

# **Guide d'installation d'OpenManage Integration pour VMware vCenter version 5.0**

## 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

<b>Chapitre 1: Introduction.....</b>	<b>5</b>
Gestion des licences d'OpenManage Integration for VMware vCenter.....	5
Achat d'une licence logicielle.....	6
Options suite au chargement de licences.....	6
Mise en application.....	7
Remarques importantes à titre de référence.....	7
La configuration matérielle requise.....	7
Configuration du mode de déploiement.....	8
Versions du BIOS et de l'iDRAC avec Lifecycle Controller.....	8
Fonctionnalités prises en charge sur les serveurs PowerEdge.....	11
Fonctionnalités prises en charge sur le châssis PowerEdge.....	12
Espace de stockage obligatoire pour le stockage provisionné.....	12
Configuration logicielle requise.....	12
Exigences d'OpenManage Integration for VMware vCenter.....	12
Informations sur les ports.....	13
Liste de contrôle des prérequis.....	15
<b>Chapitre 2: Installation et configuration de l'OMIVV.....</b>	<b>17</b>
Téléchargement d'OpenManage Integration for VMware vCenter.....	17
Déploiement de l'OVF OMIVV à l'aide du client vSphere (HTML-5).....	18
Configuration de l'appliance OMIVV.....	19
Configuration des serveurs NTP (Network Time Protocol).....	22
Configuration de l'appliance OMIVV avec deux adaptateurs réseau.....	23
Génération d'une requête de signature de certificat (CSR).....	26
Chargement d'un certificat HTTPS.....	27
Restauration du certificat HTTPS par défaut.....	27
Enregistrement d'OpenManage Integration for VMware vCenter et importation du fichier de licence.....	27
Enregistrement d'un serveur vCenter par un utilisateur non-administrateur.....	30
Privilèges requis pour les utilisateurs non administrateurs.....	30
Attribution de privilèges Dell à un rôle existant.....	31
Reconfiguration d'OMIVV après la mise à niveau d'une version vCenter enregistrée.....	32
Vérification de l'installation.....	32
Gestion des sauvegardes et restaurations.....	32
Configuration des sauvegardes et restaurations.....	32
Planification des sauvegardes automatiques.....	33
Exécution d'une sauvegarde immédiate.....	33
Restauration de la base de données OMIVV à partir d'une sauvegarde.....	33
Réinitialisation des paramètres de sauvegarde et de restauration.....	34
Mise à jour de l'appliance OMIVV et de l'emplacement de la logithèque.....	34
Mise à niveau de l'appliance OMIVV à l'aide de RPM.....	35
Mise à niveau des outils VMware.....	35
Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations.....	35
Annulation de l'enregistrement de Dell OpenManage Integration for VMware vCenter.....	36
Restauration d'OMIVV après le désenregistrement.....	37

Récupération d'OMIVV après le désenregistrement d'une version antérieure d'OMIVV.....	37
Gestion du désenregistrement et du réenregistrement.....	37
<b>Chapitre 3: Configuration de l'appliance pour VMware vCenter.....</b>	<b>38</b>
Tâches de configuration à l'aide de l'Assistant Configuration initiale.....	38
Configuration initiale.....	38
Création du profil d'identification d'hôte.....	39
Planification d'une tâche d'inventaire.....	41
Planification des tâches de récupération de la garantie.....	41
Configuration des événements et alarmes.....	42
Tâches de configuration sur la page Paramètres.....	42
Configuration des notifications d'expiration de la garantie.....	42
Configuration de la notification relative à la dernière version de l'appliance.....	43
Configuration des informations d'identification de déploiement.....	43
Remplacement de la gravité des notifications de mise à jour de l'intégrité.....	43
<b>Chapitre 4: Accès aux documents à partir du site de support Dell EMC.....</b>	<b>45</b>
<b>Chapitre 5: Documentation connexe.....</b>	<b>46</b>

# 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. Une fois OMIVV installé, pour obtenir plus d'informations sur tous les aspects relatifs à l'administration, notamment la gestion d'inventaire, la surveillance et les alertes, les mises à jour du firmware et la gestion de la garantie, voir le guide *Guide d'utilisation d'OpenManage Integration for VMware vCenter* disponible à l'adresse [Dell.com/support/manuals](http://Dell.com/support/manuals).

## Sujets :

- [Gestion des licences d'OpenManage Integration for VMware vCenter](#)
- [Remarques importantes à titre de référence](#)
- [La configuration matérielle requise](#)
- [Configuration logicielle requise](#)
- [Informations sur les ports](#)
- [Liste de contrôle des prérequis](#)

## 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 est mise sous tension pour la première fois, une licence d'évaluation est installée automatiquement. La version d'essai contient une licence d'évaluation pour cinq hôtes (serveurs) gérés par OpenManage Integration for VMware vCenter. Cette version d'évaluation de 90 jours est la licence par défaut fournie lors de l'expédition.
- Licence standard : vous pouvez acheter n'importe quel nombre de licences hôtes gérées par OMIVV. Cette licence inclut un support produit et des mises à jour de l'appliance OMIVV.

OMIVV prend en charge jusqu'à 15 vCenters. 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 15 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 de serveurs) répertoriés.
- 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.

**REMARQUE :** Toute licence achetée pour OpenManage Integration for VMware vCenter et étant toujours valide (3 ans ou 5 ans à compter de la date de l'achat) peut être utilisée avec la version 5.x. Les licences sauvegardées à partir d'une instance OMIVV existante sont transférées, ou les licences en cours téléchargées à nouveau sur le portail Digital Locker peuvent être appliquées sur des instances utilisant la version 5.x.

Lorsque vous achetez une licence, le fichier .XML (clé de licence) est téléchargeable via Dell Digital Locker sur [Dell Digital Locker](#). Si vous ne parvenez pas à télécharger vos clés de licence, contactez le service de support Dell en vous rendant sur [Support de commande](#) pour trouver le numéro de téléphone du service de support Dell de votre zone géographique pour votre produit.

## Achat d'une licence logicielle

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

1. Accédez à **ParamètresLicencesAcheter une licence**, ou **Tableau de bordAcheter une licence**, ou **Portail administrateurInscription vCenterLicenceACHETER MAINTENANT**.
2. Téléchargez et enregistrez le fichier de licence à un emplacement connu.  
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).

