# OpenManage Integration for VMware vCenter version 4.2

## Guide d'installation du client Web

Avril 2018
Rév. A00

## Remarques, précautions et avertissements

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

**PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.**

**AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.**

# Table des matières

# 1

# Introduction

Ce guide fournit des instructions étape par étape pour l'installation et la configuration d'OpenManage Integration for VMware vCenter (OMIVV) pour une utilisation avec les serveurs PowerEdge. Après l'installation d'OMIVV, pour obtenir plus d'informations sur tous les aspects de l'administration, notamment la gestion d'inventaire, la surveillance et les alertes, les mises à jour de micrologiciel et la gestion de garantie, voir l'*OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals`.

**Sujets :**



# Gestion des licences d'OpenManage Integration for VMware vCenter

Il existe deux types de licences OpenManage Integration for VMware vCenter :

- Licence d'évaluation : lorsque l'appliance OMIVV version 4.x est mise sous tension pour la première fois, une licence d'évaluation est automatiquement installée. La version d'essai contient une licence d'évaluation pour cinq hôtes (serveurs) gérés par OpenManage Integration for VMware vCenter. Celle-ci s'applique uniquement aux serveurs Dell EMC de 11e génération et de générations ultérieures. Il s'agit d'une licence par défaut uniquement valable pendant la période d'essai de 90 jours.
- Licence standard : la version complète du produit contient une licence standard pour un maximum de 10 serveurs vCenter, et vous pouvez acheter n'importe quel nombre de connexions hôtes gérées par OMIVV.

Lorsque vous effectuez la mise à niveau de la licence d'évaluation vers une licence standard complète, vous recevez un e-mail de confirmation de votre commande, et vous pouvez télécharger le fichier de licence à partir de Dell Digital Locker. Enregistrez le fichier .XML de licence sur votre système local et téléchargez le nouveau fichier de licence à l'aide de la **Console Administration**.

Les licences offrent les informations suivantes :

- Licences de connexions vCenter maximales : jusqu'à 10 connexions vCenter enregistrées et utilisées sont autorisées.
- Licences de connexions hôte maximales : nombre de connexions hôte achetées.
- En cours d'utilisation : le nombre de connexions vCenter ou connexions hôte utilisées. Pour les connexions hôte, ce nombre représente le nombre d'hôtes (ou serveurs) découverts et inventoriés.
- Disponibles : nombre de licences de connexions vCenter ou de connexions hôte disponibles pour un usage ultérieur.

**REMARQUE :** La période de licence standard est de trois ou cinq ans seulement. Les licences supplémentaires sont ajoutées à la licence existante et ne sont pas écrasées.

Lorsque vous achetez une licence, le fichier .XML (clé de licence) est téléchargeable sur la boutique en ligne Dell accessible à l'adresse http://www.dell.com/support/licensing. Si vous ne parvenez pas à télécharger vos clés de licence, contactez le service de support Dell en allant sur www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support pour trouver le numéro de téléphone du service du support Dell de votre zone géographique pour votre produit.

## Exigences de la licence pour les hôtes et les serveurs vCenter

Les éléments suivants sont les exigences en matière de licence pour les hôtes et vCenter :

- Vous pouvez acheter une licence pour prendre en charge la quantité de serveurs Dell EMC qui sera gérée par OMIVV. Une licence est utilisée uniquement après l'ajout d'un hôte à un profil de connexion. La licence n'est pas associée à un serveur spécifique.

- Une instance d'OMIVV prend en charge jusqu'à 10 instances de serveurs vCenter. Il n'y a aucune licence distincte pour le nombre de serveurs vCenter.

# Achat et chargement d'une licence logicielle

Vous exécutez une licence d'évaluation jusqu'à la mise à niveau vers une version complète du produit. Utilisez le lien **Acheter une licence** du produit pour accéder au site Web Dell et acheter une licence. Une fois l'achat effectué, vous pouvez charger cette licence à l'aide de la **Console d'administration**.

**REMARQUE :** L'option **Acheter une licence** s'affiche uniquement si vous utilisez une licence d'évaluation.

1. Dans OpenManage Integration for VMware vCenter, effectuez l'une des tâches suivantes :
   - Dans l'onglet **Licences**, en regard de **Licence logicielle**, cliquez **Acheter une licence**.
   - Dans l'onglet **Mise en route**, sous **Tâches de base**, cliquez sur **Acheter une licence**.
2. Enregistrez le fichier de licence dans un emplacement connu que vous avez téléchargé à partir de Dell Digital Locker.
3. Dans un navigateur Web, entrez l'URL de la Console Administration.
   Utilisez le format suivant : `https://<ApplianceIPAddress>`
4. Dans la fenêtre de connexion de la **Console Administration**, saisissez le mot de passe et cliquez sur **Se connecter**.
5. Cliquez sur **Charger la licence**.
6. Dans la fenêtre **Charger la licence**, cliquez sur **Parcourir** pour accéder au fichier de licence.
7. Sélectionnez le fichier de licence et cliquez sur **Charger**.

**REMARQUE :** Le fichier de licence peut être compressé dans un fichier zip. Assurez-vous de décompresser le fichier zip et de charger uniquement le fichier .xml de licence. Le nom du fichier de la licence peut correspondre à votre numéro de commande (par exemple : 123456789.xml).

# Options suite au chargement de licences

## Fichier de licence pour de nouveaux achats

Lorsque vous passez une commande pour l'achat d'une nouvelle licence, Dell vous envoie un e-mail confirmant la commande et vous pouvez télécharger le nouveau fichier de licence à partir de Dell Digital Locker, à l'adresse http://www.dell.com/support/licensing. La licence est au format .xml. Si la licence est au format .zip, extrayez le fichier .xml de licence à partir du fichier .zip avant le chargement.

## Empilage des licences

À partir de la version 2.1, OMIVV peut empiler plusieurs licences standard pour augmenter le nombre d'hôtes pris en charge aux hôtes indiqués dans les licences chargées. Une licence d'évaluation ne peut pas être empilée. Le nombre de serveurs vCenter pris en charge ne peut pas être augmenté par empilage et nécessite l'utilisation de plusieurs appliances.

La fonctionnalité d'empilage des licences présente des restrictions. Si une nouvelle licence standard est chargée avant l'expiration de la licence standard existante, les licences sont empilées. Dans le cas contraire, si la licence a expiré et une nouvelle licence est chargée, seul le nombre d'hôtes indiqué par la nouvelle licence sera pris en charge. Si plusieurs licences sont déjà chargées, le nombre d'hôtes pris en charge correspond au nombre total d'hôtes indiqué dans les licences non expirées au moment où la dernière licence a été téléchargée.

## Licences expirées

Les licences qui ont dépassé la durée de leur support, généralement trois ou cinq ans à compter de la date d'achat, sont bloquées du chargement. Si des licences ont expiré après avoir été chargées, la fonctionnalité des hôtes existants continue, mais les mises à niveau vers les nouvelles versions de l'OMIVV seront bloquées.

### Remplacement de licences

Si un problème survient avec votre commande et vous recevez une licence de remplacement de la part de Dell, celle-ci contiendra les mêmes ID de droit que la licence précédente. Lorsque vous chargez une licence de remplacement, la licence est remplacée si une licence a déjà été chargée avec les mêmes ID de droit.

## Mise en application

### Mises à jour de l'appliance

L'appliance ne permet pas les mises à jour vers des versions plus récentes lorsque toutes les licences ont expiré. Veuillez obtenir et télécharger une nouvelle licence avant toute tentative de mise à niveau de l'appliance.

### Licence d'évaluation

Lorsqu'une licence d'évaluation expire, plusieurs zones clés cessent de fonctionner et affichent un message d'erreur.

### Ajout d'hôtes à des profils de connexion

Lorsque vous tentez d'ajouter un hôte à un profil de connexion, si le nombre d'hôtes sous licence de 11ème génération ou plus récente dépasse le nombre de licences, l'ajout d'hôtes supplémentaires n'est pas autorisé.

# Remarques importantes à titre de référence

- À partir d'OMIVV 4.0 et versions ultérieures, seul le client Web VMware vSphere est pris en charge et le bureau client vSphere n'est pas pris en charge.
- Pour vCenter 6.5 et versions ultérieures, l'appliance OMIVV est disponible uniquement pour la version Flash. L'appliance OMIVV n'est pas disponible pour la version HTML5.
- Pour l'utilisation du serveur DNS, les pratiques recommandées sont les suivantes :
  - OMIVV prend en charge uniquement les adresses IP IPv4. Bien que les affectations IP statique et DHCP soient toutes les deux prises en charge, nous vous recommandons d'attribuer une adresse IP statique. Attribuez une adresse IP statique et un nom d'hôte lorsque vous déployez une appliance OMIVV avec un enregistrement DNS valide. L'adresse IP statique garantit que pendant le redémarrage du système, l'adresse IP de l'appliance OMIVV reste identique.
  - Assurez-vous que les entrées de nom d'hôte OMIVV sont présentes dans les zones de recherches directes et inversées sur votre serveur DNS.

  Pour plus d'informations sur les exigences DNS pour vSphere, voir les liens VMware suivants :

  - Exigences DNS pour vSphere 5.5
  - Exigences DNS pour vSphere 6.0
  - Exigences DNS pour vSphere 6.5 et appliance du contrôleur de services de plateforme
- Pour le mode de l'appliance OMIVV, assurez-vous que vous déployez OMIVV sous le mode approprié en fonction de votre environnement de virtualisation. Pour de plus amples informations, consultez Configuration requise pour les modes de déploiement , page 7.
- Configuration de votre réseau pour répondre aux exigences en matière de port. Pour de plus amples informations, consultez Informations sur les ports , page 12.

# La configuration matérielle requise

OMIVV prend entièrement en charge plusieurs générations de serveurs Dell EMC ainsi que l'ensemble des fonctionnalités des serveurs disposant d'iDRAC Express ou Enterprise. Vous trouverez des informations supplémentaires sur les exigences de plateforme dans les *OpenManage Integration for VMware vCenter Release Notes* (Notes de mise à jour d'OpenManage Integration for VMware vCenter) disponibles à l'adresse `Dell.com/support/manuals`. Pour vérifier que vos serveurs hôtes sont admissibles, consultez les informations sur les éléments suivants dans les sous-sections ci-dessous :

- Serveur et BIOS minimal pris en charge
- Versions prises en charge d'iDRAC (tant pour le déploiement que la gestion)
- Prise en charge OMSA des serveurs de 11ème génération et génération plus ancienne et prise en charge de la version ESXi (tant pour le déploiement que la gestion)
- Mémoire et espace pris en charge pour OMIVV

OMIVV nécessite le réseau LAN sur une carte mère/carte fille réseau pouvant accéder au réseau de gestion des systèmes iDRAC/CMC et au réseau de gestion de vCenter.

# Configuration requise pour les modes de déploiement

Assurez-vous que la configuration requise suivante est respectée pour les modes de déploiement souhaités :

### Tableau 1. Configuration requise pour les modes de déploiement

| Modes de déploiement | Nombre d'hôtes | Nombre de processeurs | Mémoire (en Go) | Stockage minimal |
|---|---|---|---|---|
| Petit | Jusqu'à 250 | 2 | 8 | 44 Go |
| Moyen | Jusqu'à 500 | 4 | 16 | 44 Go |
| Important | Jusqu'à 1000 | 8 | 32 | 44 Go |

**REMARQUE :** Pour l'un des modes de déploiement mentionnés, assurez-vous de réserver des ressources de mémoire suffisantes sur l'appliance virtuelle OMIVV à l'aide de réservations. Voir la documentation de vSphere pour obtenir les étapes concernant la réservation des ressources de mémoire.

# Versions du BIOS, de l'iDRAC et du Lifecycle Controller

Les versions du BIOS, de l'iDRAC et du Lifecycle Controller requises pour activer les fonctionnalités de l'appliance OpenManage Integration for VMware vCenter sont répertoriées dans cette section.

Nous vous recommandons d'utiliser l'image ISO amorçable créée à l'aide de Repository Manager ou de la plateforme Lifecycle Controller pour mettre à jour les serveurs vers l'une des versions de base suivantes avant d'utiliser OMIVV :

### Tableau 2. BIOS pour les serveurs PowerEdge de 11e génération

| Serveur | Version minimale |
|---|---|
| PowerEdge R210 | 1.8.2 ou version ultérieure |
| PowerEdge R210II | 1.3.1 ou version ultérieure |
| PowerEdge R310 | 1.8.2 ou version ultérieure |
| PowerEdge R410 | 1.9.0 ou version ultérieure |
| PowerEdge R415 | 1.8.6 ou version ultérieure |
| PowerEdge R510 | 1.9.0 ou version ultérieure |
| PowerEdge R515 | 1.8.6 ou version ultérieure |
| PowerEdge R610 | 6.1.0 ou version ultérieure |
| PowerEdge R710 | 6.1.0 ou version ultérieure |
| PowerEdge R710 | 6.1.0 ou version ultérieure |
| PowerEdge R715 | 3.0.0 ou version ultérieure |
| PowerEdge R810 | 2.5.0 ou version ultérieure |
| PowerEdge R815 | 3.0.0 ou version ultérieure |

### Tableau 2. BIOS pour les serveurs PowerEdge de 11e génération (suite)

| Serveur | Version minimale |
|---|---|
| PowerEdge R910 | 2.5.0 ou version ultérieure |
| PowerEdge M610 | 6.1.0 ou version ultérieure |
| PowerEdge M610x | 6.1.0 ou version ultérieure |
| PowerEdge M710HD | 5.0.1 ou version ultérieure |
| PowerEdge M910 | 2.5.0 ou version ultérieure |
| PowerEdge M915 | 2.6.0 ou version ultérieure |
| PowerEdge T110 II | 1.8.2 ou version ultérieure |
| PowerEdge T310 | 1.8.2 ou version ultérieure |
| PowerEdge T410 | 1.9.0 ou version ultérieure |
| PowerEdge T610 | 6.1.0 ou version ultérieure |
| PowerEdge T710 | 6.1.0 ou version ultérieure |

