnalité de réinitialisation matérielle de l’iDRAC à distance pour réinitialiser l’iDRAC. Toutefois, IPMI ne répond pas et je n'arrive pas à résoudre les problèmes.

Si vous essayez d’utiliser la fonctionnalité de réinitialisation matérielle de l’iSM à distance sur le **système d’exploitation VMware ESXi**, les pilotes IPMI ne répondent plus, ce qui a pour effet d’interrompre la communication à l’iSM. Vous devrez peut-être redémarrer le serveur et charger de nouveau le pilote IPMI pour résoudre le problème.

Où puis-je me procurer le journal Lifecycle répliqué sur mon système d’exploitation ?

Pour afficher les fichiers du journal Lifecycle Controller répliqués :

Tableau 20. Système d’exploitation et emplacement

Système d'exploitation	Emplacement
Microsoft Windows	**Observateur d'événements** > **Journaux Windows** > ***<groupe existant ou dossier personnalisé>***. Tous les fichiers du journal Lifecycle Cycle de l’iSM sont répliqués sous le nom de source **iDRAC Service Module**.
Red Hat Enterprise Linux et SUSE Linux	**/var/log/messages**
VMware ESXi	**/var/log/syslog.log**
Ubuntu	**/var/log/syslog**

Quel est le protocole SNMP par défaut configuré dans l’iSM pour envoyer des alertes dans les systèmes d’exploitation Linux ?

Par défaut, le protocole de multiplexage SNMP (SMUX) est configuré dans l’iSM pour envoyer des alertes.

La technologie SMUX n'est pas prise en charge sur mon système. Quel protocole dois-je configurer pour envoyer des alertes ?

Si le SMUX n'est pas pris en charge sur votre système, l'Agent-x est utilisé comme protocole par défaut.

Comment puis-je configurer l'iSM pour utiliser le protocole Agent-x pour envoyer des alertes par défaut ?

Vous pouvez configurer l'Agent-x comme protocole par défaut à l'aide de la commande `./Enable-iDRACSNMPTrap.sh 1/agentx -force`. Si –force n'est pas spécifié, assurez-vous que le net-SNMP est configuré et redémarrez le service snmpd.

Quels sont les fichiers exécutables ou packages dépendants Linux à installer pour l'installation sous Linux ?

Pour afficher la liste des packages dépendants de Linux, voir Dépendances Linux.

J'ai créé un dossier personnalisé dans l'Observateur d'événements Windows, mais les fichiers du journal Lifecycle ne sont pas répliqués dans mon dossier personnalisé. Que dois-je faire à présent pour répliquer les fichiers du journal Lifecycle ?

Assurez-vous de fermer l'**Observateur d'événements** Windows après avoir créé le dossier personnalisé. Ouvrez le l'**Observateur d'événements** pour afficher les fichiers du journal Lifecycle répliqués.

J'ai choisi l'option d'installation personnalisée dans l'interface graphique au cours de l'installation de l'iSM et j'ai désactivé une fonctionnalité, mais je n'arrive pas à activer celle-ci à l'aide de l'une des autres interfaces. Comment puis-je réactiver la fonctionnalité ?

Sur les systèmes exécutant Microsoft Windows, une fonctionnalité activée à l'aide du programme d'installation et désactivée à l'aide d'une interface autre que le programme d'installation, ne peut être activée qu'à l'aide de la même interface ou du programme d'installation en mode d'interface graphique.

Par exemple, il se peut que vous ne puissiez pas activer une fonctionnalité qui a été désactivée à partir de l'interface graphique lors de l'installation d'iSM à l'aide des commandes CLI RACADM.

Je n'arrive pas à accéder à la page de l'iDRAC par l'intermédiaire du système d'exploitation hôte en tant qu'utilisateur Active Directory sur LDAP. J'essaie

d'accéder à la page de l'iDRAC par l'intermédiaire du système d'exploitation hôte, mais une erreur indiquant que le site est inaccessible s'affiche. Comment puis-je résoudre ce problème ?

Lorsque vous essayez d'accéder à la page de l'iDRAC par l'intermédiaire du système d'exploitation hôte, il se peut qu'une erreur indiquant que le site est inaccessible s'affiche. Assurez-vous que le réseau iDRAC est configuré pour l'authentification en tant qu'utilisateur LDAP. Vous pouvez également vous connecter en tant qu'utilisateur local ou invité.