## Chargement d'une licence sur le portail d'administration

Vous pouvez utiliser cette option pour télécharger la licence de l'hôte OMIVV.

1. Accédez à `https://<ApplianceIP/hostname/>`.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe.
3. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**.  
Les serveurs vCenter enregistrés s'affichent dans le volet de travail.
4. Cliquez sur **Charger la licence**.
5. Dans la boîte de dialogue **CHARGER LA LICENCE**, cliquez sur **Parcourir** pour accéder au fichier de licence, puis cliquez sur **Charger**.

Si le fichier de licence est modifié, l'appliance OMIVV le considère comme corrompu, et il ne fonctionnera pas.

## 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 sur [Dell Digital Locker](#). 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

L'OMIVV peut empiler plusieurs licences standard pour augmenter le nombre d'hôtes pris en charge à la somme des hôtes présents dans les licences chargées. Une licence d'évaluation ne peut pas être empilée. Par défaut, OMIVV prend en charge jusqu'à 15 instances vCenter. Si vous souhaitez gérer plus de 15 instances vCenter, utilisez plusieurs appliances.

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 leur chargement, certaines fonctionnalités peuvent ne pas fonctionner. Toutefois, les mises à niveau vers les nouvelles versions des OMIVV sont 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. Pour pouvoir mettre à niveau l'appliance, chargez une nouvelle licence.

### Licence d'évaluation

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

### Ajout d'hôtes à un profil d'identification d'hôte

Lorsque vous tentez d'ajouter un hôte à un profil d'identification d'hôte, si le nombre d'hôtes sous licence dépasse le nombre de licences, l'ajout d'hôtes supplémentaires n'est pas autorisé. OMIVV ne prend pas en charge la gestion d'un nombre d'hôtes supérieur au nombre de licences d'hôte disponibles.

## Remarques importantes à titre de référence

- À partir d'OMIVV 5.0 et versions ultérieures, seul le client VMware vSphere (HTML-5) est pris en charge, pas le client Web vSphere (FLEX).
- Pour utiliser le 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, Dell EMC vous recommande 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 6.5 et appliance du contrôleur de services de plateforme](#)
- [Exigences DNS pour vSphere 6.7 et appliance du contrôleur de services sur Windows](#)
- 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 plus d'informations, voir [Configuration du mode de déploiement](#) , page 8.
- Configuration de votre réseau pour répondre aux exigences en matière de port. Pour plus d'informations, voir [Informations sur les ports](#) , page 13.
- Dell EMC recommande d'utiliser Google Chrome pour accéder aux fonctionnalités OMIVV. OMIVV prend en charge Google Chrome et Mozilla Firefox. Microsoft Internet Explorer n'est pas pris en charge.

## 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. 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 \(tant pour le déploiement que la gestion\)](#)
- [Mémoire, processeur et espace de stockage pris en charge pour OMIVV](#)

OMIVV nécessite le réseau LAN sur une carte mère ou une carte fille réseau pouvant accéder au réseau de gestion iDRAC et CMC, ou au réseau de gestion des systèmes OME-Modular et au réseau de gestion de vCenter. Pour de plus amples informations, consultez [Configuration de l'appliance OMIVV](#) , page 19 et [Configuration de l'appliance OMIVV avec deux adaptateurs réseau](#) , page 23.

## Configuration du mode de déploiement

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

Assurez-vous que la configuration requise suivante est respectée pour les modes de déploiement requis, en affectant ces ressources ci-dessous à la machine virtuelle hébergeant OMIVV :

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

Modes de déploiement	Nombre d'hôtes	Nombre de processeurs	Mémoire (Go)	Stockage minimal
Petit	Jusqu'à 250	2	8	95 Go
Moyen	Jusqu'à 500	4	16	95 Go
Important	Jusqu'à 1000	8	32	95 Go
Mode Très grand	Jusqu'à 2 000	12	32	95 Go

**REMARQUE :** La fonctionnalité de mise à jour de firmware du châssis MX n'est prise en charge que pour les modes de déploiement moyen, grand et très grand.

Vous pouvez sélectionner un mode de déploiement approprié pour qu'OMIVV s'adapte au nombre de nœuds de votre environnement.

1. Sur la page **GESTION DE L'APPLIANCE**, faites défiler l'affichage vers le bas, jusqu'à **Mode de déploiement**. Les valeurs de configuration du mode de déploiement telles que **Petit**, **Moyen**, **Grand** et **Très grand** s'affichent. Par défaut, la valeur est définie sur **Petit**.
2. Pour modifier un mode de déploiement basé sur un environnement, cliquez sur **Modifier**.
3. Dans le mode **Modifier**, assurez-vous que les conditions préalables sont remplies et sélectionnez le mode de déploiement requis.
4. Cliquez sur **Appliquer**.  
Le processeur et la mémoire alloués sont vérifiés par rapport au processeur et à la mémoire requis pour le mode de déploiement défini et un ou plusieurs des événements suivants se produisent :
  - Si la vérification échoue, un message d'erreur est affiché.
  - Si la vérification aboutit, l'appliance OMIVV redémarre et le mode de déploiement est modifié dès que vous confirmez la modification.
  - Si le mode de déploiement requis est déjà défini, un message s'affiche.
5. En cas de modification du mode de déploiement, confirmez les modifications. Ensuite, l'appliance redémarre pour permettre la mise à jour du mode de déploiement.

**REMARQUE :** Pendant le démarrage de l'appliance OMIVV, les ressources système allouées sont vérifiées par rapport au mode de déploiement défini. Si ces ressources système allouées sont insuffisantes pour le mode de déploiement défini, l'appliance OMIVV ne démarre pas sur l'écran de connexion. Pour démarrer l'appliance OMIVV, fermez-la, mettez à jour les ressources système pour les adapter au mode de déploiement défini existant, puis effectuez la tâche [Rétrograder le mode de déploiement](#).

## Rétrogradation du mode de déploiement

1. Connectez-vous à la Console Administration.
2. Remplacez le mode de déploiement par le mode du niveau requis.
3. Mettez l'appliance OMIVV hors tension et modifiez les ressources système pour les définir sur le niveau requis.
4. Mettez l'appliance OMIVV sous tension.