### Tableau 3. BIOS pour les serveurs PowerEdge de 12e génération

| Serveur | Version minimale |
|---|---|
| T320 | 1.0.1 ou version ultérieure |
| T420 | 1.0.1 ou version ultérieure |
| T620 | 1.2.6 ou version ultérieure |
| M420 | 1.2.4 ou version ultérieure |
| M520 | 1.2.6 ou version ultérieure |
| M620 | 1.2.6 ou version ultérieure |
| M820 | 1.2.6 ou version ultérieure |
| R220 | 1.0.3 ou version ultérieure |
| R320 | 1.2.4 ou version ultérieure |
| R420 | 1.2.4 ou version ultérieure |
| R520 | 1.2.4 ou version ultérieure |
| R620 | 1.2.6 ou version ultérieure |
| R720 | 1.2.6 ou version ultérieure |
| R720xd | 1.2.6 ou version ultérieure |
| R820 | 1.7.2 ou version ultérieure |
| R920 | 1.1.0 ou version ultérieure |

### Tableau 4. BIOS pour les serveurs PowerEdge de 13e génération

| Serveur | Version minimale |
|---|---|
| R630 | 1.0.4 ou version ultérieure |
| R730 | 1.0.4 ou version ultérieure |
| R730xd | 1.0.4 ou version ultérieure |
| R430 | 1.0.4 ou version ultérieure |
| R530 | 1.0.2 ou version ultérieure |
| R830 | 1.0.2 ou version ultérieure |

### Tableau 4. BIOS pour les serveurs PowerEdge de 13e génération (suite)

| Serveur | Version minimale |
|---|---|
| R930 | 1.0.2 ou version ultérieure |
| R230 | 1.0.2 ou version ultérieure |
| R330 | 1.0.2 ou version ultérieure |
| T630 | 1.0.2 ou version ultérieure |
| T130 | 1.0.2 ou version ultérieure |
| T330 | 1.0.2 ou version ultérieure |
| T430 | 1.0.2 ou version ultérieure |
| M630 | 1.0.0 ou version ultérieure |
| M830 | 1.0.0 ou version ultérieure |
| FC430 | 1.0.0 ou version ultérieure |
| FC630 | 1.0.0 ou version ultérieure |
| FC830 | 1.0.0 ou version ultérieure |

### Tableau 5. BIOS pour les serveurs PowerEdge de 14e génération

| Serveur | Version minimale |
|---|---|
| R940 | 1.0.0 ou version ultérieure |
| R740 | 1.0.0 ou version ultérieure |
| R740xd | 1.0.0 ou version ultérieure |
| R640 | 1.0.0 ou version ultérieure |
| M640 | 1.0.0 ou version ultérieure |
| T640 | 1.0.0 ou version ultérieure |
| T440 | 1.0.0 ou version ultérieure |
| R540 | 1.0.0 ou version ultérieure |
| FC640 | 1.0.0 ou version ultérieure |
| R6415 | 1.0.0 ou version ultérieure |
| R7425 | 1.0.0 ou version ultérieure |
| R7415 | 1.0.0 ou version ultérieure |

### Tableau 6. iDRAC et Lifecycle Controller pour le déploiement

| Génération | Version | |
|---|---|---|
| | iDRAC | Lifecycle Controller |
| Serveurs PowerEdge de 11e génération | 3.35 pour type modulaire, 1.85 pour rack ou tour | 1.5.2 ou version ultérieure |
| Serveurs PowerEdge de 12e génération | 1.00.0 ou version ultérieure | 1.0.0.3017 ou version ultérieure |
| Serveurs PowerEdge de 13e génération | 2.30.30.30 ou version ultérieure | 2.30.30.30 ou version ultérieure |
| Serveurs PowerEdge de 14e génération | 3.00.00.00 et versions ultérieures | 3.00.00.00 et versions ultérieures |

### Tableau 7. Exigences du BIOS et de l'iDRAC pour le serveur cloud

| Modèle | BIOS | iDRAC avec Lifecycle Controller |
|---|---|---|
| C6320 | 1.0.2 | 2.30.30.30 ou version ultérieure |

### Tableau 7. Exigences du BIOS et de l'iDRAC pour le serveur cloud (suite)

| Modèle | BIOS | iDRAC avec Lifecycle Controller |
|---|---|---|
| C4130 | 1.0.2 | 2.30.30.30 ou version ultérieure |
| C6420 | 1.0.0 ou version ultérieure | 3.00.00.00 ou version ultérieure |
| C4140 | 1.0.0 ou version ultérieure | 3.00.00.00 ou version ultérieure |

# Fonctionnalités prises en charge sur les serveurs PowerEdge

Les fonctionnalités suivantes sont prises en charge sur les hôtes gérés par OpenManage Integration for VMware vCenter.

### Tableau 8. Fonctionnalités prises en charge sur les serveurs PowerEdge

| Ressource | Plate-forme | | |
|---|---|---|---|
| | 11e | 12e et 13e | 14e |
| Inventaire du matériel | O | O | O |
| Événements et alarmes | O (SNMP v1 uniquement) | O (SNMP v1 et v2) | O (SNMP v1 et v2) |
| Surveillance de l'intégrité au niveau des composants* | O | O | O |
| Mises à jour du BIOS/Micrologiciel# | O | O | O |
| Proactive HA$ | N | O | O |
| Informations sur la garantie | O | O | O |
| Conformité de l'hôte | O | O | O |
| Détection manuelle/automatique de serveur sans système d'exploitation | O | O | O |
| Conformité Bare-Metal | O | O | O |
| Configuration matérielle | O | O | O |
| Déploiement d'hyperviseur sans système d'exploitation | O | O | O |
| Faire clignoter le voyant LED du serveur | O | O | O |
| Afficher/Effacer les journaux d'événements système (SEL) | O | O | O |
| Lien et lancement d'iDRAC | O | O | O |
| Réinitialisation d'iDRAC | O | O | O |
| Mode de verrouillage du système | N | N | O |
| Profil système | N | N | O |
| Profil de cluster | N | O ^ | O |

* Dans le Cloud, dans le cas du modèle numéro C6320, la surveillance de l'intégrité n'est pas prise en charge pour les cartes mezzanine.

# Dans le Cloud, dans le cas du modèle numéro C6320, les mises à jour du micrologiciel ne sont pas prises en charge pour les cartes mezzanine.

$ La fonctionnalité Proactive HA ne s'applique que sur vCenter 6.5 ou une version ultérieure doté de ESXi 6.0 ou d'une version ultérieure. En outre, la fonctionnalité Proactive HA n'est pas prise en charge sur des serveurs disposant d'un bloc d'alimentation intégré et de modèles de serveur de Cloud.

^ Dans le profil de cluster, le déplacement de configuration n'est pas pris en charge.

# Fonctionnalités prises en charge sur le châssis PowerEdge

Cette rubrique fournit des informations sur les fonctionnalités prises en charge sur le châssis PowerEdge.

**Tableau 9. Fonctionnalités prises en charge sur une infrastructure modulaire**

| Fonctionnalités | M1000e | VRTX | FX2s |
|---|---|---|---|
| Alertes SNMP | O | O | O |
| Inventaire du matériel | O | O | O |
| Lien et lancement du CMC | O | O | O |
| Informations sur la licence | N/A | O | O |
| Informations sur la garantie | O | O | O |
| Rapport d'intégrité | O | O | O |

# Espace requis pour le stockage provisionné

L'appliance virtuelle OMIVV exige au minimum 44 Go d'espace disque pour le stockage provisionné.

## Configuration de l'appliance virtuelle par défaut

L'appliance virtuelle OMIVV est provisionnée avec 8 Go de RAM et 2 UC virtuelles.

# Configuration logicielle requise

Assurez-vous que l'environnement vSphere répond aux exigences de l'appliance virtuelle, d'accès de port et de port d'écoute.

**Conditions requises pour le client Web VMware vSphere**

- Prend en charge vCenter 5.5 et versions ultérieures
- Nécessite les services du client Web à partir de vCenter (le client de bureau vSphere n'est pas pris en charge)

Pour connaître les exigences de logiciel particulières, vous pouvez également consulter le document *OpenManage Integration for VMware vCenter Compatibility Matrix* (Matrice de compatibilité d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals`.

# Exigences d'OpenManage Integration for VMware vCenter

## Versions ESXi prises en charge sur les hôtes gérés

Le tableau suivant fournit des informations sur les versions ESXi prises en charge sur les hôtes gérés :

**Tableau 10. Versions ESXi prises en charge**

| prise en charge des versions ESXi | Génération du serveur | | | |
|---|---|---|---|---|
| | 11G | 12G | 13G | 14G |
| v5.0 | O | O | N | N |
| v5.0 U1 | O | O | N | N |
| v5.0 U2 | O | O | N | N |
| v5.0 U3 | O | O | N | N |
| v5.1 | O | O | N | N |

**Tableau 10. Versions ESXi prises en charge (suite)**

| prise en charge des versions ESXi | Génération du serveur | | | |
|---|---|---|---|---|
| | 11G | 12G | 13G | 14G |
| v5.1 U1 | O | O | N | N |
| v5.1 U2 | O | O | O | N |
| v5.1 U3 | O | O | Y (à l'exception de M830, FC830 et de FC430) | N |
| v5.5 | O | O | N | N |
| v5.5 U1 | O | O | N | N |
| v5.5 U2 | O | O | O | N |
| v5.5 U3 | O | O | O | N |
| v6.0 | O | O | O | N |
| v6.0 U1 | O | O | O | N |
| v6.0 U2 | O | O | O | N |
| v6.0 U3 | O | O | O | O |
| v6.5 | N | O | O | N |
| v6.5 U1 | N | O | O | O |
| v6.7 | N | O | O | O |

L'OpenManage Integration for VMware vCenter prend en charge chacune des versions du serveur vCenter ci-dessous :

**Tableau 11. Versions du serveur vCenter prises en charge**

| Version vCenter | Prise en charge du client Web |
|---|---|
| v6.0 U2 | O |
| v6.0 U3 | O |
| v6.5 | O |
| v6.5 U1 | O |
| v6.7 | O |

**REMARQUE :** Pour plus d'informations sur l'enregistrement d'un serveur vCenter, voir *OpenManage Integration for VMware vCenter Version 4.2 Web Client Install Guide* (Guide d'installation d'OpenManage Integration for VMware vCenter version 4.2 pour client Web) disponible à l'adresse `Dell.com/support/manuals`.

OpenManage Integration for VMware vCenter version 4.2 prend en charge VMware vRealize Operations Manager (vROPS) versions 1.1 et 1.2.

# Informations sur les ports

## Appliance virtuelle et nœuds gérés

Dans OMIVV, lorsque vous déployez l'agent OMSA à l'aide du lien *Résoudre les hôtes non conformes* disponibles dans l'Assistant **Résoudre les hôtes vSphere non conformes**, OMIVV effectue l'action suivante :

- Démarre le service client HTTP
- Active le port 8080
- Met à disposition le port pour ESXi 5.0 ou version ultérieure pour télécharger et installer OMSA VIB

Une fois l'installation d'OMSA VIB terminée, le service s'arrête automatiquement et le port se ferme.

### Tableau 12. Appliance virtuelle

| Numéro de port | Protocoles | Port Type (Type de port) | Niveau de cryptage maximum | Direction | Destination | Utilisation | Description |
|---|---|---|---|---|---|---|---|
| 53 | DNS | TCP | None (Aucun) | Sortant | Appliance OMIVV vers serveur DNS | Client DNS | Connectivité au serveur DNS ou résolution des noms d'hôte. |
| 69 | TFTP | UDP | None (Aucun) | Sortant | Appliance OMIVV vers serveur TFTP | Client TFTP | Utilisé pour la mise à jour du micrologiciel sur les serveurs de 11e génération avec un ancien micrologiciel. |
| 80 | HTTP | TCP | None (Aucun) | Sortant | Appliance OMIVV vers Internet | Accès Dell Online Data | Connectivité à la garantie en ligne (Internet), au micrologiciel et aux dernières informations RPM. |
| 80 | HTTP | TCP | None (Aucun) | Entrant | Serveur ESXi vers appliance OMIVV | Serveur HTTP | Utilisé dans le flux de déploiement du système d'exploitation afin que les scripts post-installation communiquent avec l'appliance OMIVV. |
| 162 | Agent SNMP | UDP | None (Aucun) | Entrant | iDRAC/ESXi vers appliance OMIVV | Agent SNMP (serveur) | Pour recevoir des traps SNMP à partir de nœuds gérés. |
| 443 | HTTPS | TCP | 128 bits | Entrant | Interface utilisateur OMIVV vers appliance OMIVV | Serveur HTTPS | Services Web offerts par OMIVV. Ces services Web sont consommés par le client Web vCenter et le portail d'administration Dell. |
| 443 | WS-MAN | TCP | 128 bits | Entrée/Sortie | Appliance OMIVV vers/depuis iDRAC/OMSA | Communication iDRAC/OMSA | Communications IDRAC, OMSA et CMC utilisées pour gérer et surveiller les nœuds gérés. |
| 445 | SMB | TCP | 128 bits | Sortant | Appliance OMIVV vers CIFS | Communication CIFS | Pour communiquer avec le partage Windows. |
| 4433 | HTTPS | TCP | 128 bits | Entrant | iDRAC vers appliance OMIVV | Découverte automatique | Serveur de provisionnement utilisé pour la découverte de nœuds gérés. |
| 2049 | NFS | UDP/TCP | None (Aucun) | Entrée/Sortie | Appliance OMIVV vers NFS | Partage public | Partage public NFS exposé par l'appliance OMIVV vers les nœuds gérés et utilisé dans la mise à jour du micrologiciel et les flux de déploiement du système d'exploitation. |
| 4001 à 4004 | NFS | UDP/TCP | None (Aucun) | Entrée/Sortie | Appliance OMIVV vers NFS | Partage public | Partage public NFS exposé par l'appliance OMIVV vers les nœuds gérés, et utilisé dans la mise à jour du micrologiciel et les flux de déploiement du système d'exploitation. |
| 11620 | Agent SNMP | UDP | None (Aucun) | Entrant | iDRAC vers appliance OMIVV | Agent SNMP (serveur) | Communications IDRAC, OMSA et CMC utilisées pour gérer et surveiller les nœuds gérés. |
| Défini par l'utilisateur | N'importe lequel | UDP/TCP | None (Aucun) | Sortant | Appliance OMIVV vers serveur proxy | Proxy | Pour communiquer avec le serveur proxy |