Je n'arrive pas à accéder à la page de l'iDRAC par l'intermédiaire du système d'exploitation hôte après avoir exécuté une opération de rétablissement des paramètres d'usine de l'iDRAC, telle que `racadm racresetcfg`. Comment puis-je résoudre ce problème ?

Assurez-vous que le canal de connexion directe entre le système d'exploitation et l'iDRAC est activé. Par défaut, elle est désactivée en mode usine. Pour activer le canal de communication directe entre le système d'exploitation et l'iDRAC, utilisez la commande `racadm set idrac.os-bmc.adminstate 1`.

L'adresse 169.254.0.2 s'affiche comme l'adresse IP source dans le trap SNMP de l'iDRAC reçue par le biais de l'iSM. Comment puis-je résoudre ce problème ?

Sous le système d'exploitation Linux, les traps SNMP de l'iDRAC reçus par le biais du système d'exploitation hôte affichent le nom d'hôte ou l'adresse IP source en tant que 169.254.0.2 au lieu de l'adresse IP ou du nom du système d'exploitation hôte réel. C'est le système d'exploitation qui spécifie que l'entrée doit être renseignée avant que l'interruption ne soit transmise à l'utilisateur.

J'ai configuré la connexion directe entre mon système d'exploitation et l'iDRAC jusqu'à LOM, et lorsque j'essaie d'exécuter dcism-sync, l'opération de mise à jour échoue. Comment puis-je procéder ?

La connexion directe entre le système d'exploitation et l'iDRAC doit être configuré pour utiliser le mode USB-NIC. Il s'agit d'une condition préalable à l'installation et à la mise à jour de l'iSM.

Je peux activer ou désactiver la fonctionnalité WMIInfo de l'iSM sur les systèmes d'exploitation Linux et

VMware ESXi en utilisant les commandes RACADM et WS-Man. Quel est l'impact sur ma configuration iSM sur le système d'exploitation hôte ?

La fonctionnalité WMIInfo de l'iSM n'est applicable qu'aux systèmes d'exploitation Microsoft Windows. Toutefois, l'activation ou la désactivation de cette fonctionnalité depuis l'une des interfaces iDRAC sur un système d'exploitation autre que Microsoft Windows n'a pas d'impact sur la configuration iSM sur le système d'exploitation hôte.

Si je supprime l'adresse IP de l'interface USBNIC sur le système d'exploitation hôte, l'iSM ne peut plus communiquer avec l'iDRAC.

L'iSM ne configure l'interface USBNIC du système d'exploitation hôte qu'une seule fois. Si vous arrêtez ensuite l'interface USBNIC sur le système d'exploitation hôte en supprimant l'adresse IP, en déconnectant la liaison de l'interface ou en désactivant l'adresse IPV4 ou IPV6 sur cette interface, l'iSM conserve la configuration utilisateur et ne remplace pas les paramètres de l'interface. Pour restaurer la communication entre l'iSM et l'iDRAC, redémarrez le service iSM sur le système d'exploitation hôte.

Après avoir installé l'iSM à l'aide du fichier de commandes ISM_Win.BAT depuis la partition logique « SMINST » exposée de l'iDRAC sur le système d'exploitation Microsoft Windows, je rencontre un message d'erreur indiquant : « Le système ne trouve pas le fichier spécifié ».

Une fois l'iSM installé, la partition logique **SMINST** est démontée du système d'exploitation hôte. Ce message s'affiche si le script BAT est appelé depuis la partition **SMINST** elle-même. L'installation aboutit. Aucune action n'est nécessaire de la part de l'utilisateur.

Si les packages dépendants de l'iSM ne sont pas présents sur le système d'exploitation Ubuntu, l'installation par l'intermédiaire du package de mise à jour Dell (DUP) du système d'exploitation installe l'iSM à l'état installation+décompression.

Vous pouvez le vérifier à l'aide de la commande ci-dessous :

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

Pour résoudre ce problème, exécutez la commande `apt-get install -f`. Les packages dépendants sont alors installés.

Lorsque j'installe l'iSM 3.4.0 ou version ultérieure sur les systèmes d'exploitation Linux tels que Red Hat Enterprise Linux, je vois des messages dans les journaux du système d'exploitation tels que 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.