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

Les versions suivantes du BIOS et de l'iDRAC avec Lifecycle Controller sont requises pour activer les fonctions d'OpenManage Integration for VMware vCenter.

Dell EMC vous recommande 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. Version du BIOS prise en charge pour les serveurs PowerEdge**

**Tableau 2. Version du BIOS prise en charge pour les serveurs PowerEdge**

<b>Serveur</b>	<b>Version minimale</b>
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
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
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
R240	1.0.0 ou version ultérieure
R340	1.0.0 ou version ultérieure
R940	1.0.0 ou version ultérieure

**Tableau 2. Version du BIOS prise en charge pour les serveurs PowerEdge**

Serveur	Version minimale
R940xa	1.0.0 ou version ultérieure
R740	1.0.0 ou version ultérieure
R740xd	1.0.0 ou version ultérieure
R740xd2	1.0.0 ou version ultérieure
R640	1.0.0 ou version ultérieure
R840	1.0.0 ou version ultérieure
R440	1.0.0 ou version ultérieure
M640	1.0.0 ou version ultérieure
T140	1.0.0 ou version ultérieure
T340	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
MX740C	1.0.0 ou version ultérieure
MX840C	1.0.0 ou version ultérieure
R6515	1.0.3 ou version ultérieure
R7515	1.0.3 ou version ultérieure
R6525	1.0.0 ou version ultérieure

**Tableau 3. iDRAC et Lifecycle Controller pris en charge pour le déploiement**

Génération	iDRAC avec Lifecycle Controller
Serveurs PowerEdge de 12e génération	2.50.50.50 ou version ultérieure
Serveurs PowerEdge de 13e génération	2.50.50.50 ou version ultérieure
Serveurs PowerEdge de 14e génération	3.00.00.00 et versions supérieures

**Tableau 4. Exigences du BIOS et de l'iDRAC pour le serveur cloud**

Modèle	BIOS	iDRAC avec Lifecycle Controller
C6320	1.0.2	2.50.50.50 ou version ultérieure
C4130	1.0.2	2.50.50.50 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
C6525	1.0.0 ou version ultérieure	3.42.42.42 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 5. Fonctionnalités prises en charge sur les serveurs PowerEdge**

Fonctionnalités	Plate-forme	
	12G et 13G	14G
Inventaire du matériel	O	O
Événements et alarmes	O (SNMP v1 et v2)	O (SNMP v1 et v2)
Surveillance de l'intégrité au niveau des composants*	O	O
Mises à jour du BIOS/Micrologiciel#	O	O
Proactive HA\$	O	O
Informations sur la garantie	O	O
Gestion de la conformité	O	O
Conformité de la configuration	O	O
Détection manuelle/automatique de serveur sans système d'exploitation	O	O
Conformité Bare-Metal	O	O
Configuration matérielle	O	O
Déploiement du SE	O	O
Faire clignoter le voyant LED du serveur	O	O
Afficher/Effacer les journaux d'événements système (SEL)	O	O
Lien et lancement d'iDRAC	O	O
Réinitialisation d'iDRAC	O	O
Mode de verrouillage du système	N	O
Profil système	O	O
Profil de cluster	O	O
Gestion d'hôte à l'aide de l'IP unifiée du châssis	N	O@
Prise en charge du serveur OEM	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.

@ Applicable uniquement pour un hôte de châssis MX. Les fonctions de mise à jour d'inventaire, de surveillance, de haute disponibilité proactive et de micrologiciel sont prises en charge.

~ Pris en charge uniquement pour les serveurs rack.

## Fonctionnalités prises en charge sur le châssis PowerEdge

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

**Tableau 6. Fonctionnalités prises en charge sur une infrastructure modulaire**

Fonctionnalités	M1000e	VRTX	FX2s	MX
Alertes SNMP	Y	Y	Y	Y
Inventaire du matériel	Y	Y	Y	Y
Lier et lancer CMC ou le module de gestion	Y	Y	Y	Y
Informations sur la licence	S/O	Y	Y	Y
Informations sur la garantie	Y	Y	Y	Y
Rapport d'intégrité	Y	Y	Y	Y
Informations de relation de groupe de gestion de châssis multiple	N	N	N	Y
Mise à jour du micrologiciel	N	N	N	Y

## Espace de stockage obligatoire pour le stockage provisionné

L'appliance virtuelle OMIVV exige au minimum 95 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 deux CPU virtuels (mode de déploiement Petit).

## Configuration logicielle requise

Assurez-vous que l'environnement vSphere répond aux exigences de configuration matérielle de l'appliance virtuelle ainsi qu'aux exigences relatives à l'accès au port, à la synchronisation de l'horloge et au port d'écoute.

### Conditions pour le client VMware vSphere (HTML-5)

vCenter 6.5 et versions ultérieures

## 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 7. Versions ESXi prises en charge**

Version ESXi	Génération du serveur		
	YX2X	YX3X	YX4X
6,0 U3	O	O	N
6.5	O	O	N

**Tableau 7. Versions ESXi prises en charge**

Version ESXi	Génération du serveur		
6.5 U1	O	O	O
6,5 U2	O	O	O
6.5 U3	O	O	O
6.7	N	O	O
6.7 U1	N	O	O
6.7 U2	N	O	O
6,7 U3	N	O	O

**REMARQUE :** L'hôte PowerEdge MX est pris en charge uniquement lorsqu'il est utilisé avec ESXi 6.5 U2 et les versions supérieures.

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

**Tableau 8. Versions du serveur vCenter prises en charge**

Version vCenter	Prise en charge client
6,5 U2	O
6.5 U3	O
6,7	O
6.7 U1	O
6.7 U2	O
6,7 U3	O

OpenManage Integration for VMware vCenter version 5.0 prend en charge VMware vRealize Operations Manager (vROPS) version 2.0.

L'appliance OMIVV 5.0 prend en charge CentOS 7.6.1810.

## Informations sur les ports

Cette section répertorie toutes les exigences relatives aux ports pour configurer votre appliance virtuelle et les nœuds gérés.