### Tableau 13. Nœuds gérés (ESXi)

| Numéro de port | Protocoles | Port Type (Type de port) | Niveau de cryptage maximum | Direction | Destination | Utilisation | Description |
|---|---|---|---|---|---|---|---|
| 162, 11620 | SNMP | UDP | None (Aucun) | Sortant | ESXi vers appliance OMIVV | Événements matériels | Traps SNMP asynchrones envoyés à partir d'ESXi. Ce port doit s'ouvrir à partir d'ESXi. |
| 443 | WS-MAN | TCP | 128 bits | Entrant | Appliance OMIVV vers ESXi (OMSA) | Communication iDRAC/OMSA | Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi. |
| 443 | HTTPS | TCP | 128 bits | Entrant | Appliance OMIVV vers ESXi | Serveur HTTPS | Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi. |
| 8080 | HTTP | TCP | 128 bits | Sortant | ESXi vers appliance OMIVV | Serveur HTTP ; télécharge OMSA VIB et répare les hôtes vSphere non conformes | Aide ESXi à télécharger l'OMSA/le pilote VIB. |

### Tableau 14. Nœuds gérés (iDRAC/CMC)

| Numéro de port | Protocoles | Port Type (Type de port) | Niveau de cryptage maximum | Direction | Destination | Utilisation | Description |
|---|---|---|---|---|---|---|---|
| 443 | WSMAN /HTTPS | TCP | 128 bits | Entrant | Appliance OMIVV vers iDRAC/CMC | Communication iDRAC | Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir de l'iDRAC et du CMC. |
| 4433 | HTTPS | TCP | 128 bits | Sortant | iDRAC vers appliance OMIVV | Découverte automatique | Pour la découverte automatique de l'iDRAC (nœuds gérés) dans la station de gestion. |
| 2049 | NFS | UDP | None (Aucun) | Entrée/ Sortie | iDRAC vers/ depuis OMIVV | Partage public | Pour que l'iDRAC accède au partage public NFS qui est exposé par l'appliance OMIVV. Utilisé pour le déploiement du système d'exploitation et la mise à jour du micrologiciel.<br>Pour accéder aux configurations de l'iDRAC à partir de l'OMIVV. Utilisé dans le flux de déploiement. |
| 4001 à 4004 | NFS | UDP | None (Aucun) | Entrée/ Sortie | iDRAC vers/ depuis OMIVV | Partage public | Pour que l'iDRAC accède au partage public NFS qui est exposé par l'appliance OMIVV. Utilisé pour le déploiement du système d'exploitation et la mise à jour du micrologiciel.<br>Pour accéder aux configurations de l'iDRAC à partir de l'OMIVV. Utilisé dans le flux de déploiement. |
| 69 | TFTP | UDP | 128 bits | Entrée/ Sortie | iDRAC vers/ depuis OMIVV | Protocole simplifié de transfert de fichiers | Utilisé afin de gérer l'iDRAC avec succès à partir de la station de gestion. |

# Liste de contrôle des prérequis

Liste de contrôle avant le démarrage de l'installation du produit :

- Vérifiez que vous avez un nom d'utilisateur et un mot de passe pour qu'OMIVV accède au serveur vCenter. L'utilisateur peut avoir un rôle d'administrateur disposant de toutes les autorisations nécessaires ou d'utilisateur non administrateur avec les privilèges nécessaires. Pour plus d'informations sur la liste des privilèges requis pour le fonctionnement d'OMIVV, voir Required privileges for non-administrator users (Privilèges requis pour les utilisateurs non-administrateurs).
- Vérifiez que vous avez le mot de passe racine pour les systèmes hôtes ESXi ou les références d'authentification Active Directory dotées des droits d'administration sur l'hôte.
- Vérifiez si vous avez le nom d'utilisateur et le mot de passe associés à iDRAC Express ou Enterprise possédant des droits d'administration sur l'iDRAC.
- Vérifiez si le serveur vCenter est en cours d'exécution.
- Déterminez l'emplacement du répertoire d'installation d'OMIVV.
- Vérifiez que l'environnement VMware vSphere répond aux exigences de l'appliance virtuelle, d'accès de port et de port d'écoute. Installez également Adobe Flash Player sur un système client si nécessaire. Pour plus d'informations sur la version de Flash Player prise en charge, voir le document *OpenManage Integration for VMware vCenter Compatibility Matrix* (Matrice de compatibilité d'OpenManage Integration for VMware vCenter).

**REMARQUE :** L'appliance virtuelle fonctionne comme une machine virtuelle ordinaire ; toute interruption ou tout arrêt a un effet sur la fonctionnalité générale de l'appliance virtuelle.

**REMARQUE :** L'OMIVV présente les outils VMware comme étant En cours d'exécution (obsolètes) lorsqu'il est déployé sur ESXi 5.5 et les versions ultérieures. Vous pouvez mettre à niveau les outils VMware, après un déploiement réussi de l'appliance OMIVV, à tout moment par la suite.

**REMARQUE :** il est recommandé de conserver OMIVV et le serveur vCenter sur le même réseau.

**REMARQUE :** Le réseau de l'appliance OMIVV doit avoir accès à iDRAC, l'hôte et vCenter.

# Installation, configuration et mise à niveau d'OMIVV

Assurez-vous que les exigences matérielles sont remplies et que vous exécutez le logiciel VMware vCenter requis.

Les étapes de haut niveau suivantes constituent la procédure d'installation et de configuration pour l'OMIVV :

1. Téléchargez le fichier *DellEMC_OpenManage_Integration_<version number>.<build number>.zip* à partir du site Web de support de Dell à l'adresse `Dell.com/support`.
2. Naviguez jusqu'à l'emplacement où vous avez téléchargé le fichier, puis extrayez son contenu.
3. À l'aide du client Web vSphere, déployez le fichier OVF (Open Virtualization Format) qui contient l'appliance OMIVV. Voir Déploiement de l'OVF OMIVV.
4. Chargez le fichier de licence. Pour plus d'informations sur la gestion des licences, voir Chargement de licence.
5. Enregistrez l'appliance OMIVV auprès du serveur vCenter à l'aide de la Console Administration. Voir Enregistrement d'OMIVV et importation du fichier de licence.
6. Pour configurer l'appliance, suivez l'**Assistant Configuration initiale**. Voir les Tâches de configuration via l'Assistant Configuration.

## Déploiement de l'OVF OMIVV à l'aide du client Web vSphere

Vous devez télécharger et extraire le fichier .zip du produit *Dell_OpenManage_Integration_<version number>.<build number>.zip* à partir du site Web Dell.

1. Localisez le disque virtuel OMIVV que vous avez téléchargé et extrait et exécutez **Dell_OpenManage_Integration.exe**.

   Le système d'exploitation du client pris en charge pour l'extraction et l'exécution de l'exe est Windows 7 SP1 et version ultérieure.

   Le système d'exploitation du serveur pris en charge pour l'extraction et l'exécution de l'exe est Windows 2008 R2 et version ultérieure.
2. Acceptez le **CLUF** et enregistrez le fichier OVF.
3. Copiez ou déplacez le fichier OVF vers un emplacement accessible à l'hôte VMware vSphere sur lequel vous téléchargez l'appliance.

4. Démarrez le **client Web VMware vSphere**.
5. Dans le **client Web VMware vSphere**, sélectionnez un hôte et, dans le menu principal, cliquez sur **Actions** > **Déployer le modèle OVF**.

   Vous pouvez également cliquer avec le bouton droit sur **Hôte** et sélectionner **Déployer le modèle OVF**.

   L'Assistant **Déploiement du modèle OVF** s'affiche.
6. Dans la fenêtre **Sélectionner une source**, effectuez les sous-tâches suivantes :
   a. Sélectionnez **URL** si vous souhaitez télécharger le progiciel OVF depuis Internet.
   b. Sélectionnez le **fichier local** et cliquez sur **Parcourir** si vous souhaitez sélectionner le progiciel OVF depuis votre système local.

   **REMARQUE :** Le processus d'installation peut prendre de 10 à 30 minutes si le package OVF réside sur un partage réseau. Pour une installation rapide, il est recommandé d'héberger l'OVF sur un lecteur local.
7. Cliquez sur **Suivant**.
   La fenêtre **Afficher les détails** s'affiche avec les informations suivantes :
   - **Produit** : le nom du modèle OVF s'affiche.
   - **Version** : la version du modèle OVF s'affiche.
   - **Fournisseur** : le nom du fournisseur s'affiche.
   - **Éditeur** : les détails sur l'éditeur s'affichent.
   - **Taille de téléchargement** : la taille réelle du modèle OVF en giga-octets s'affiche.
   - **Taille sur disque** : les informations sur les détails alloués statiquement et dynamiquement s'affichent.
   - **Description** : le commentaire s'affiche ici.
8. Cliquez sur **Suivant**.
   La fenêtre **Sélectionner un nom et un dossier** s'affiche.
9. Dans la fenêtre **Sélectionner un nom et un emplacement** , effectuez les sous-étapes suivantes :
   a. Dans **Nom**, entrez le nom du modèle. Le nom peut comprendre jusqu'à 80 caractères.
   b. Dans la liste **Sélectionner un dossier ou un centre de données**, sélectionnez un emplacement pour le déploiement du modèle.
10. Cliquez sur **Suivant**.
    La fenêtre **Sélectionner un espace de stockage** s'affiche.
11. Dans la fenêtre **Sélectionner un stockage**, effectuez les sous-étapes suivantes :
    a. Dans la liste déroulante **Sélectionnez un format de disque virtuel**, sélectionnez l'un des formats suivants :
       - `Thick Provision Lazy Zeroed (Allocation statique avec mise à zéro tardive)`
       - `Thick Provision Eager Zeroed (Allocation statique avec mise à zéro immédiate)`
       - `Thin provision (Allocation dynamique)`

       Il est recommandé de sélectionner Thick Provision Eager Zeroed (Allocation statique avec mise à zéro immédiate).
    b. Dans la liste déroulante **Stratégie de stockage de la machine virtuelle**, sélectionnez une stratégie.
12. Cliquez sur **Suivant**.
    La fenêtre **Configurer des réseaux** s'affiche et inclut des détails sur les réseaux source et de destination.
13. Dans la fenêtre **Configurer des réseaux**, cliquez sur **Suivant**.

    **REMARQUE :** Il est recommandé de conserver l'appliance OMIVV et le serveur vCenter sur le même réseau.
14. Dans la fenêtre **Prêt à terminer**, vérifiez les options sélectionnées pour la tâche de déploiement d'OVF, puis cliquez sur **Terminer**.
    La tâche de déploiement qui s'exécute affiche une fenêtre d'état d'achèvement dans laquelle vous pouvez faire le suivi de l'avancement.

# Chargement d'un certificat HTTPS

Assurez-vous que le certificat utilise le format PEM.

Utilisez les certificats HTTPS pour sécuriser les communications entre l'appliance virtuelle et les systèmes hôtes. Pour configurer ce type de communication sécurisée, une requête de signature de certificat doit être envoyée à une autorité de certification, puis le certificat obtenu est chargé en utilisant l'Administration Console. Il y a aussi un certificat par défaut qui est auto-signé et peut être utilisé pour sécuriser les communications ; ce certificat est unique à chaque installation.

**REMARQUE :** Vous pouvez utiliser Microsoft Internet Explorer, Firefox ou Chrome pour charger des certificats.

1. Dans la page **GESTION DE L'APPLIANCE**, cliquez sur **Charger le certificat** dans la zone **CERTIFICATS HTTPS**.
2. Cliquez sur **OK** dans la boîte de dialogue **CHARGER LE CERTIFICAT**.

3. Pour sélectionner le certificat à charger, cliquez sur **Parcourir**, puis sur **Charger**.
4. Si vous souhaitez annuler le téléchargement, cliquez sur **Annuler**.

   **REMARQUE :** Si vous souhaitez charger un certificat personnalisé pour l'appliance, assurez-vous de charger le nouveau certificat avant l'enregistrement dans vCenter. Si vous chargez le nouveau certificat personnalisé après l'enregistrement dans vCenter, des erreurs de communication s'affichent dans le client Web. Pour résoudre ce problème, annulez l'enregistrement et recommencez l'enregistrement de l'appliance dans vCenter.

## Restauration du certificat HTTPS par défaut

1. Dans la page **GESTION DE L'APPLIANCE**, cliquez sur **Restaurer le certificat par défaut** dans la zone **CERTIFICATS HTTPS**.
2. Dans la boîte de dialogue **RESTAURER LE CERTIFICAT PAR DÉFAUT**, cliquez sur **Appliquer**.

# Enregistrement d'un vCenter Server par un utilisateur non-administrateur

Vous pouvez enregistrer des serveurs vCenter pour l'appliance OMIVV avec des informations d'identification d'administrateur vCenter ou en tant qu'utilisateur non-administrateur doté des privilèges Dell.

Pour autoriser un utilisateur non-administrateur disposant des privilèges requis à enregistrer un vCenter Server, procédez comme suit :

1. Pour modifier les privilèges sélectionnés pour un rôle, ajoutez le rôle et sélectionnez les privilèges requis pour celui-ci, ou modifiez un rôle existant.

   Pour connaître les étapes à suivre afin de créer ou de modifier un rôle et sélectionner des privilèges dans le client Web vSphere, voir la documentation de VMware vSphere. Pour sélectionner tous les privilèges requis pour le rôle, voir la section Privilèges requis pour les utilisateurs non administrateurs.

   **REMARQUE :** L'administrateur vCenter doit ajouter ou modifier un rôle.

2. Après avoir créé et défini un rôle, attribuez-lui un utilisateur et sélectionnez les privilèges correspondants.

   Pour plus d'informations sur l'attribution d'autorisations dans le client Web vSphere, reportez-vous à la documentation de VMware vSphere.

   **REMARQUE :** L'administrateur vCenter doit affecter des autorisations dans vSphere Client.

   Un utilisateur non-administrateur du serveur vCenter disposant des privilèges requis peut désormais enregistrer ou désenregistrer des serveurs vCenter, modifier les données d'identification ou mettre à jour le certificat.
3. Enregistrez un serveur vCenter à l'aide d'un utilisateur non-administrateur disposant des privilèges requis. Voir Enregistrement d'un serveur vCenter par un utilisateur non-administrateur disposant des privilèges requis.
4. Attribuez les privilèges Dell au rôle créé ou modifié à l'étape 1. Voir Attribution de privilèges Dell au rôle dans le client Web vSphere.