Ces messages sont liés au gestionnaire de bureau GNOME. Divers groupes de systèmes d'exploitation disposent d'éléments Bugzilla pour faire face à ce scénario. Par exemple : https://bugzilla.redhat.com/show_bug.cgi?id=1594177. Aucune action n'est nécessaire de la part de l'utilisateur.

Je vois un terminal vide sur le système d'exploitation Red Hat Enterprise Linux lorsque je clique sur le raccourci du Lanceur de l'interface utilisateur d'iDRAC sous Menu > Accessoires.

La visibilité du texte sur le terminal dépend de la version GNOME exécutée sur le système d'exploitation résident. Vous pouvez également exécuter le lanceur depuis un shell compatible avec les interfaces utilisateurs. Par exemple : `bash#> sh /opt/dell/srvadmin/iSM/bin/iDRACLauncher.sh` en tant qu'utilisateur sudo.

Si la connexion directe entre le système d'exploitation et l'iDRAC est désactivée dans l'iDRAC, vous voyez un terminal vierge lorsque l'interface utilisateur de l'iDRAC est lancée depuis le système d'exploitation Linux, par exemple Red Hat Enterprise Linux 7.x et 8.x. Sélectionnez **o** ou **O**, et appuyez sur **Entrée** pour indiquer la configuration de l'interface USBNIC sur le système d'exploitation hôte.

Vous pouvez également activer la connexion directe entre le système d'exploitation et l'iDRAC dans l'iDRAC en mode USBNIC et exécuter à nouveau le programme de lancement de l'iDRAC depuis le système d'exploitation hôte.

Lorsque j'essaie de lancer la fonctionnalité d'authentification unique dans un environnement purement IPv6, la session de l'interface utilisateur de l'iDRAC ne se lance pas et un écran vide s'affiche.

Par défaut, l'appareil USB_NIC dispose des adresses IPv4 (liaison locale) et IPv6 (liaison locale), ainsi qu'une adresse ULA. Assurez-vous que les trois adresses IP sont présentes dans l'appareil USB_NIC. Si l'adresse ULA n'est pas présente, vérifiez que le paramètre de protocole IPv6 de l'appareil est défini sur Désactivé ou sur État de la liaison locale. La fonctionnalité d'authentification unique (SSO) doit être en mode automatique pour fonctionner.

L’alerte SNMP OMSA de l’hôte iSM est activée même si l’alerte SNMP de l’hôte iSM parent est désactivée.

Pour désactiver la fonctionnalité d’alerte SNMP OMSA de l’hôte iSM, vous devez d’abord activer l’alerte SNMP de l’hôte iSM parent, puis désactiver la fonctionnalité d’alerte SNMP OMSA de l’hôte iSM enfant.

La fonctionnalité d’alerte SNMP OMSA de l’hôte iSM peut être désactivée à l’aide de l’une des options suivantes :

- Interface RACADM
- Programme d’installation iSM pour le système d’exploitation, lorsqu’il est pris en charge.

Le mappage d’alerte SNMP entre l’iDRAC et OMSA est activé lorsque OMSA est en cours d’exécution.

Pour désactiver l’alerte SNMP OMSA de l’hôte iSM, redémarrez l’iDRAC Service Module.

8

Packages du programme d'installation Linux et Ubuntu

Les packages du programme d'installation pour systèmes d'exploitation Linux et Ubuntu pris en charge sont les suivants :

Tableau 21. Packages d'installation de Linux

Système d'exploitation Linux pris en charge	Package du programme d'installation
Red Hat Enterprise Linux 7	`SYSMGMT\iSM\linux\RHEL7\x86_64\dcism-4.1.0.0-<bldno>.el7.x86_64.rpm`
Red Hat Enterprise Linux 8	`SYSMGMT\iSM\linux\RHEL8\x86_64\dcism-4.1.0.0-<bldno>.el8.x86_64.rpm`
Ubuntu 20	`SYSMGMT\iSM\linux\Ubuntu20\x86_64\dcism-4.1.0.0-<bldno>.ubuntu20.deb`
SUSE Linux Enterprise Server 15	`SYSMGMT\iSM\linux\SLES15\x86_64\dcism-4.1.0.0-<bldno>.sles15.x86_64.rpm`

REMARQUE : Vous pouvez utiliser l'un des packages du programme d'installation Red Hat Enterprise Linux répertoriés pour installer l'iSM sur CentOS.