**Tableau 9. Appliance virtuelle**

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
53	DNS	TCP	Aucun	Sortant	Appliance O MIVV vers serveur DNS	Client DNS	Connectivité au serveur DNS ou résolution des noms d'hôte.
80/443	HTTP/HTTPS	TCP	Aucun	Sortant	Appliance O MIVV vers Internet	Accès Dell Online Data	Connectivité à la garantie en ligne (Internet), au micrologiciel et aux dernières informations RPM.
80	HTTP	TCP	Aucun	Entrant	Serveur ESXi vers appliance OM IVV	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	Aucun	Entrant	iDRAC/ESXi vers appliance OM IVV	Agent SNMP (serveur)	Pour recevoir des traps SNMP à partir de nœuds gérés.

**Tableau 9. Appliance virtuelle**

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
443	HTTPS	TCP	128 bits	Entrant	Interface utilisateur O MIVV vers appliance OM IVV	Serveur HTTPS	Services Web offerts par OMIVV. Ces services Web sont consommés par le client vSphere et le portail d'administration Dell.
443	WS-MAN	TCP	128 bits	Entrée/Sortie	Appliance O MIVV vers/ depuis iDRAC	Communication iDRAC	Communications iDRAC et CMC ou OME-Modular utilisées pour gérer et surveiller les nœuds gérés.
445	SMB	TCP	128 bits	Sortant	Appliance O MIVV vers CIFS	Communication CIFS	Pour communiquer avec le partage Windows.
4433	HTTPS	TCP	128 bits	Entrant	iDRAC vers appliance OM IVV	Découverte automatique	Serveur de configuration utilisé pour la détection automatique de nœuds gérés.
2049	NFS	UDP/TCP	Aucun	Entrée/Sortie	Appliance O MIVV 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	Aucun	Entrée/Sortie	Appliance O MIVV vers NFS	Partage public	Ces ports doivent être maintenus ouverts pour exécuter les services statd, quotd, lockd et mountd par les protocoles V2 et V3 du serveur NFS.
11620	Agent SNMP	UDP	Aucun	Entrant	iDRAC vers appliance OM IVV	Agent SNMP (serveur)	Port utilisé pour recevoir les alertes SNMP standard à l'aide du port UDP:162. Les données provenant d'iDRAC et CMC ou d'OME-Modular sont reçues pour gérer et surveiller les nœuds gérés.
Défini par l'utilisateur	N'importe lequel	UDP/TCP	Aucun	Sortant	Appliance O MIVV vers serveur proxy	Proxy	Pour communiquer avec le serveur proxy.

**Tableau 10. Nœuds gérés (ESXi)**

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
162, 11620	SNMP	UDP	Aucun	Sortant	ESXi vers appliance OMIVV	Événements matériels	Traps SNMP asynchrones envoyés par ESXi. Ce port doit s'ouvrir à partir d'ESXi.
443	WS-MAN	TCP	128 bits	Entrant	Appliance OMIVV vers ESXi	Communication iDRAC	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.

**Tableau 11. Nœuds gérés (iDRAC ou CMC ou OME-Modular)**

**Tableau 11. Nœuds gérés (iDRAC ou CMC ou OME-Modular)**

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
443	WSMAN/ HTTPS, REST/ HTTPS	TCP	128 bits	Entrant	Appliance OMI VV pour iDRAC ou CMC ou OME-Modular	Communication iDRAC	Utilisé pour fournir des informations à la station de gestion et communiquer au châssis MX à l'aide des protocoles REST ou HTTPS. Ce port doit s'ouvrir à partir d'iDRAC et CMC ou d'OME-Modular.
4433	HTTPS	TCP	128 bits	Sortant	iDRAC vers appliance OMI VV	Découverte automatique	Pour la découverte automatique de l'iDRAC (nœuds gérés) dans la station de gestion.
2049	NFS	UDP	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.  Pour accéder aux configurations de l'iDRAC à partir de l'OMIVV. Utilisé dans le flux de déploiement.
4001 à 4004	NFS	UDP	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.  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

Avant de commencer 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 [Privilèges requis pour les utilisateurs non-administrateurs](#).
- Vous avez le mot de passe racine pour les systèmes hôtes ESXi ou les informations d'identification Active Directory dotées des droits d'administration sur l'hôte.
- Vous avez le nom d'utilisateur et le mot de passe associés à iDRAC Express ou Enterprise qui possèdent les droits d'administration sur l'iDRAC.
- Le serveur vCenter est en cours d'exécution.
- Vous déterminez l'emplacement du répertoire d'installation d'OMIVV.
- L'OMIVV et le serveur vCenter se trouvent sur le même réseau.
- Il existe un itinéraire entre les réseaux vCenter, OMIVV et iDRAC si vCenter, OMIVV et iDRAC sont connectés à différents réseaux. Cela s'applique uniquement si l'appliance OMIVV n'est pas configurée avec deux adaptateurs réseau.
- Assurez-vous que l'environnement VMware vSphere répond aux exigences de configuration matérielle de l'appliance virtuelle ainsi qu'aux exigences relatives à l'accès au port, à la synchronisation de l'horloge et au port d'écoute.

- 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.

# Installation et configuration de l'OMIVV

Assurez-vous que les exigences matérielles sont remplies et que vous exécutez l'instance VMware vCenter requise.

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](https://www.dell.com/support). Pour plus d'informations sur le téléchargement d'OMIVV, voir [Téléchargement d'OpenManage Integration for VMware vCenter](#), page 17.
2. Naviguez jusqu'à l'emplacement où vous avez téléchargé le fichier, puis extrayez son contenu.
3. À l'aide du client vSphere (HTML-5), déployez le fichier OVF (Open Virtualization Format) qui contient l'appliance OMIVV. Voir [Déploiement de l'OVF OMIVV](#).
4. Une fois le fichier OVF déployé, définissez le fuseau horaire, ainsi que la date et l'heure actuelles.
5. Chargez le fichier de licence. Pour plus d'informations sur les licences, voir [Chargement d'une licence sur le portail d'administration](#), page 6.
6. Définissez le mode de déploiement en fonction de vos besoins. Pour plus d'informations, voir [Configuration du mode de déploiement](#), page 8.
7. 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](#).
8. Pour configurer l'appliance, suivez l'**Assistant Configuration initiale**. Voir [Tâches de configuration via l'Assistant Configuration](#).