Un utilisateur non administrateur disposant des privilèges requis peut désormais utiliser les fonctionnalités OMIVV avec des hôtes Dell EMC.

## Privilèges requis pour les utilisateurs non administrateurs

Pour enregistrer OMIVV auprès d'un serveur vCenter, un utilisateur non administrateur doit disposer des privilèges suivants :

**REMARQUE :** Lorsqu'un utilisateur non administrateur ne disposant pas des privilèges ci-dessous enregistre un serveur vCenter auprès d'OMIVV, un message d'erreur s'affiche.

- Alarmes
  - Créer l'alarme
  - Modifier l'alarme
  - Supprimer l'alarme
- Poste
  - Enregistrer le poste
  - Annuler l'enregistrement du poste
  - Mettre à jour le poste
- Global

- Annuler la tâche
- Événement journal
- Paramètres

**REMARQUE :** Attribuez les privilèges de mise à jour de l'intégrité suivants si vous utilisez VMware vCenter 6.5 ou si vous opérez une mise à niveau vers vCenter 6.5 ou version ultérieure :

- Fournisseur de mise à jour de l'intégrité
  - Enregistrer
  - Annuler l'enregistrement
  - Mettre à jour
- Hôte
  - CIM
    - Interaction CIM
  - Configuration
    - Paramètres avancés
    - Connexion
    - Maintenance
    - Configuration réseau
    - Demander un correctif
    - Profil de sécurité et pare-feu

    **REMARQUE :** Attribuez les privilèges suivants si vous utilisez VMware vCenter 6.5 ou si vous opérez une mise à niveau vers vCenter 6.5 ou version ultérieure :
    - Host.Config
      - Paramètres avancés
      - Connexion
      - Maintenance
      - Configuration réseau
      - Demander un correctif
      - Profil de sécurité et pare-feu
  - Inventaire
    - Ajouter un hôte au cluster
    - Ajouter un hôte autonome
    - Modifier le cluster

      **REMARQUE :** Assurez-vous que vous attribuez le privilège de modification du cluster si vous utilisez vCenter 6.5 ou si vous opérez une mise à niveau vers vCenter 6.5 ou version ultérieure.
- Profil d'hôte
  - Modifier
  - Afficher
- Droits
  - Modifier les droits
  - Modifier le rôle
- Sessions
  - Valider la session
- Tâche
  - Créer une tâche
  - Mettre à jour la tâche

**REMARQUE :** Si un utilisateur non-administrateur tente d'enregistrer un serveur vCenter, il est obligatoire d'ajouter des privilèges Dell au rôle existant. Pour en savoir plus sur l'affectation de privilèges Dell, voir Attribution de privilèges Dell à un rôle existant , page 19.

## Enregistrement d'un serveur vCenter par un utilisateur non administrateur disposant des privilèges requis

Vous pouvez enregistrer un serveur vCenter pour l'appliance OMIVV en tant qu'utilisateur non administrateur doté des privilèges appropriés. Reportez-vous aux étapes 5 à 9 de la rubrique **Enregistrement d'OpenManage Integration for VMware vCenter**

**et importation du fichier de licence**. pour en savoir plus sur l'enregistrement d'un serveur vCenter en tant qu'utilisateur non administrateur ou en tant qu'administrateur.

## Attribution de privilèges Dell à un rôle existant

Vous pouvez modifier un rôle existant pour affecter les privilèges Dell.

**REMARQUE :** Assurez-vous que vous êtes connecté en tant qu'utilisateur doté de droits d'administrateur.

1. Connectez-vous au client Web vSphere avec des droits d'administrateur.
2. Dans le volet de gauche, cliquez sur **Administration → Rôles** dans le client Web vSphere.
3. Sélectionnez un système de serveur vCenter dans la liste déroulante **Fournisseur de rôles**.
4. Sélectionnez le rôle dans la liste des **Rôles**, puis cliquez sur .
5. Cliquez sur **Privilèges**, développez **Dell**, puis sélectionnez les privilèges Dell suivants pour le rôle sélectionné et cliquez sur **OK** :
   - Dell.Configuration
   - Dell Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   Pour plus d'informations sur les rôles OMIVV disponibles dans vCenter, voir la section Rôles et autorisations de sécurité du document *OpenManage Integration for VMware vCenter User's Guide (Guide d'utilisation d'OpenManage Integration for VMware vCenter)* disponible sur le site `Dell.com/support/manuals`.

Les modifications apportées aux autorisations et aux rôles prennent effet immédiatement. L'utilisateur disposant des privilèges nécessaires peut désormais effectuer les opérations d'intégration OpenManage pour VMware vCenter.

**REMARQUE :** Pour toutes les opérations vCenter, l'OMIVV utilise les privilèges de l'utilisateur inscrit et non les privilèges de l'utilisateur connecté.

**REMARQUE :** Si certaines pages d'OMIVV sont accessibles sans affectation de privilèges Dell à l'utilisateur connecté, l'erreur 2000000 s'affiche.

# Enregistrement d'OpenManage Integration for VMware vCenter et importation du fichier de licence

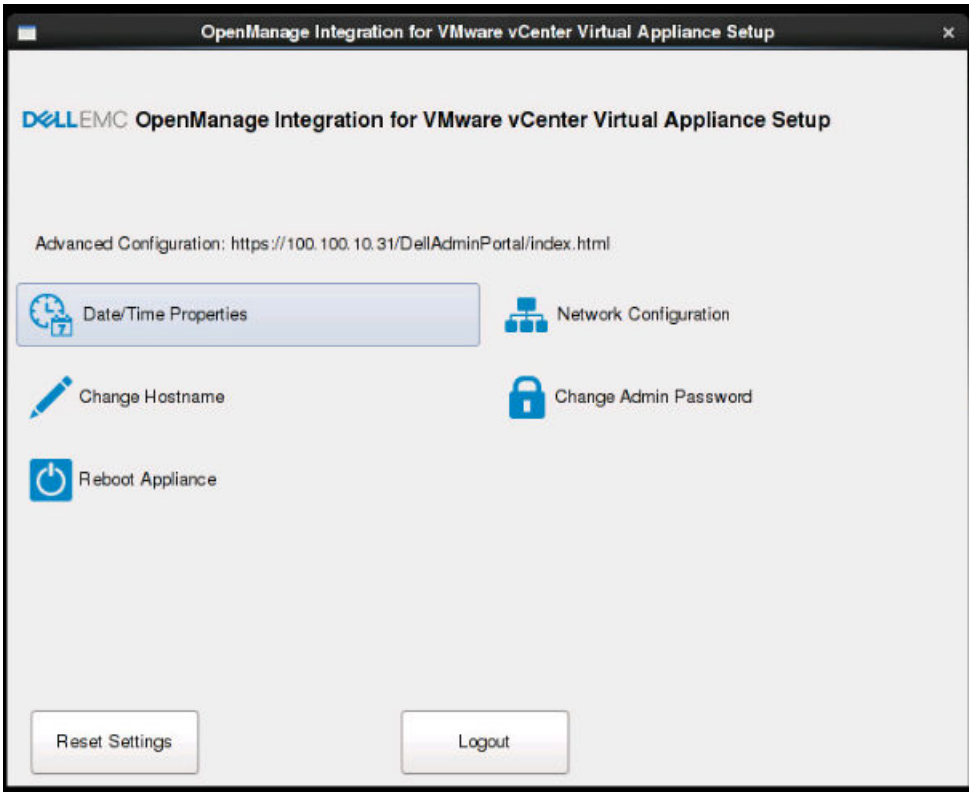
Assurez-vous que vos licences sont prêtes à être téléchargées à l'adresse http://www.dell.com/support/licensing. Si vous avez commandé plusieurs licences, elles peuvent être expédiées séparément, à des moments différents. Vous pouvez contrôler l'état d'autres éléments de licence dans la section État des commandes. Le fichier de licence est disponible au format .XML.

**REMARQUE :** Si vous souhaitez charger un certificat personnalisé pour votre appliance, assurez-vous de charger le nouveau certificat avant l'enregistrement dans vCenter. Si vous chargez le nouveau certificat personnalisé après l'enregistrement dans vCenter, des erreurs de communication s'affichent dans le client Web. Pour résoudre ce problème, annulez l'enregistrement et recommencez l'enregistrement de l'appliance dans vCenter.

1. Dans le client Web vSphere, cliquez sur **Accueil** > **Hôtes et clusters**, puis dans le panneau de gauche, localisez l'OMIVV que vous venez de déployer et cliquez ensuite sur **Mettre sous tension la machine virtuelle**.

   Au cours du déploiement, si vous sélectionnez **Mettre sous tension après le déploiement**, la machine virtuelle se met sous tension automatiquement une fois le déploiement terminé.
2. Pour exécuter la **Console d'administration**, cliquez sur l'onglet **Console** dans la fenêtre principale **VMware vCenter**.
3. Permettez à l'OMIVV de terminer son démarrage, puis saisissez le nom d'utilisateur **Admin** (par défaut) et appuyez sur **Entrée**.
4. Entrez un nouveau mot de passe administrateur. Assurez-vous que le mot de passe administrateur est conforme aux règles de complexité des mots de passe qui s'affichent à l'écran. Appuyez sur **Entrée**.
5. Entrez à nouveau le mot de passe fourni précédemment et appuyez sur **Entrée**.
   Appuyez sur **Entrée** pour configurer le réseau et les informations de fuseau horaire dans l'appliance OMIVV.
6. Pour configurer les informations de fuseau horaire d'OMIVV, cliquez sur **Propriétés Date/Heure**.

**Figure 1. Onglet Console**




7. Dans l'onglet **Date et heure**, sélectionnez l'option **Synchroniser la date et l'heure sur le réseau**.
   La boîte de dialogue **Serveurs NTP** s'affiche.
8. Ajoutez les détails du serveur NTP valide avec lequel votre vCenter est synchronisé.
9. Cliquez sur **Fuseau horaire** et sélectionnez le fuseau horaire applicable, puis cliquez sur **OK**.
10. Pour configurer une adresse IP statique à l'appliance OMIVV, cliquez sur **Configuration réseau** ou passez à l'étape 17.
11. Sélectionnez **Auto eth0**, puis cliquez sur **Modifier**.
12. Sélectionnez l'onglet **Paramètres IPv4** et sélectionnez **Manuel** dans la liste déroulante **Méthode**.
13. Cliquez sur **Ajouter**, puis ajoutez une adresse IP, un masque de réseau et des informations de passerelle valides.
14. Dans le champ **Serveurs DNS**, fournissez les informations du serveur DNS.
15. Cliquez sur **Appliquer**.
16. Pour modifier le nom d'hôte de l'appliance OMIVV, cliquez sur **Modifier le nom d'hôte**.
17. Entrez un nom d'hôte valide et cliquez sur **Mettre à jour le nom d'hôte**.

    **REMARQUE :** Une fois le nom d'hôte et le NTP modifiés, assurez-vous de redémarrer le système.

    **REMARQUE :** Si des serveurs vCenter sont enregistrés avec l'appliance OMIVV, désenregistrez puis enregistrez de nouveau toutes les instances de vCenter.

    Avant d'ouvrir la console d'administration, assurez-vous de mettre à jour manuellement toutes les références sur l'appliance, telles que le serveur de provisionnement dans l'iDRAC, DRM.

18. Ouvrez la **Console Administration** depuis un navigateur pris en charge.

    Pour ouvrir la **Console Administration**, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou ouvrez un navigateur web et saisissez l'URL `https://<ApplianceIP or Appliance hostname>`.

    L'adresse IP est l'adresse IP de la machine virtuelle de l'appliance, non pas celle de l'hôte ESXi. Vous pouvez accéder à la Console Administration en utilisant l'URL mentionnée dans la partie supérieure de la console.
    Par exemple : `https://10.210.126.120` ou `https://myesxihost`
    L'URL n'est pas sensible à la casse.

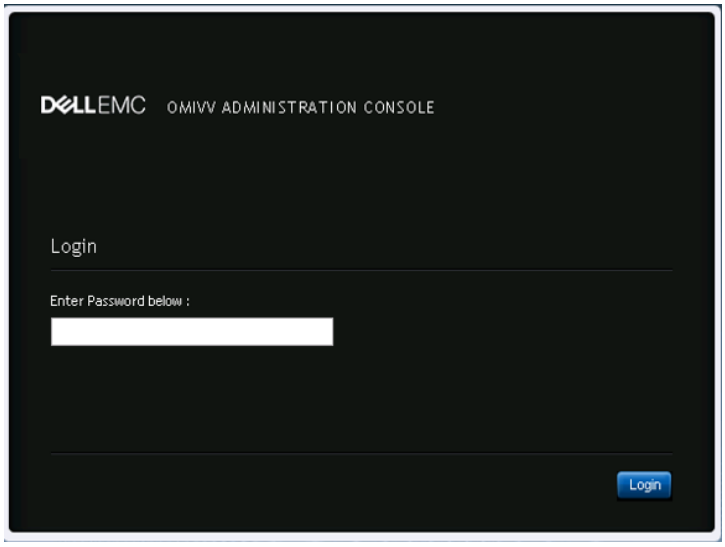



**Figure 2. Console Administration**

19. Dans la fenêtre d'ouverture de session de la **Console d'administration**, entrez le mot de passe, puis cliquez sur **Connexion**.