9

Ressources et support

Pour plus d'informations sur les fonctionnalités de cette version, reportez-vous à la documentation de l'iDRAC Service Module 4.1.0.0.

Derniers documents publiés

Pour accéder à la version la plus récente des documents d'iDRAC Service Module :

- Rendez-vous sur www.dell.com/ismmanuals.com.
- Cliquez sur la version d'iDRAC Service Module souhaitée.
- Cliquez sur **Manuels et documents**.

Accès aux documents à l'aide de liens directs

Tableau 22. Liens directs vers les documents

URL	Produit
https://www.dell.com/idracmanuals	iDRAC et Lifecycle Controller
https://www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
https://www.dell.com/esmmanuals	Enterprise System Management
https://www.dell.com/serviceabilitytools	Outils de facilité de maintenance
https://www.dell.com/omconnectionsclient	Client System Management

Accès aux documents à l'aide de la recherche de produit

1. Rendez-vous sur https://www.dell.com/support.
2. Dans la zone de recherche **Entrez un numéro de série ...**, saisissez le nom du produit. Par exemple, PowerEdge ou iDRAC. Une liste des clusters NAS s'affiche.
3. Sélectionnez votre produit et cliquez sur l'icône de recherche ou appuyez sur Entrée.
4. Cliquez sur **Manuels et documents**.

Accès aux documents à l'aide de la sélection de produits

Vous pouvez également accéder aux documents en sélectionnant votre produit.

1. Rendez-vous sur https://www.dell.com/support.
2. Cliquez sur **Parcourir tous les produits**.
3. Cliquez sur la catégorie de produit souhaitée : Serveurs, Logiciel, Stockage, etc.
4. Cliquez sur le produit souhaité, puis sur la version souhaitée le cas échéant.

   REMARQUE : Pour certains produits, vous devrez peut-être parcourir les sous-catégories.
5. Cliquez sur **Manuels et documents**.

Sujets :

- Identification de la série de vos serveurs Dell EMC PowerEdge

Identification de la série de vos serveurs Dell EMC PowerEdge

Les séries PowerEdge de la solution de serveurs Dell EMC sont divisées en différentes catégories en fonction de leur configuration. Elles sont appelées séries de serveurs YX2X, YX3X, YX4X, YX4XX ou YX5XX. La structure de la convention de dénomination est décrite ci-après :

La lettre Y se rapporte aux caractères compris dans le numéro de modèle du serveur. Les caractères indiquent le format du serveur. Les formats sont répertoriés ci-dessous :

- C — Cloud
- F — Flexible
- M ou MX — Modulaire
- R — Rack
- T — Tour
- XR — Serveur industriel pour environnements extrêmes

La lettre X se rapporte aux chiffres du numéro de modèle du serveur. Les nombres indiquent plusieurs caractéristiques concernant le serveur. Ils sont répertoriés comme suit :

- Le premier chiffre (X) représente la chaîne ou la classe de valeurs du serveur.
  - 1 à 5 — iDRAC Basic
  - 6 à 9 — iDRAC Express
- Le deuxième chiffre indique la série du serveur. Il est conservé dans la convention de dénomination du serveur et ne remplace pas la lettre X.
  - 0 — Série 10
  - 1 — Série 11
  - 2 — Série 12
  - 3 — Série 13
  - 4 — Série 14
  - 5 — Série 15
- Le dernier chiffre (X) indique toujours la marque du processeur, comme indiqué ci-dessous :
  - 0 — Intel
  - 5 — AMD

REMARQUE : Pour les serveurs qui utilisent un processeur AMD, le numéro de modèle est composé de quatre chiffres au lieu de trois. Le troisième chiffre (X) indique le nombre de sockets des processeurs pris en charge par les séries de serveurs.

- 1 : serveur à 1 socket
- 2 : serveur à 2 sockets

Tableau 23. Convention de dénomination des serveurs PowerEdge et exemples

Système YX3X	Système YX4X	Système YX4XX	Système 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

Contacter Dell EMC

Dell EMC propose plusieurs options de services et support en ligne et par téléphone. La disponibilité des services varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre zone géographique. Pour contacter Dell EMC pour des questions commerciales, de support technique ou de service client, consultez le site www.dell.com/contact.

Si vous n'avez pas de connexion Internet active, vous pouvez trouver les informations de contact dans votre confirmation de commande, votre bordereau d'expédition, votre facture ou dans le catalogue produits.