## Sujets :

- [Téléchargement d'OpenManage Integration for VMware vCenter](#)
- [Déploiement de l'OVF OMIVV à l'aide du client vSphere \(HTML-5\)](#)
- [Configuration de l'appliance OMIVV](#)
- [Configuration des serveurs NTP \(Network Time Protocol\)](#)
- [Configuration de l'appliance OMIVV avec deux adaptateurs réseau](#)
- [Génération d'une requête de signature de certificat \(CSR\)](#)
- [Chargement d'un certificat HTTPS](#)
- [Enregistrement d'OpenManage Integration for VMware vCenter et importation du fichier de licence](#)
- [Enregistrement d'un serveur vCenter par un utilisateur non-administrateur](#)
- [Reconfiguration d'OMIVV après la mise à niveau d'une version vCenter enregistrée](#)
- [Vérification de l'installation](#)
- [Gestion des sauvegardes et restaurations](#)
- [Mise à jour de l'appliance OMIVV et de l'emplacement de la logithèque](#)
- [Mise à niveau de l'appliance OMIVV à l'aide de RPM](#)
- [Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations](#)
- [Annulation de l'enregistrement de Dell OpenManage Integration for VMware vCenter](#)
- [Restauration d'OMIVV après le désenregistrement](#)

## Téléchargement d'OpenManage Integration for VMware vCenter

Conservez le numéro de série de votre serveur Dell EMC PowerEdge. Il est recommandé d'utiliser le numéro de série pour accéder à l'ensemble du support sur le site Web de support de Dell. Vous êtes ainsi assuré de télécharger la version appropriée du logiciel pour votre plate-forme.

Pour télécharger OMIVV :

1. Accédez à <https://www.dell.com/support>.
2. Effectuez l'une des actions suivantes :
  - Entrez le numéro de série de votre serveur Dell EMC PowerEdge, puis sélectionnez Rechercher.

- Sélectionnez **Parcourir tous les produits > Serveurs > PowerEdge**.
3. Sélectionnez le modèle de serveur PowerEdge approprié.
  4. Sur la page du support technique de votre serveur, sélectionnez **Pilotes et téléchargements**.
  5. Dans la liste **Système d'exploitation**, sélectionnez la version de VMware ESXi appropriée.
  6. Dans la liste **Catégorie**, sélectionnez **Gestion des systèmes**.  
La version prise en charge d'OMIVV s'affiche.
  7. Cliquez sur **Télécharger** ou cochez la case pour ajouter le logiciel à votre liste de téléchargement.

## Déploiement de l'OVF OMIVV à l'aide du client vSphere (HTML-5)

Vous devez télécharger et décompresser le fichier .zip du produit *DellEMC\_OpenManage\_Integration\_<numéro de version>.<numéro de build>.zip* à partir du site Web de support.

**REMARQUE :** Les tâches suivantes sont recommandées uniquement si vous utilisez le client vSphere (HTML-5). Si vous utilisez le client Web, les étapes peuvent varier.

1. Accédez à l'emplacement où vous avez téléchargé OMIVV, puis double-cliquez sur **DellEMC\_OpenManage\_Integration.exe** pour décompresser le fichier.  
Le système d'exploitation du client pris en charge pour l'extraction et l'exécution du fichier exe est Windows 7 SP1 et version ultérieure.  
Le système d'exploitation du client pris en charge pour l'extraction et l'exécution du fichier 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 VMware vSphere (HTML-5)**.
5. Dans le **client 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 page **Sélectionner un modèle OVF**, effectuez les opérations suivantes :
  - a. Pour télécharger le package OVF à partir d'Internet, sélectionnez l'**URL**.
  - b. Sélectionnez **Fichier local** et cliquez sur **Choisir les fichiers** si vous souhaitez sélectionner le package OVF depuis votre système local.
  - c. Cliquez sur **Suivant**.  
La fenêtre **Sélectionner un nom et un dossier** s'affiche.

**REMARQUE :** Si le package OVF est enregistré sur un partage réseau, le processus d'installation peut prendre entre 10 et 30 minutes. Pour une installation rapide, Dell EMC vous recommande d'héberger l'OVF sur un lecteur local.
7. Dans la fenêtre **Sélectionner un nom et un emplacement**, procédez comme suit :
  - a. Dans le champ **Nom de la machine virtuelle**, saisissez le nom du modèle. Le nom peut comprendre jusqu'à 80 caractères.
  - b. Dans la liste **Sélectionner un emplacement pour la machine virtuelle**, sélectionnez un emplacement pour le déploiement du modèle.
  - c. Cliquez sur **Suivant**.  
La fenêtre **Sélectionner des ressources de calcul** s'affiche.
8. Dans la liste **Sélectionner une ressource de calcul**, sélectionnez la ressource de calcul de destination, puis cliquez sur **Suivant**.  
La fenêtre **Afficher les détails** s'affiche avec les informations suivantes :
  - **Éditeur** : les données de l'éditeur
  - **Taille de téléchargement** : la taille réelle du modèle OVF en giga-octets
  - **Taille sur disque** : les informations sur les détails alloués statiquement et dynamiquement
9. Cliquez sur **Suivant**.  
La fenêtre **Sélectionner un espace de stockage** s'affiche.
10. Dans la fenêtre **Sélectionner un stockage**, procédez comme suit :
  - a. Dans la liste déroulante **Sélectionner 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.

c. Cliquez sur **Suivant**.

La fenêtre **Sélectionner des réseaux** affiche des informations sur les réseaux source et de destination.

11. Dans la fenêtre **Sélectionner des réseaux**, sélectionnez un réseau de destination pour chaque réseau source, puis cliquez sur **Suivant**.

Pour gérer les serveurs Dell EMC dans votre environnement vSphere, OMIVV doit disposer d'un accès à la fois au réseau vSphere (vCenter et réseau de gestion ESXi), ainsi qu'au réseau hors bande (iDRAC, CMC et Dell EMC OpenManage Enterprise Modular (OME-Modular)).