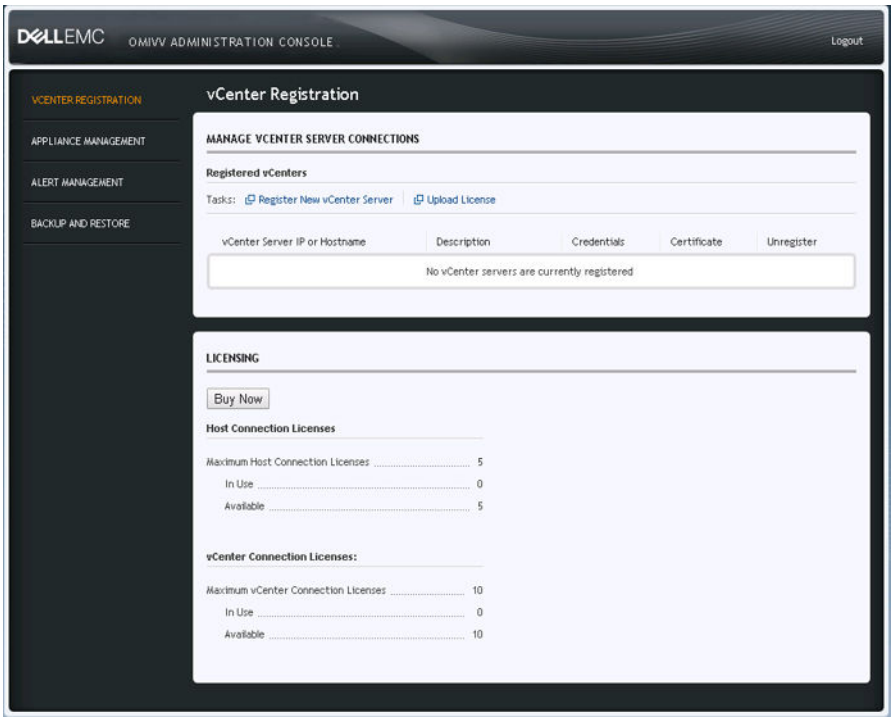



**Figure 3. Fenêtre d'enregistrement vCenter provenant de la Console d'administration**

20. Dans la fenêtre **Enregistrement vCenter**, cliquez sur **Enregistrer un nouveau serveur vCenter**.
21. Dans la fenêtre **Enregistrer un nouveau serveur vCenter**, effectuez les sous-étapes suivantes :
    a. Sous **Nom vCenter**, dans la zone de texte **Adresse IP ou nom d'hôte du serveur vCenter**, entrez l'adresse IP ou le nom d'hôte du serveur, puis dans la zone de texte **Description**, entrez une description.

    La description est facultative.

    **REMARQUE :** Il est recommandé d'enregistrer OpenManage Integration for VMware vCenter dans VMware vCenter en utilisant le nom de domaine complet. Assurez-vous que le nom d'hôte de vCenter est compréhensible par le serveur DNS pour les enregistrements utilisant un nom de domaine complet.

    b. Sous **Compte d'utilisateur vCenter**, entrez le nom de l'utilisateur Admin ou le nom de l'utilisateur disposant des privilèges nécessaires dans **Nom d'utilisateur vCenter**.

Entrez le **nom d'utilisateur** en tant que `domaine\utilisateur` ou `domaine/utilisateur` ou `utilisateur@domaine`. Le logiciel OMIVV utilise le compte administrateur ou le compte utilisateur disposant des privilèges nécessaires pour l'administration de vCenter.

c. Sous **Mot de passe**, saisissez le mot de passe.

d. Dans **Vérifier le mot de passe**, entrez à nouveau le mot de passe.

22. Cliquez sur **S'inscrire**.

**REMARQUE :** OpenManage Integration for VMware vCenter prend actuellement en charge jusqu'à 1 000 hôtes pour un mode de déploiement large avec une seule instance vCenter ou plusieurs serveurs vCenter en utilisant le mode lié.

23. Effectuez l'une des actions suivantes :

- Si vous utilisez la version d'essai d'OMIVV, vous pouvez afficher l'icône OMIVV.
- Si vous utilisez la version de produit intégrale, le fichier de licence peut être téléchargé à partir de Dell Digital Locker, à l'adresse http://www.dell.com/support/licensing et vous pouvez importer cette licence vers votre appliance virtuelle. Pour importer le fichier de licence, cliquez sur **Charger la licence**.

24. Dans la fenêtre **Charger la licence**, cliquez sur le bouton **Parcourir** pour atteindre le fichier de licence. Ensuite, cliquez sur **Charger** pour importer ce fichier.

**REMARQUE :** Si vous modifiez le fichier de licence (fichier .XML), celui-ci ne fonctionne pas et vous pouvez télécharger le fichier .XML (clé de licence) via Dell Digital Locker. Si vous ne parvenez pas à télécharger vos clés de licence, contactez le service de support Dell en allant sur www.dell.com/support/softwarecontacts pour trouver le numéro de téléphone du service du support Dell de votre zone géographique pour votre produit.

Une fois l'OMIVV enregistré, l'icône OMIVV s'affiche sous la catégorie **Administration** de la page d'accueil du client Web.

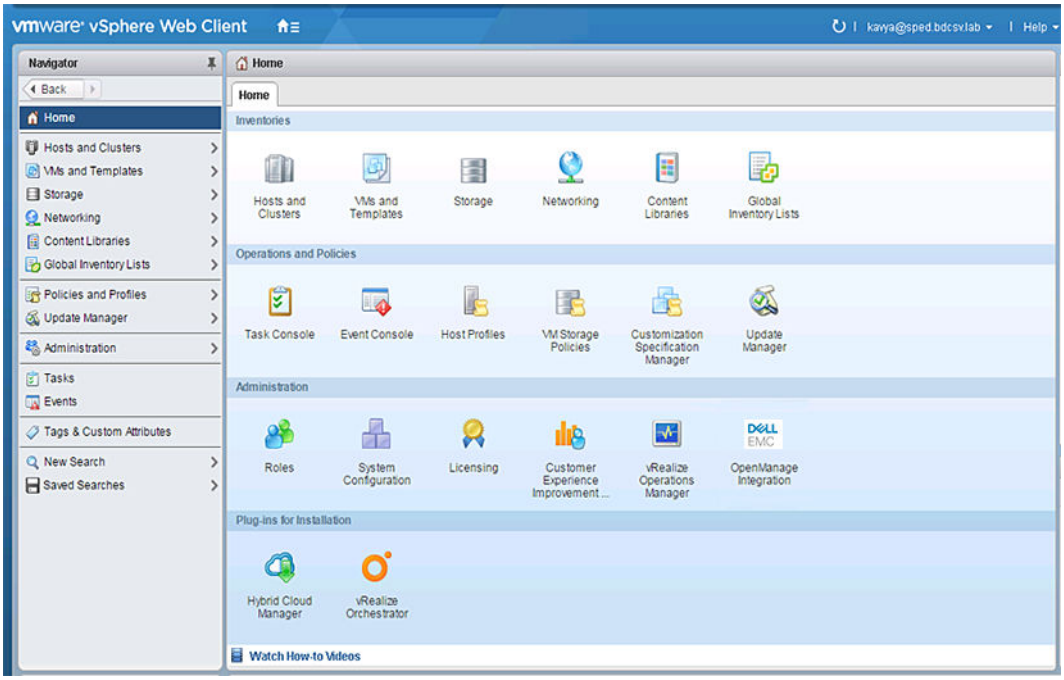



**Figure 4. OpenManage Integration for VMware vCenter a été ajouté avec succès à vCenter**

Pour toutes les opérations vCenter, l'OMIVV utilise les privilèges d'un utilisateur inscrit et non les privilèges d'un utilisateur connecté.

Par exemple, un utilisateur X disposant des privilèges nécessaires enregistre OMIVV avec vCenter et l'utilisateur Y ne dispose que des privilèges Dell. L'utilisateur Y peut désormais se connecter au vCenter et déclencher une tâche de mise à jour du micrologiciel à partir d'OMIVV. Lors de l'exécution de la tâche de mise à jour du micrologiciel, OMIVV utilise les privilèges de l'utilisateur X pour mettre la machine en mode maintenance ou redémarrer l'hôte.

# Mise à niveau des vCenter enregistrés

Vous pouvez mettre à niveau un vCenter enregistré pour des utilisateurs administrateurs ou non administrateurs. Avant de mettre à niveau un vCenter enregistré, voir la documentation VMware si vous mettez à niveau vers la dernière version du serveur vCenter, comme vCenter 6.5. Effectuez les tâches dans l'une des options suivantes après la mise à niveau d'un vCenter enregistré, le cas échéant :

- Pour les utilisateurs non-administrateurs :
  1. Attribuez des privilèges supplémentaires aux utilisateurs non-administrateurs, si nécessaire. Voir Privilèges requis pour les utilisateurs non administrateurs , page 17.

     Par exemple, lorsque vous mettez à niveau de vCenter 6.0 vers vCenter 6.5, attribuez les privilèges supplémentaires.
  2. Redémarrez l'appliance OMIVV enregistrée.
- Pour les utilisateurs administrateurs :
  1. Redémarrez l'appliance OMIVV enregistrée.

# Vérification de l'installation

Les étapes suivantes vérifient la réussite de l'installation d'OMIVV :

1. Fermez toutes les fenêtres vSphere Client et démarrez un nouveau client Web VSphere.
2. Assurez-vous que l'icône OMIVV s'affiche dans le client Web VSphere.
3. Vérifiez si le vCenter peut communiquer avec OMIVV en envoyant une commande PING à partir du serveur vCenter vers l'adresse IP ou le nom d'hôte de l'appliance virtuelle.
4. Dans le client Web vSphere, cliquez sur **Accueil** > **Administration** > **Solutions**, puis cliquez sur **Gestion des plug-ins** (dans les anciennes versions vCenter) ou **Plug-ins du client** (dans les versions plus récentes).

   Pour plus d'informations sur les restrictions d'accès à la page **Gestion des plug-ins** ou **Plug-ins du client**, voir la documentation VMware.
5. Dans la fenêtre **Gestion des plug-ins** ou **Plug-ins du client**, vérifiez si OMIVV est installé et activé.

# Migration d'une version antérieure à la version 4.2

Vous pouvez démarrer avec un nouveau déploiement d'OVF version 4.2 après la désinstallation d'une version antérieure, puis migrer les données de la version antérieure à la version 4.2 en utilisant le chemin de sauvegarde et de restauration.

Pour effectuer une migration à partir d'une version antérieure à la version OMIVV 4.2, procédez comme suit :

1. Effectuez une sauvegarde de la base de données de la version antérieure (v4.x).

   Pour plus d'informations sur la sauvegarde, voir le *Guide d'utilisation d'OpenManage Integration for VMware vCenter* disponible à l'adresse `Dell.com/support/manuals`.
2. Mettez l'ancienne appliance hors tension depuis le vCenter.

   **REMARQUE :** N'annulez pas l'enregistrement du plug-in OMIVV sur le serveur vCenter. Cela entraînerait la suppression de toutes les alarmes enregistrées sur le serveur vCenter par le plug-in OMIVV ainsi que de toutes les personnalisations effectuées sur les alarmes, telles que les actions. Pour plus d'informations, voir *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2* (Guide d'installation rapide d'OpenManage Integration for VMware vCenter version 4.2 pour client Web vSphere), si vous avez annulé l'enregistrement du plug-in après la sauvegarde.
3. Déployez le nouvel OpenManage Integration OVF version 4.2.

   Pour plus d'informations sur le déploiement de l'OVF, voir *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2* (Guide d'installation rapide d'OpenManage Integration for VMware vCenter version 4.2 pour client Web vSphere).
4. Mettez l'appliance OpenManage Integration version 4.2 sous tension.
5. Configurez le réseau et le fuseau horaire de l'appliance OMIVV.

   Assurez-vous que la nouvelle appliance OpenManage Integration version 4.2 dispose de la même adresse IP que l'ancienne appliance. Pour configurer les détails du réseau, voir *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2* (Guide d'installation rapide d'OpenManage Integration for VMware vCenter version 4.2 pour client Web vSphere).

**REMARQUE :** Le plug-in OMIVV risque de ne pas fonctionner correctement si l'adresse IP de l'appliance OMIVV 4.2 est différente de l'adresse IP de l'ancienne appliance. Dans ce cas, annulez puis recommencez l'enregistrement de toutes les instances vCenter.

6. Restaurez la base de données sur la nouvelle appliance OMIVV.

   **REMARQUE :** Si vous avez activé Proactive HA dans des clusters, OMIVV annule l'enregistrement du fournisseur Dell Inc pour ces clusters et enregistre à nouveau le fournisseur Dell Inc après restauration. Par conséquent, les mises à jour d'intégrité pour les hôtes Dell ne sont pas disponibles tant que la restauration n'est pas terminée.

   Pour en savoir plus, voir la section **Restauration de la base de données OMIVV depuis une sauvegarde** dans l'*OpenManage Integration for VMware vCenter User Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals`.

7. Chargez le nouveau fichier de licence.

   Pour plus d'informations sur la gestion des licences, voir *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2* (Guide d'installation rapide d'OpenManage Integration for VMware vCenter version 4.2 pour client Web vSphere).

8. Vérifiez l'appliance.

   Pour plus d'informations sur la vérification de l'appliance, voir *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2* (Guide d'installation rapide d'OpenManage Integration for VMware vCenter version 4.2 pour client Web vSphere) pour garantir le bon déroulement de la migration de la base de données.

9. Exécutez l'**inventaire** sur tous les hôtes.

   **REMARQUE :**

   Une fois la mise à niveau effectuée, il est recommandé d'exécuter à nouveau l'inventaire sur tous les hôtes gérés par l'OMIVV. Pour plus d'informations, voir **Exécution de tâches d'inventaire** dans le document *OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter).

   Si l'adresse IP de la nouvelle appliance OMIVV version 4.2 est différente de celle de l'ancienne appliance, la destination des interruptions SNMP doit être configurée de sorte à pointer vers la nouvelle appliance. Pour les serveurs de 12e génération et de générations ultérieures, ce problème est réglé en exécutant l'inventaire sur ces hôtes. Avec les hôtes antérieurs à la 12e génération qui étaient compatibles avec les versions antérieures, le changement d'adresse IP s'affiche comme non compatible et vous oblige à configurer Dell EMC OpenManage Server Administrator (OMSA). Pour plus d'informations sur la résolution la compatibilité des hôtes, voir **Rapports et correction de la conformité des hôtes vSphere** dans le document *OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals`.

# Récupération d'OMIVV après le désenregistrement d'une version antérieure d'OMIVV

Si vous avez désenregistré le plug-in OMIVV après avoir effectué une sauvegarde de la base de données de l'ancienne version, suivez les étapes suivantes avant de poursuivre la migration :

**REMARQUE :** Le désenregistrement du plug-in supprime toutes les personnalisations effectuées sur les alarmes enregistrées par le plug-in. Les étapes suivantes ne restaurent pas les personnalisations, mais elles enregistrent à nouveau les alarmes dans leur état par défaut.

1. Effectuez les étapes 3 à 5 de la section Migration d'une version antérieure à la version 4.2 , page 23.
2. Enregistrez le plug-in sur le vCenter enregistré préalablement dans l'ancien plug-in.
3. Pour terminer la migration, effectuez les étapes 6 à 9 dans Migration d'une version antérieure à la version 4.2 , page 23.

# 2

# Configuration d'appliance pour VMware vCenter

Une fois l'installation de base d'OMIVV effectuée et les vCenters enregistrés, cliquez sur l'icône OMIVV pour afficher l'**Assistant Configuration initiale**. Pour procéder à la configuration de l'appliance, utilisez l'une des méthodes suivantes :

- Configuration de l'appliance via l'**Assistant Configuration initiale**.
- Configuration de l'appliance via l'onglet **Paramètres** dans OMIVV.

Vous pouvez utiliser l'**Assistant Configuration initiale** pour configurer les paramètres de l'appliance OMIVV au premier lancement. Pour les instances suivantes, utilisez l'onglet **Paramètres**.

**REMARQUE :** Les deux méthodes utilisent une interface utilisateur similaire.

**Sujets :**



# Tâches de configuration via l'Assistant Configuration

**REMARQUE :** Si une erreur de communication Web s'affiche lors de l'exécution des tâches associées à OMIVV après la modification des paramètres DNS, effacez le cache du navigateur, déconnectez-vous du client Web, puis reconnectez-vous.

L'Assistant Configuration permet d'afficher et d'effectuer les tâches suivantes :

- Afficher la page d'accueil de l'Assistant Configuration.
- Sélection de vCenters. Voir Sélection de vCenters.
- Création d'un profil de connexion. Voir Création d'un profil de connexion.
- Configuration des événements et alarmes. Voir configuration des événements et alarmes.
- Planification des tâches d'inventaire. Voir Planification des tâches d'inventaire.
- Exécution d'une tâche de récupération de la garantie. Voir Exécution d'une tâche de récupération de la garantie.

## Affichage de la boîte de dialogue de bienvenue de l'Assistant Configuration

Pour configurer OMIVV après l'installation et l'enregistrement auprès du vCenter, affichez l'**Assistant Configuration initiale** en procédant comme suit :

1. Dans le client Web vSphere, cliquez sur **Accueil**, puis sur l'icône **OpenManage Integration**.

   Pour accéder à l'Assistant Configuration initiale, vous pouvez utiliser l'une des méthodes suivantes :

   - Lorsque vous cliquez sur l'icône **OpenManage Integration** pour la première fois, l'**Assistant Configuration initiale** s'affiche automatiquement.
   - Depuis **OpenManage Integration** > **Mise en route**, cliquez sur **Démarrer l'Assistant Configuration initiale**.
2. Dans la boîte de dialogue **Accueil**, examinez les étapes, puis cliquez sur **Suivant**.

## Sélection de vCenters

Dans la boîte de dialogue **Sélection de vCenter**, vous pouvez configurer les serveurs vCenter suivants :

- un vCenter particulier

- Tous les vCenters enregistrés

Pour accéder à la boîte de dialogue **Sélection de vCenter** :

1. Dans l'**Assistant Configuration initiale**, dans la boîte de dialogue **Bienvenue**, cliquez sur **Suivant**.
2. Sélectionnez un ou tous les vCenters enregistrés dans la liste déroulante **vCenters**.

   Sélectionnez un vCenter parmi ceux qui ne sont pas encore configurés ou sélectionnez un vCenter que vous venez d'ajouter à votre environnement. La page Sélection de vCenter vous permet de sélectionner un ou plusieurs vCenters pour en configurer les paramètres.
3. Pour continuer et afficher la boîte de dialogue **Description du profil de connexion**, cliquez sur **Suivant**.

   **REMARQUE :** Si vous disposez de plusieurs serveurs vCenter faisant partie de la même authentification unique (SSO) et enregistrés avec la même appliance OMIVV, et si vous choisissez de configurer un seul serveur vCenter, les étapes 1 à 3 doivent être répétées jusqu'à ce que vous ayez configuré chaque vCenter.

# Création d'un profil de connexion

Avant d'utiliser les informations d'identification Active Directory pour un profil de connexion, assurez-vous que :

- Le compte d'utilisateur Active Directory existe dans Active Directory.
- Le contrôleur iDRAC et l'hôte sont configurés pour l'authentification basée sur Active Directory.

Un profil de connexion stocke les informations d'identification du contrôleur iDRAC et de l'hôte utilisées par OMIVV pour communiquer avec les serveurs EMC Dell. Chaque serveur Dell EMC doit être associé à un profil de connexion pour être géré par OMIVV. Vous pouvez attribuer plusieurs serveurs à un même profil de connexion. Vous pouvez créer un profil de connexion à l'aide de l'Assistant de configuration ou depuis l'onglet **OpenManage Integration for VMware vCenter** > **Paramètres**. Vous pouvez vous connecter à l'iDRAC et à l'hôte à l'aide des informations d'identification Active Directory.

**REMARQUE :** Les informations d'identification Active Directory du contrôleur iDRAC et de l'hôte peuvent être identiques ou distinctes.

**REMARQUE :** Il est impossible de créer un profil de connexion si le nombre d'hôtes ajoutés dépasse la limite de licences permettant la création d'un profil de connexion.

**REMARQUE :** Un hôte de châssis MX peut être géré à l'aide d'une seule adresse IP de gestion de châssis unifiée. Pour gérer un châssis MX à l'aide d'un profil de châssis, voir Création d'un profil de châssis. Dell EMC recommande de gérer les hôtes dotés d'un châssis MX avec une IP iDRAC afin d'obtenir l'intégralité des fonctions OMIVV.

1. Dans la boîte de dialogue **Description du profil de connexion**, cliquez sur **Suivant**.
2. Dans la boîte de dialogue **Nom et informations d'identification du profil de connexion**, saisissez le **Nom du profil** de connexion et éventuellement une **Description** du profil de connexion.
3. Dans la boîte de dialogue **Nom et informations d'identification du profil de connexion**, sous **Informations d'identification iDRAC**, effectuez l'une des opérations suivantes, selon que vous configurez le contrôleur iDRAC avec ou sans Active Directory :

   **REMARQUE :** Le compte iDRAC exige que l'utilisateur détienne des privilèges d'administration pour mettre à jour le micrologiciel, appliquer des profils matériels, appliquer des profils système aux serveurs de 14e génération et déployer un hyperviseur.

   - Pour les adresses IP de l'iDRAC déjà configurées et activées pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; sinon, configurez les informations d'identification iDRAC plus bas.
     a. Dans **Nom d'utilisateur** Active Directory, saisissez le nom de l'utilisateur. Saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou nom_utilisateur@domaine. Le nom d'utilisateur est limité à 256 caractères.
     b. Dans **Mot de passe** Active Directory, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
     c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.
     d. En fonction de vos besoins, effectuez l'une des opérations suivantes :
        - Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
        - Pour ne pas stocker le certificat iDRAC et en effectuer la vérification au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.
   - Pour configurer les informations d'identification iDRAC sans Active Directory, procédez comme suit :
     a. Dans **Nom d'utilisateur**, saisissez le nom de l'utilisateur. Le nom d'utilisateur est limité à 16 caractères. Pour en savoir plus sur les restrictions de nom d'utilisateur de la version d'iDRAC que vous utilisez, voir la documentation iDRAC.
     b. Dans la zone de texte **Mot de passe**, saisissez le mot de passe. Le mot de passe ne doit pas comporter plus de 20 caractères.
     c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.

d. Effectuez l'une des actions suivantes :
   - Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
   - Pour ne pas stocker le certificat iDRAC et en effectuer la vérification au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.

4. Dans **Racine hôte**, effectuez l'une des opérations suivantes :
   - Dans le cas des hôtes déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, sélectionnez **Utiliser Active Directory** et effectuez les opérations suivantes ; sinon, configurez les informations d'identification de l'hôte :
     a. Dans **Nom d'utilisateur** Active Directory, saisissez le nom de l'utilisateur. Saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou nom_utilisateur@domaine. Le nom d'utilisateur est limité à 256 caractères.

        **REMARQUE :** Pour les restrictions de nom d'utilisateur et de domaine d'hôte, voir les informations suivantes :

        Exigences relatives au nom d'utilisateur d'hôte :
        - Entre 1 et 64 caractères
        - Aucun caractère non imprimable

        Exigences pour le domaine d'hôte :
        - Entre 1 et 64 caractères
        - Le premier caractère doit être alphabétique.
        - Ne peut pas contenir d'espace.

     b. Dans **Mot de passe** Active Directory, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
     c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.
     d. Effectuez l'une des actions suivantes :
        - Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
        - Pour ne pas stocker le certificat iDRAC et en effectuer la vérification au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.
   - Pour configurer les informations d'identification de l'hôte sans Active Directory, procédez comme suit :
     a. Dans **Nom d'utilisateur**, le nom d'utilisateur est **`root`**. Il s'agit du nom d'utilisateur par défaut et vous ne pouvez pas le modifier. Toutefois, si l'option Active Directory est configurée, vous pouvez choisir n'importe quel utilisateur Active Directory au lieu de racine.
     b. Dans la zone de texte **Mot de passe**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.

        **REMARQUE :** Les informations d'identification OMSA sont les mêmes que celles utilisées pour les hôtes ESXi.

     c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.
     d. Effectuez l'une des actions suivantes :
        - Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
        - Pour ne pas stocker le certificat iDRAC et effectuer la vérification du certificat au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.

5. Cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Hôtes associés au profil de connexion**, sélectionnez les hôtes pour le profil de connexion, puis cliquez sur **OK**.

   **REMARQUE :** Si les hôtes OEM ne sont pas affichés sur la fenêtre Sélectionner les hôtes, ajoutez les OEM hôtes à l'aide de l'Assistant Ajouter les hôtes OEM. Voir la rubrique **Ajouter des hôtes OEM** du *Guide d'utilisation* (Ajout d'hôtes OEM).

7. Pour tester le profil de connexion, sélectionnez un ou plusieurs hôtes, puis cliquez sur **Tester la connexion**.

   **REMARQUE :** Cette étape est facultative. Elle est utilisée pour vérifier si les informations d'identification de l'hôte et de l'iDRAC sont correctes. Bien que cette étape soit facultative, Dell EMC vous recommande de tester le profil de connexion.

   **REMARQUE :** Si le service WBEM est désactivé pour tous les hôtes exécutant ESXi 6.5 ou une version ultérieure, WBEM est automatiquement activé lorsque vous effectuez le test de connexion et l'inventaire sur ces hôtes.

   **REMARQUE :** Si vous sélectionnez **Tous les vCenters enregistrés** lors de la création du profil de connexion, le test de connexion échoue pour tous les hôtes exécutant ESXi 6.5 ou une version ultérieure avec le service WBEM désactivé. Le cas échéant, il est recommandé de terminer les actions de l'Assistant Profil de connexion, d'exécuter l'inventaire sur les hôtes, puis d'effectuer à nouveau le test de profil de connexion.

**REMARQUE :** Vous pouvez voir que le test de connexion échoue pour l'hôte et indique que des informations d'identification non valides ont été entrées, même après la saisie d'informations valides. Cela peut se produire car l'ESXi bloque l'accès. Patientez 15 minutes, puis relancez le test de connexion.

8. Pour terminer la création du profil, cliquez sur **Suivant**.
   Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis l'Assistant. Vous pouvez modifier ou créer d'autres profils de connexion pour ce serveur vCenter depuis la page **Gérer** > **Profils Profils de connexion** après avoir exécuté l'Assistant de configuration. Voir la rubrique **Modification d'un profil de connexion** dans *OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals.`.

**REMARQUE :** Pour les serveurs non dotés de carte iDRAC Express ou Enterprise, le résultat du test de connexion de l'iDRAC n'est pas applicable pour ce système.

Une fois les hôtes ajoutés au profil de connexion, l'adresse IP d'OMIVV est automatiquement définie sur la destination d'interruption SNMP de l'iDRAC de l'hôte et OMIVV active automatiquement le service WBEM pour les hôtes exécutant ESXi 6.5 ou une version ultérieure. OMIVV utilise le service WBEM pour synchroniser correctement les relations de l'hôte ESXi et du contrôleur iDRAC. Si la configuration de la destination d'interruption SNMP échoue et/ou l'activation du service WBEM échoue pour certains hôtes, ceux-ci sont répertoriés comme non conformes. Pour afficher les hôtes non conformes qui nécessitent une destination d'interruption SNMP pour être reconfigurés et/ou des services WBEM pour être activés, voir la rubrique **Rapports et correction de la conformité des hôtes vSphere** dans l'*OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) disponible à l'adresse `Dell.com/support/manuals.`.

# Planification des tâches d'inventaire

Vous pouvez configurer la planification de l'inventaire à l'aide de l'Assistant Configuration ou d'OpenManage Integration, dans l'onglet **OpenManage Integration** > **Gérer** > **Paramètres**.

**REMARQUE :** Pour vous assurer qu'OMIVV continue d'afficher des informations à jour, Dell recommande de planifier une tâche d'inventaire périodique. Le travail d'inventaire consomme un minimum de ressources et ne dégrade pas les performances de l'hôte.

**REMARQUE :** Le châssis est automatiquement détecté après l'exécution de l'inventaire de tous les hôtes. Si le châssis est ajouté à un profil de châssis, l'inventaire s'exécute alors automatiquement. Dans un environnement SSO avec plusieurs serveurs vCenter, l'inventaire du châssis s'exécute automatiquement pour chaque vCenter lorsque l'inventaire de n'importe lequel d'entre eux s'exécute à une heure planifiée.

**REMARQUE :** Les paramètres de cette page sont réinitialisés sur les paramètres par défaut chaque fois que l'Assistant Configuration est appelé. Si vous avez déjà configuré une planification pour l'inventaire, assurez-vous que vous répliquez la planification précédente dans cette page avant de suivre les fonctions de l'Assistant afin que la planification précédente ne soit pas remplacée par les paramètres par défaut.