Si le réseau vSphere et le réseau hors bande sont gérés comme des réseaux isolés distincts dans votre environnement, OMIVV doit pouvoir accéder aux deux réseaux. Dans ce cas, l'appliance OMIVV doit être configurée avec deux adaptateurs réseau. Si le réseau hors bande est accessible à l'aide du réseau vSphere, ne configurez pas d'adaptateur réseau pour l'appliance OMIVV. Pour plus d'informations sur la configuration de deux adaptateurs, voir [Configuration de l'appliance OMIVV avec deux adaptateurs réseau](#), page 23.

- Réseau hors bande : réseau de gestion auquel un iDRAC, un CMC et un OME-Modular sont connectés.
- Réseau vSphere : réseau de gestion auquel sont connectés les hôtes ESXi, les vCenters et les PSC.

12. 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 s'exécute et affiche la fenêtre d'état d'achèvement dans laquelle vous pouvez suivre l'état de progression de la tâche.

13. Mettez la machine virtuelle sous tension.

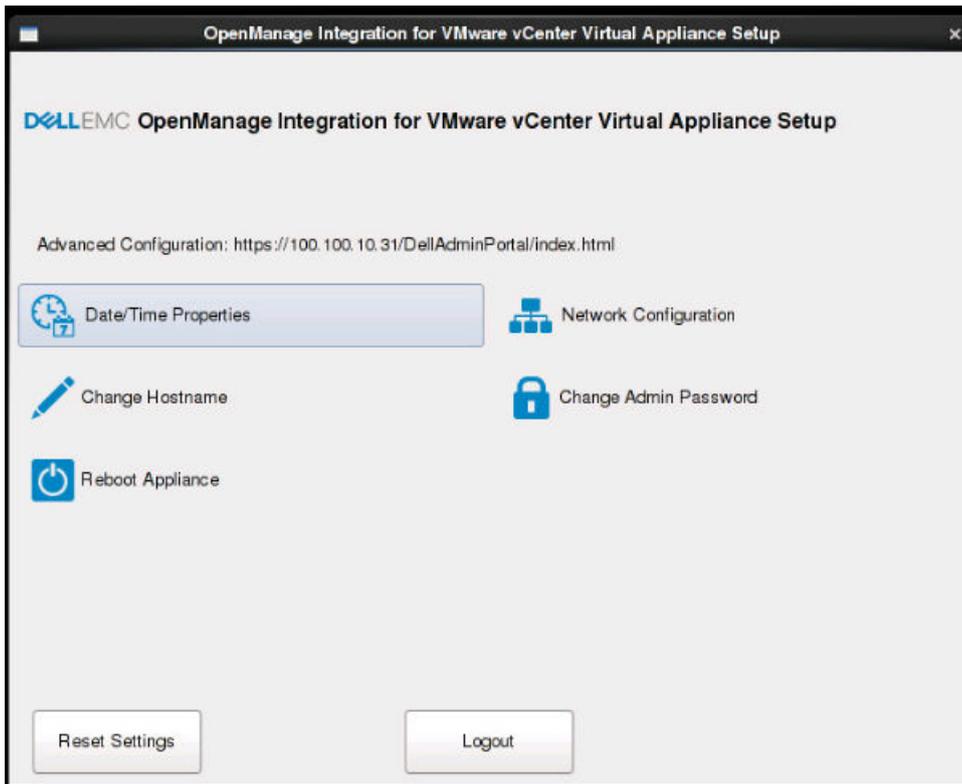
 **REMARQUE** : Une fois le fichier OVF déployé, vous devez obligatoirement définir la date et l'heure actuelles avant de vous enregistrer sur OMIVV.

## Configuration de l'appliance OMIVV

1. Mettez la machine virtuelle sous tension.
2. Dans le volet de droite, cliquez sur **Lancer la console Web**.
3. Connectez-vous en tant qu'administrateur (nom d'utilisateur par défaut : `admin`).
4. Si vous vous connectez pour la première fois, suivez les instructions qui s'affichent à l'écran pour définir le mot de passe (utilisateur administrateur et en lecture seule).

 **REMARQUE** : Si vous oubliez le mot de passe administrateur, il ne peut pas être récupéré à partir de l'appliance OpenManage Integration for VMware vCenter.

5. Pour configurer les informations de fuseau horaire d'OMIVV, cliquez sur **Propriétés Date/Heure**.



**REMARQUE :** Lorsque l'apppliance OMIVV n'est pas capable de récupérer une adresse IP du réseau (DHCP), 0 . 0 . 0 . 0 est l'adresse IP qui s'affiche. Pour résoudre ce problème, vous devez configurer manuellement l'IP statique.

- a. Sous l'onglet **Date et heure**, cochez la case **Synchroniser la date et l'heure sur le réseau**. La case à cocher **Synchroniser la date et l'heure sur le réseau** n'est activée qu'après configuration réussie du NTP à l'aide du portail d'administration. Pour plus d'informations sur la configuration du NTP, voir [Configuration des serveurs NTP \(Network Time Protocol\)](#) , page 22.
  - b. Cliquez sur **Fuseau horaire** et sélectionnez le fuseau horaire applicable, puis cliquez sur **OK**.
6. Pour configurer le réseau de l'apppliance OMIVV, cliquez sur **Configuration réseau**.