1. Dans l'**Assistant Configuration initiale**, dans la boîte de dialogue **Planification d'inventaire**, sélectionnez **Activer la récupération des données d'inventaire** si cette option n'est pas déjà activée. Par défaut, l'option **Activer la récupération des données d'inventaire** est activée.
2. Sous **Planification de la récupération des données d'inventaire**, procédez comme suit :
   a. Cochez la case en regard de chaque jour de la semaine pendant lequel vous voulez exécuter l'inventaire.
      Par défaut, **tous les jours** sont sélectionnés.
   b. Dans **Heure de récupération des données**, entrez l'heure au format HH:MM.
      L'heure entrée est votre heure locale. Par conséquent, si vous voulez exécuter l'inventaire dans le fuseau horaire de l'appliance virtuelle, calculez le décalage horaire entre votre fuseau horaire local et celui de l'appliance virtuelle, puis entrez l'heure de manière appropriée.
   c. Pour appliquer les modifications et continuer, cliquez sur **Suivant**.

   Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis cet Assistant. Vous pouvez modifier les détails de planification de l'inventaire des hôtes depuis l'onglet **Gérer** > **Paramètres** après avoir terminé la configuration depuis l'Assistant Configuration. Voir **Modification des planifications de tâche d'inventaire** dans le document *OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter) à l'adresse `Dell.com/support/manuals`.

# Exécution de tâches de récupération de la garantie

La configuration d'une tâche de récupération de la garantie peut être effectuée via l'onglet Paramètres d'OMIVV. De plus, vous pouvez également exécuter ou planifier une tâche de récupération de la garantie à partir de la **File d'attente des tâches** > **Garantie**. Les tâches planifiées sont répertoriées dans la file d'attente des tâches. Dans un environnement SSO comprenant plusieurs serveurs vCenter, la garantie du châssis s'exécute automatiquement avec chaque vCenter lorsque la garantie d'un vCenter quelconque est exécutée. Cependant, la garantie ne s'exécute pas automatiquement si elle n'est pas ajoutée au profil du châssis.

**REMARQUE :** Les paramètres de cette page sont réinitialisés sur les paramètres par défaut chaque fois que l'Assistant Configuration est appelé. Si vous avez déjà configuré une tâche de récupération de garantie, assurez-vous que vous répliquez la tâche de récupération de garantie planifiée sur cette page avant de suivre les fonctions de l'Assistant afin que la récupération de garantie précédente ne soit pas écrasée par les paramètres par défaut.

1. Dans la boîte de dialogue **Planification de garantie**, sélectionnez **Activer la récupération des données de garantie**.
2. Dans **Planification de la récupération des données de garantie**, procédez comme suit :
   a. Cochez la case en regard de chaque jour de la semaine pendant lequel vous voulez exécuter l'inventaire.
   b. Entrez l'heure au format HH:MM.

      L'heure entrée est votre heure locale. Par conséquent, si vous voulez exécuter l'inventaire dans le fuseau horaire de l'appliance virtuelle, calculez le décalage horaire entre votre fuseau horaire local et celui de l'appliance virtuelle, puis entrez l'heure de manière appropriée.
3. Pour enregistrer vos modifications et continuer, cliquez sur **Suivant** afin de poursuivre le paramétrage des **Événements et alarmes**. Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis l'Assistant. Vous ne pourrez modifier les planifications de tâches de garantie qu'à l'issue de l'exécution de l'Assistant de configuration, à partir de l'onglet **Paramètres**. Voir **Modification des planifications de tâche de garantie** dans le document *OpenManage Integration for VMware vCenter User's Guide (Guide d'utilisation d'OpenManage Integration for VMware vCenter)* disponible sur le site `Dell.com/support/manuals`.

# Configuration des événements et alarmes

Vous pouvez configurer les événements et les alarmes à l'aide de l'**Assistant Configuration initiale** ou à partir de l'onglet **Paramètres** des événements et alarmes. Pour recevoir des événements des serveurs, OMIVV est configuré comme destination d'interruption. Pour les hôtes de 12e génération et ultérieures, vérifiez que la destination d'interruption SNMP est définie dans le contrôleur iDRAC. Pour les hôtes antérieurs à la 12e génération, vérifiez que la destination d'interruption est définie dans l'OMSA.

**REMARQUE :** OMIVV prend en charge les alertes SNMP v1 et v2 pour les hôtes de 12e génération et générations ultérieures et prend en charge uniquement les alertes SNMP v1 pour les hôtes antérieurs à la 12e génération.

1. Dans l'**Assistant Configuration initiale**, sous **Niveaux de publication d'événement**, sélectionnez l'une des options suivantes :
   - Ne publier aucun événement : bloque les événements matériels
   - Publier tous les événements : publie tous les événements matériels
   - Publier uniquement les événements critiques et d'avertissement : publie uniquement les événements matériels de niveau critique et d'avertissement
   - Publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation : publie uniquement les événements critiques et d'avertissement relatifs à la virtualisation ; il s'agit du niveau de publication d'événement par défaut
2. Pour activer tous les événements et alarmes relatifs au matériel, sélectionnez **Activer les alarmes pour tous les hôtes Dell EMC**.

   **REMARQUE :** Les hôtes Dell EMC pour lesquels des alarmes sont activées répondent à certains événements critiques en passant en mode maintenance et vous pouvez alors modifier l'alarme, si nécessaire.

   La boîte de dialogue **Activation des avertissements d'alarmes Dell EMC** s'affiche.
3. Cliquez sur **Continuer** pour accepter la modification ou sur **Annuler** pour l'annuler.

   **REMARQUE :** Cette opération ne peut être effectuée que si vous sélectionnez **Activer les alarmes d'hôtes Dell EMC**.
4. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell EMC, cliquez sur **Restaurer les alarmes par défaut**.

   Il peut s'écouler une minute avant que le changement prenne effet.

   **REMARQUE :** Après la restauration de l'appliance, les paramètres des événements et alarmes ne sont pas activés même si l'interface utilisateur graphique les montre comme activés. Vous devez réactiver les paramètres **Événements et alarmes** depuis l'onglet **Paramètres**.

**REMARQUE :** Les interruptions BMC n'ont pas d'ID de message, de sorte que les alertes ne possèdent pas ces détails dans OMIVV.

5. Cliquez sur **Appliquer**.

## Configuration de la chaîne de communauté d'interruption SNMP

1. Dans la page **OpenManage Integration for VMware vCenter**, sous l'onglet **Gérer** > **Paramètres**, sous **Paramètres d'appliance**, cliquez sur l'icône en regard de la **Chaîne de communauté d'interruption SNMP OMSA**.
   La boîte de dialogue **Paramètres de chaîne de communauté d'interruption SNMP OMSA** s'affiche. Par défaut, la chaîne de communauté d'interruption SNMP est configurée sur **public**.
2. Vous pouvez modifier le texte **public** comme vous le voulez, puis cliquez sur **Appliquer**.

**REMARQUE :** La configuration de la chaîne de communauté d'interruption SNMP pour les serveurs PowerEdge de 11e génération est définie lors de l'installation ou de la mise à niveau d'OMSA via OMIVV.

# Tâches de configuration via l'onglet Paramètres

À l'aide de l'onglet Paramètres, vous pouvez afficher et effectuer les tâches de configuration suivantes :

- Activer le lien OMSA. Voir Activation du lien OMSA.
- Configurer les paramètres de notification d'expiration de la garantie. Voir Configuration des paramètres de notification d'expiration de la garantie.
- Configurer l'espace de stockage de mise à jour du micrologiciel. Voir Configuration de l'espace de stockage de mise à jour du micrologiciel.
- Configurer les notifications de la dernière version de l'appliance. Voir Configuration des notifications de la dernière version de l'appliance.
- Configurer et afficher les événements et alarmes. Voir Configuration des événements et alarmes.
- Afficher les planifications de récupération des données pour l'inventaire et la garantie. Voir Affichage des planifications de récupération des données pour l'inventaire et la garantie.

## Paramètres d'appliance

Dans cette section, configurez les éléments suivants pour l'appliance OMIVV :

- Notification d'expiration de la garantie
- Espace de stockage de mise à jour du micrologiciel
- Notification relative à la dernière version de l'appliance
- Informations d'identification pour le déploiement

## Configuration des paramètres de notification d'expiration de la garantie

1. Dans OpenManage Integration for VMware vCenter, dans l'onglet **Gérer** > **Paramètres**, sous **Paramètres de l'appliance**, cliquez sur **Notification d'expiration de la garantie**.
2. Développez **Notification d'expiration de la garantie** pour afficher les éléments suivants :
   - **Notification d'expiration de la garantie :** indique si le paramètre est activé ou désactivé
   - **Avertissement :** nombre de jours du premier paramètre d'avertissement
   - **Critique :** nombre de jours du paramètre d'avertissement critique
3. Pour configurer des seuils d'expiration de la garantie pour l'avertissement de l'expiration de la garantie, cliquez sur l'icône située à droite de **Notification d'expiration de la garantie**.
4. Dans la boîte de dialogue **Notification d'expiration de la garantie**, procédez comme suit :
   a. Si vous souhaitez activer ce paramètre, sélectionnez **Activer la notification d'expiration de la garantie des hôtes**. Cocher la case active la notification d'expiration de la garantie.
   b. Sous **Alerte de seuil de nombre minimal de jours**, procédez comme suit :

i. Dans la liste déroulante **Avertissement**, sélectionnez le moment où vous souhaitez être averti, en nombre de jours avant expiration de la garantie.
ii. Dans la liste déroulante **Critique**, sélectionnez le moment où vous souhaitez être averti, en nombre de jours avant expiration de la garantie.

5. Cliquez sur **Appliquer**.

## Configuration du référentiel de mise à jour du micrologiciel

Vous pouvez configurer le référentiel de mise à jour du micrologiciel dans l'onglet **Paramètres** d'OMIVV.

1. Dans l'onglet **Gérer** > **Paramètres** d'OpenManage Integration for VMware vCenter, sous **Paramètres d'appliance** à droite de l'option **Référentiel de mise à jour du micrologiciel**, cliquez sur l'icône .
2. Dans la boîte de dialogue **Référentiel de mise à jour du micrologiciel**, sélectionnez une des options suivantes :
   - **Dell Online** : vous pouvez accéder à l'emplacement qui utilise le référentiel Dell de mise à jour du micrologiciel (ftp.dell.com). OpenManage Integration for VMware vCenter télécharge les mises à jour du micrologiciel sélectionnées dans le référentiel Dell et met à jour les hôtes gérés.

     **REMARQUE :** En fonction des paramètres réseau, activez les paramètres de proxy, si le réseau a besoin d'un proxy.
   - **Dossier de réseau partagé :** vous pouvez conserver un référentiel local du micrologiciel dans un partage réseau CIFS ou NFS. Ce référentiel peut soit servir de dépôt pour Server Update Utility (SUU) que Dell utilise pour proposer des mises à jour périodiques ou de référentiel personnalisé créé à l'aide de DRM. Ce partage réseau doit être accessible par OMIVV.

     **REMARQUE :** Si vous utilisez le partage CIFS, les mots de passe de référentiel ne peuvent pas dépasser 31 caractères.

     **REMARQUE :** Assurez-vous que vous utilisez la version la plus récente de Dell EMC Repository Manager (DRM) version (3.0 ) et versions ultérieures.
3. Si vous sélectionnez **Dossier de réseau partagé**, renseignez le champ **Emplacement du fichier de catalogue** en respectant le format suivant :
   - Partage NFS pour le fichier XML : host:/share/filename.xml
   - Partage NFS pour le fichier gz : host:/share/filename.gz
   - Partage CIFS pour le fichier XML : \\host\share\filename.xml
   - Partage CIFS pour le fichier gz : \\host\share\filename.gz

   **REMARQUE :** OMIVV prend uniquement en charge les partages CIFS des versions 1.0 et 2.0 de Server Message Block (SMB).

   **REMARQUE :** Si vous utilisez un partage CIFS, OMIVV vous invite à entrer le nom d'utilisateur et le mot de passe. Les caractères @, % et , ne sont pas pris en charge dans les noms d'utilisateur ni les mots de passe du dossier de réseau partagé.
4. Une fois le téléchargement terminé, cliquez sur **Appliquer**.

**REMARQUE :** La lecture du catalogue à partir de la source et la mise à jour de la base de données OMIVV peut prendre jusqu'à 60-90 minutes.

## Configuration de la notification relative à la dernière version de l'appliance

Pour recevoir des notifications périodiques relatives à la disponibilité de la dernière version d'OMIVV (RPM, OVF, RPM/OVF), effectuez les étapes suivantes pour configurer les notifications concernant la dernière version :

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer → Paramètres**, puis sous **Paramètres d'appliance**, à droite de l'option **Notification relative à la dernière version**, cliquez sur l'icône .
   Par défaut, la notification relative à la dernière version est désactivée.
2. Dans la boîte de dialogue **Notification et planification de récupération relatives à la dernière version**, procédez comme suit :
   a. Si vous souhaitez activer la notification relative à la dernière version, cochez la case **Activer la notification relative à la dernière version**.
   b. Sous **Planification de récupération de la dernière version**, sélectionnez les jours de semaine où vous souhaitez que cette tâche soit exécutée.
   c. Dans **Heure de récupération de la dernière version**, spécifiez l'heure locale requise.
   L'heure que vous fournissez doit être votre heure locale. Tenez compte de l'éventuel décalage horaire pour exécuter cette tâche à un moment approprié sur l'appliance OMIVV.

3. Pour enregistrer les paramètres, cliquez sur **Appliquer**. Pour réinitialiser les paramètres, cliquez sur **Effacer**. Enfin, si vous souhaitez interrompre l'opération, cliquez sur **Annuler**.