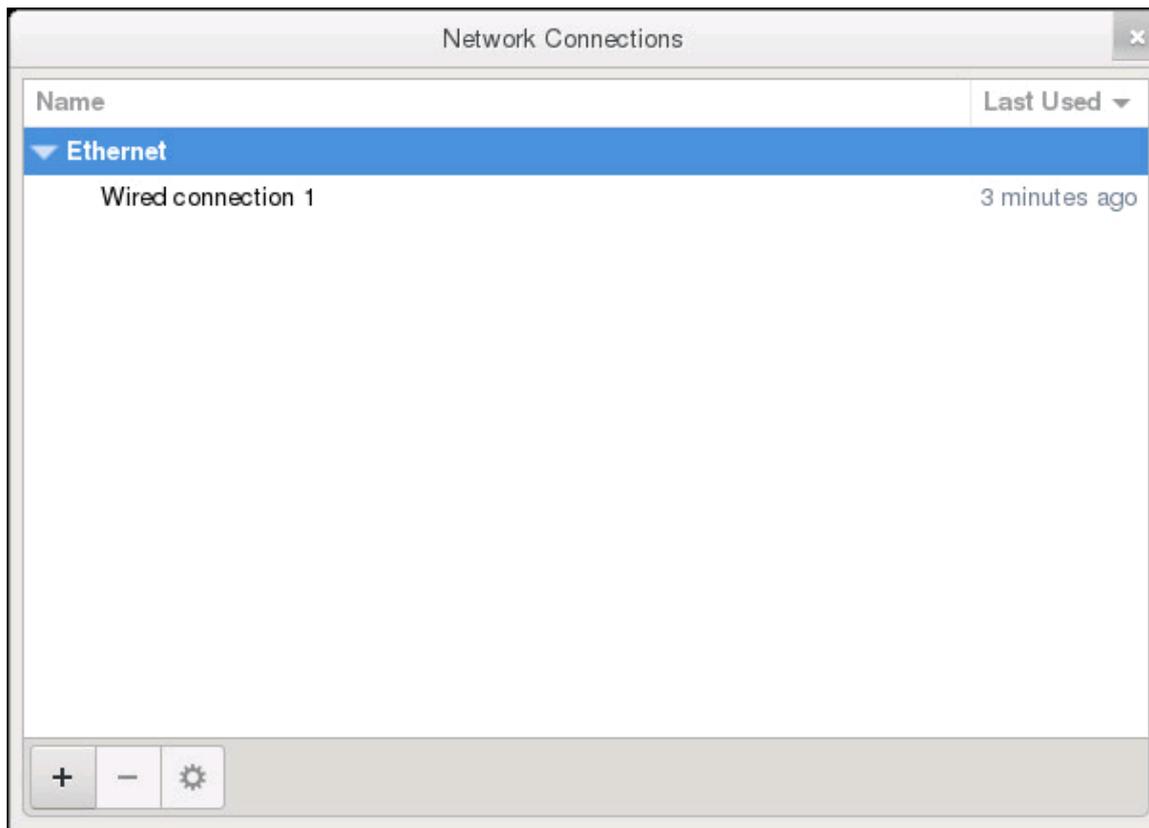
Pour gérer les serveurs Dell EMC dans votre environnement vSphere, OMIVV doit disposer d'un accès à la fois au réseau vSphere (vCenter et réseau de gestion ESXi), ainsi qu'au réseau hors bande (iDRAC, CMC et OME-Modular).

Si le réseau vSphere et le réseau hors bande sont gérés comme des réseaux isolés distincts dans votre environnement, OMIVV doit pouvoir accéder aux deux réseaux. Dans ce cas, l'apppliance OMIVV doit être configurée avec deux adaptateurs réseau. Dell EMC vous recommande de configurer les deux réseaux lors de la configuration initiale.

Si le réseau hors bande est accessible à l'aide du réseau vSphere, ne configurez pas deux adaptateurs réseau pour l'apppliance OMIVV. Pour plus d'informations sur la configuration d'une deuxième carte réseau, voir [Configuration de l'apppliance OMIVV avec deux adaptateurs réseau](#) , page 23.



7. Sélectionnez **Connexion filaire 1**, puis cliquez sur  .



- a. Cliquez sur l'onglet **Paramètres IPv4**, sélectionnez **Manuel** dans la liste déroulante **Méthode**, puis cliquez sur **Ajouter**.  
**i** **REMARQUE** : Si vous sélectionnez Automatique (DHCP), ne saisissez aucune adresse IP car l'appliance OMIVV recevra automatiquement l'adresse IP via le serveur DHCP lors du prochain redémarrage.
- b. Saisissez une adresse IP valide, un masque de réseau (au format CIDR (Classless Inter-Domain Routing)) et des informations de passerelle.  
Si vous saisissez une adresse IP dans le champ **Masque de réseau**, celle-ci est automatiquement convertie dans son format CIDR adapté.
- c. Saisissez l'adresse IP du serveur DNS et les domaines à rechercher dans les champs **Serveurs DNS** et **Domaines de recherche** respectivement.
- d. Cochez la case **Adressage IPv4 requis pour pouvoir établir cette connexion**, puis cliquez sur **Enregistrer**.

Editing Wired connection 1

Connection name:

General   Ethernet   802.1X Security   DCB   Proxy   **IPv4 Settings**   IPv6 Settings

Method:

**Addresses**

Address	Netmask	Gateway
100.100.9.102	22	100.100.8.1

Add  
Delete

DNS servers:

Search domains:

DHCP client ID:

Require IPv4 addressing for this connection to complete

Routes...

Cancel   Save

**REMARQUE :**

Parfois, après avoir configuré l'appliance OMIVV avec une adresse IP statique, la page de l'utilitaire de terminal OMIVV ne s'actualise pas et n'affiche pas immédiatement l'adresse IP actualisée. Pour résoudre ce problème, quittez l'utilitaire de terminal OMIVV, puis reconnectez-vous.

8. Pour modifier le nom d'hôte de l'appliance OMIVV, cliquez sur **Modifier le nom d'hôte**.

a. Saisissez un nom d'hôte valide et cliquez sur **Mettre à jour le nom d'hôte**.

**REMARQUE :** Si des serveurs vCenter sont déjà enregistrés avec l'appliance OMIVV, désenregistrez puis enregistrez de nouveau toutes les instances de vCenter. Pour plus d'informations, reportez-vous à la [Gestion du désenregistrement et du réenregistrement](#), page 37.

9. Redémarrez l'appliance.

## Configuration des serveurs NTP (Network Time Protocol)

Vous pouvez utiliser le protocole Network Time Protocol (NTP) pour synchroniser les horloges de l'appliance OMIVV avec celle d'un serveur NTP.

1. Sur la page **GESTION DE L'APPLIANCE**, cliquez sur **Modifier** dans la zone **Paramètres NTP**.
2. Sélectionnez **Activé**. Saisissez le nom d'hôte ou l'adresse IP d'un serveur NTP privilégié et secondaire, puis cliquez sur **Appliquer**.
3. Après avoir configuré NTP, démarrez la console du terminal et cochez la case **Synchroniser la date et l'heure sur le réseau**.