## Configuration des informations d'identification pour le déploiement

Les informations d'identification pour le déploiement vous permettent de configurer des informations d'identification afin de communiquer en toute sécurité avec un système sans système d'exploitation détecté par détection automatique, jusqu'à ce que le déploiement du système d'exploitation soit terminé. Pour une communication sécurisée avec l'iDRAC, OMIVV utilise les informations d'identification de la détection initiale jusqu'à la fin du processus de déploiement. Au terme du processus de déploiement du système d'exploitation, OMIVV modifie les informations d'identification iDRAC d'après le profil de connexion. Si vous modifiez les informations d'identification pour le déploiement, tout système nouvellement détecté sera dynamiquement provisionné avec les nouvelles informations d'identification. En revanche, les informations d'identification présentes sur les serveurs détectés avant le changement des informations d'identification pour le déploiement ne sont pas concernées par ce changement.

**REMARQUE :** OMIVV fonctionne comme un serveur de configuration. Les informations d'identification pour le déploiement permettent de communiquer avec l'iDRAC qui utilise le plug-in OMIVV comme serveur de configuration au cours du processus de détection automatique.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer** > **Paramètres**, sous **Paramètres d'appliance** à droite de **Informations d'identification pour le déploiement**, puis cliquez sur l'icône .
2. Dans **Informations d'identification pour déployer un serveur sans système d'exploitation**, sous **Informations d'identification**, saisissez les valeurs suivantes :
   - Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.

     Le nom d'utilisateur doit comporter 16 caractères maximum (uniquement des caractères ASCII imprimables)
   - Dans la zone de texte **Mot de passe**, entrez le mot de passe.

     Le mot de passe doit comporter 20 caractères maximum (uniquement des caractères ASCII imprimables)
   - Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe.

     Assurez-vous que les mots de passe sont identiques.
3. Pour enregistrer les informations d'identification spécifiées, cliquez sur **Appliquer**.

# Paramètres vCenter

Dans cette section, configurez les paramètres vCenter suivants :

- Activer le lien OMSA. Voir Activation du lien OMSA.
- Configurer les événements et alarmes. (Voir la section Configuration des événements et alarmes.)
- Configurer les planifications de récupération des données pour l'inventaire et la garantie. (Voir la section Affichage des planifications de récupération des données pour l'inventaire et la garantie.)

## Activation du lien OMSA

Avant d'activer le lien OMSA, installez et configurez un serveur Web OMSA. Reportez-vous au document *OpenManage Server Administrator Installation Guide (Guide d'installation d'OpenManage Server Administrator)* pour connaître la version d'OMSA utilisée et obtenir des instructions sur l'installation et la configuration du serveur Web OMSA.

**REMARQUE :** OMSA est requis uniquement sur les serveurs PowerEdge de 11e génération ou antérieurs.

1. Dans OpenManage Integration for VMware vCenter, sur l'onglet **Gérer** > **Paramètres**, sous **Paramètres de vCenter** et à droite de l'option URL du serveur Web OMSA, cliquez sur l'icône .
2. Dans la boîte de dialogue **URL du serveur Web OMSA**, entrez l'URL.
   Entrez l'URL complète ainsi que l'adresse HTTPS et le numéro de port 1311.
   *https://<adresse IP du serveur OMSA ou nom FQDN>:1311*
3. Pour appliquer l'URL OMSA à tous les serveurs vCenter, sélectionnez **Appliquer ces paramètres à tous les vCenters**.

   **REMARQUE :** Si vous ne cochez pas cette case, l'URL OMSA ne sera appliquée qu'à un seul vCenter.

4. Pour vérifier que le lien URL OMSA que vous avez fourni fonctionne, accédez à l'onglet **Récapitulatif** de l'hôte et vérifiez que le lien vers la console OMSA est actif dans la section **Informations sur l'hôte OMIVV**.

## Configuration des événements et alarmes

La boîte de dialogue Événements et alarmes du Dell EMC Management Center active ou désactive toutes les alarmes matérielles. L'état actuel des alertes est affiché dans l'onglet Alarmes vCenter. Un événement critique indique un dysfonctionnement du système ou une perte de données réelle ou imminente. Un événement d'avertissement n'est pas forcément significatif, mais peut indiquer un problème futur éventuel. Les événements et alarmes peuvent également être activés à l'aide de VMware Alarm Manager. Les événements sont affichés dans l'onglet Tâches et événements vCenter de la vue Hôtes et clusters. Pour recevoir les événements à partir des serveurs, OMIVV est configuré en tant que destination d'interruption SNMP. Pour les hôtes de 12e génération et générations ultérieures, la destination d'interruption SNMP est définie dans l'iDRAC. Pour les hôtes antérieurs à la 12e génération, la destination d'interruption est définie dans OMSA. Vous pouvez configurer des événements et des alarmes à l'aide d'OpenManage Integration for VMware vCenter depuis l'onglet **Gestion** > **Paramètres**. Sous **Paramètres** vCenter, développez l'en-tête **Événements et alarmes** pour afficher les alarmes vCenter des hôtes Dell EMC (Activé ou Désactivé), ainsi que le niveau de publication de l'événement.

**REMARQUE :** OMIVV prend en charge les alertes SNMP v1 et v2 pour les hôtes de 12e génération et de générations ultérieures. Pour les hôtes antérieurs à la 12e génération, OMIVV prend en charge les alertes SNMP v1.

**REMARQUE :** Pour recevoir les événements Dell, activez les alarmes et les événements.

1. Dans l'onglet **Gérer** > **Paramètres** sous **Paramètres vCenter** d'OpenManage Integration for VMware vCenter, développez **Événements et alarmes**.
   Les **Alarmes vCenter concernant les hôtes Dell EMC** actuelles (activées ou désactivées) ou toutes les alarmes vCenter et le **Niveau de publication d'événement** sont affichés.
2. Cliquez sur l'icône  située à droite de l'en-tête **Événements et alarmes**.
3. Pour activer tous les événements et alarmes relatifs au matériel, sélectionnez **Activer les alarmes pour tous les hôtes Dell EMC**.

   **REMARQUE :** Les hôtes Dell EMC pour lesquels des alarmes sont activées répondent aux événements critiques en passant en mode maintenance, et vous pouvez alors modifier l'alarme si nécessaire.

4. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell gérés, cliquez sur **Restaurer les alarmes par défaut**.
   Cette étape peut prendre jusqu'à une minute avant que le changement soit appliqué. Par ailleurs, elle est uniquement disponible si **Activer les alarmes d'hôtes Dell EMC** est sélectionné.
5. Dans **Niveau de publication d'événement**, sélectionnez soit « Ne pas publier d'événements », « Publier tous les événements », « Publier uniquement les événements de type Critique et Avertissement » ou « Publier uniquement les événements de type Critique et Avertissement concernant la virtualisation ». Pour plus d'informations, voir la section sur la **surveillance des événements, des alarmes et de l'intégrité** dans *OpenManage Integration for VMware vCenter User's Guide* (Guide d'utilisation d'OpenManage Integration for VMware vCenter).
6. Pour appliquer ces paramètres à tous les vCenters, sélectionnez **Appliquer ces paramètres à tous les vCenters**.

   **REMARQUE :** Si vous sélectionnez cette option, tous les paramètres existants pour tous les vCenters sont ignorés.

   **REMARQUE :** Cette option n'est pas disponible si vous avez déjà sélectionné **Tous les vCenters enregistrés** dans la liste déroulante dans l'onglet **Paramètres**.

7. Pour enregistrer les valeurs, cliquez sur **Appliquer**.

## Affichage des planifications de récupération des données pour l'inventaire et la garantie

1. Dans OpenManage Integration for VMware vCenter, sous l'onglet **Gérer** > **Paramètres**, sous **Paramètres vCenter**, cliquez sur **Planification de récupération des données**.
   En cliquant sur Planification de récupération des données, vous développez l'affichage et les options de modification des données d'inventaire et de garantie apparaissent.
2. Cliquez sur l'icône  en regard de **Récupération des données d'inventaire** ou de **Récupération des données de garantie**.
   La boîte de dialogue **Récupération des données d'inventaire/de garantie** vous permet de consulter les informations suivantes pour la récupération des données d'inventaire ou de garantie :
   - L'option de récupération d'inventaire et/ou de garantie option est-elle activée ou désactivée ?

- Les jours de la semaine pour lesquels l'option est activée.
- L'heure pour laquelle l'option est activée.

3. Pour modifier les planifications de récupération des données, procédez comme suit :
   a. Sous **Données d'inventaire/de garantie**, cochez la case **Activer la récupération des données d'inventaire/de garantie**.
   b. Sous **Planification de récupération des données d'inventaire/de garantie**, sélectionnez les jours de la semaine d'exécution de votre tâche.
   c. Dans la zone de texte **Heure de récupération des données d'inventaire/de garantie**, saisissez l'heure locale de la tâche.

      Il peut être nécessaire de prendre en compte le décalage horaire entre la configuration d'une tâche et la mise en œuvre d'une tâche.
   d. Pour enregistrer les paramètres, cliquez sur **Appliquer**. Pour réinitialiser les paramètres, cliquez sur **Effacer**. Enfin, si vous souhaitez interrompre l'opération, cliquez sur **Annuler**.
4. Cliquez de nouveau sur **Planification de récupération des données** pour masquer les planifications d'inventaire et de garantie et afficher une seule ligne.

# Création d'un profil de châssis

Un profil de châssis est requis pour surveiller le châssis. Un profil d'identification du châssis peut être créé et associé à un ou plusieurs châssis.

Vous pouvez vous connecter à l'iDRAC et à l'hôte à l'aide des informations d'identification Active Directory.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.
3. Développez la section **Profils de référence**, puis cliquez sur l'onglet **Profils de châssis**.
4. Dans la page **Profils du châssis**, cliquez sur l'icône pour créer un **Nouveau profil de châssis**.
5. Dans la page **Assistant Profil du châssis**, procédez comme suit :

   Dans la section **Nom et références**, sous **Profil de châssis** :
   a. Dans la zone de texte **Nom de profil**, entrez le nom du profil.
   b. Dans la zone de texte **Description**, entrez une description (facultatif).

   Dans la section **Informations d'identification** :
   a. Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur doté de privilèges d'administrateur, lequel est généralement utilisé pour se connecter au contrôleur CMC (Chassis Management Controller).
   b. Dans le champ **Mot de passe**, entrez le mot de passe correspondant au nom d'utilisateur spécifié.
   c. Dans la zone de texte **Vérifier le mot de passe**, entrez le même mot de passe que vous avez saisi dans la zone de texte **Mot de passe**. Les mots de passe doivent correspondre.

   **REMARQUE :** Les informations d'identification peuvent être locales ou associées à un compte Active Directory Pour que vous puissiez utiliser les informations d'identification Active Directory avec un profil de châssis, il doit exister un compte d'utilisateur Active Directory dans Active Directory et le contrôleur de gestion du châssis doit être configuré pour l'authentification Active Directory.
6. Cliquez sur **Suivant**.

   La page **Sélectionner le châssis** qui s'affiche montre tous les châssis disponibles.

   **REMARQUE :** Les châssis ne sont détectés et associables au profil de châssis qu'après l'exécution réussie de l'inventaire d'un hôte modulaire présent sous ce châssis.
7. Pour sélectionner un châssis unique ou plusieurs châssis, cochez les cases correspondantes en regard de la colonne **Adresse IP/Nom d'hôte**.

   Si le châssis sélectionné fait déjà partie d'un autre profil, le message d'avertissement qui s'affiche indique que le châssis sélectionné est associé à un profil.

   Par exemple, vous disposez d'un profil **Test** associé au Châssis A. Si vous créez un autre profil **Test 1** et essayez d'associer le Châssis A au **Test 1**, un message d'avertissement s'affiche.
8. Cliquez sur **OK**.

   La page **Châssis associés** s'affiche.
9. Pour tester la connectivité du châssis, sélectionnez le châssis, puis cliquez sur l'icône afin de vérifier les informations d'identification. Le résultat est indiqué dans la colonne **Résultat du test** par la mention **Réussite** ou **Échec**.
10. Pour terminer l'opération, cliquez sur **Terminer**.

# 3

# Accès aux documents à partir du site de support Dell EMC

Vous pouvez accéder aux documents requis de l'une des façons suivantes :

- À l'aide des liens suivants :
  - Pour les documents sur la gestion des systèmes Enterprise Dell EMC, la gestion à distance des systèmes Enterprise Dell EMC et les solutions de virtualisation Dell EMC : Www.dell.com/esmmanuals
  - Pour les documents Dell EMC OpenManage : www.dell.com/openmanagemanuals
  - Pour les documents sur l'iDRAC : www.dell.com/idracmanuals
  - Pour les documents de gestion des systèmes Dell EMC OpenManage Connections Enterprise : www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les documents relatifs aux outils facilitant la maintenance Dell EMC : https://www.dell.com/serviceabilitytools
- Sur le 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 parmi les suivants :
     - **Analyses**
     - **Gestion des systèmes Client**
     - **Applications d'entreprise**
     - **Gestion des systèmes Enterprise**
     - **Mainframe**
     - **Systèmes d'exploitation**
     - **Solutions du secteur public**
     - **Outils de facilité de la gestion**
     - **Compatibilité**
     - **Utilitaires**
     - **Solutions de virtualisation**
  4. Pour afficher un document, cliquez sur le produit requis, puis sur la version requise.
- Avec les moteurs de recherche :
  - Saisissez le nom et la version du document dans la zone de recherche.

# 4

# Documentation connexe

Outre ce guide, les autres manuels sont disponibles sur `Dell.com/support`. Cliquez sur **Faites votre choix parmi tous les produits**, puis sur **Logiciel et sécurité** > **Solutions de virtualisation**. Cliquez sur **OpenManage Integration for VMware vCenter 4.2** pour accéder aux documents suivants :

- *OpenManage Integration for VMware vCenter Version 4.2 Web Client User's Guide (Guide d'utilisation d'OpenManage Integration for VMware vCenter pour client Web version 4.2)*
- *OpenManage Integration for VMware vCenter Version 4.2 Release notes (Notes de mise à jour d'OpenManage Integration for VMware vCenter version 4.2)*
- *OpenManage Integration for VMware vCenter Version 4.2 Compatibility Matrix (Tableau de compatibilité d'OpenManage Integration for VMware vCenter version 4.2)*

Les ressources techniques, y compris les livres blancs, sont disponibles à l'adresse **delltechcenter.com**. Sur la page d'accueil Wiki du TechCenter de Dell, cliquez sur **Gestion des systèmes** > **OpenManage Integration for VMware vCenter** pour accéder à ces articles.