**REMARQUE :** La synchronisation des horloges d'OMIVV avec le serveur NTP dure environ 10 minutes.

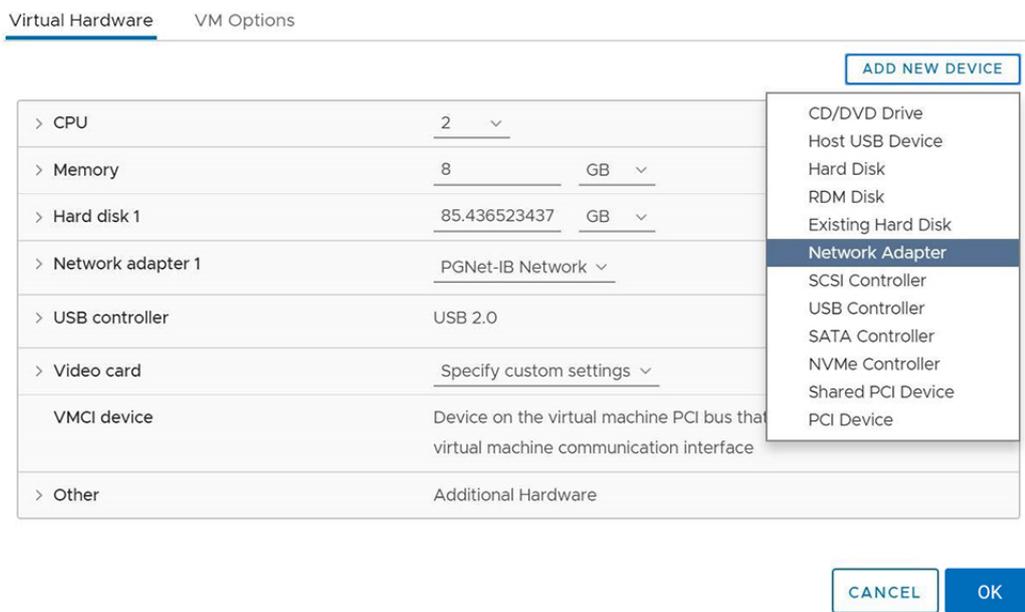
# Configuration de l'appliance OMIVV avec deux adaptateurs réseau

Pour gérer les serveurs Dell EMC dans votre environnement vSphere, OMIVV doit disposer d'un accès à la fois au réseau vSphere (vCenter et réseau de gestion ESXi), ainsi qu'au réseau hors bande (iDRAC, CMC et OME-Modular). Si le réseau vSphere et le réseau hors bande sont gérés comme des réseaux isolés distincts dans votre environnement, OMIVV doit pouvoir accéder aux deux réseaux. Dans ce cas, l'appliance OMIVV doit être configurée avec deux adaptateurs réseau. Si le réseau hors bande est accessible à l'aide du réseau vSphere, ne configurez pas deux adaptateurs réseau pour l'appliance OMIVV.

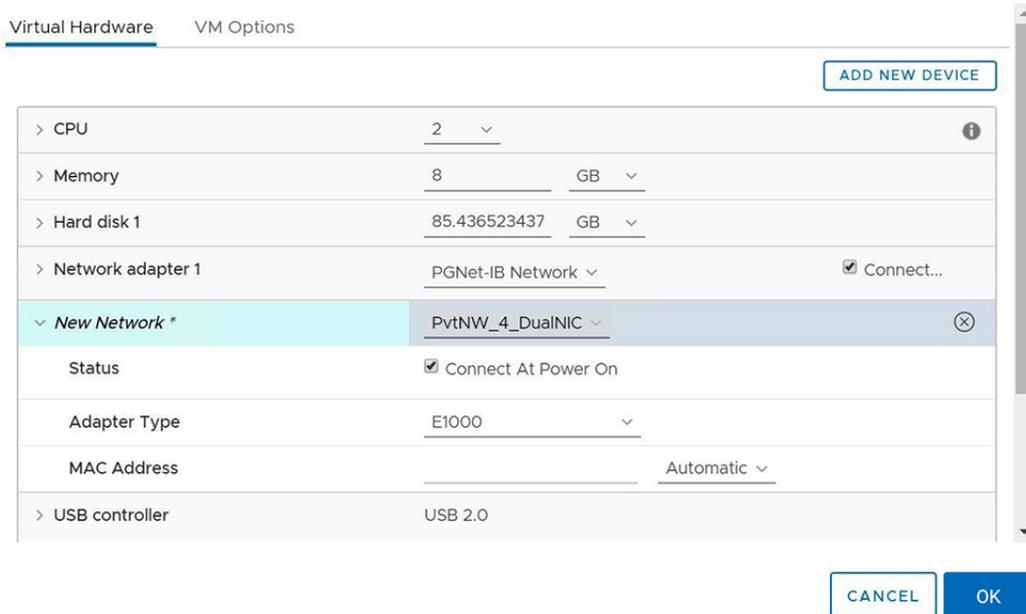
Assurez-vous que vous disposez des informations suivantes pour le réseau hors bande et le réseau vSphere :

- Adresse IP, masque réseau (au format CIDR) et passerelle de l'appliance (si statique)
- Passerelle par défaut : vous devez configurer la passerelle par défaut sur un seul réseau disposant d'une connexion Internet. Il est recommandé d'utiliser le réseau vSphere en tant que passerelle par défaut.
- Exigences de routage (IP réseau, masque de réseau et passerelle) : configurez les routes statiques pour les autres réseaux externes qui ne peuvent être atteints directement ou à l'aide de la passerelle par défaut.
- Exigences DNS : OMIVV prend en charge la configuration DNS pour un seul réseau. Pour plus d'informations sur la configuration DNS, passez à l'étape 9 (b) de cette rubrique.

1. Arrêtez l'appliance OMIVV.
2. Modifiez les paramètres de la machine virtuelle à l'aide du client vSphere (HTML-5) et ajoutez l'adaptateur réseau supplémentaire. Pour modifier les paramètres de la machine virtuelle, cliquez avec le bouton droit sur celle-ci, puis cliquez sur **Modifier les paramètres**.
3. Cliquez sur **AJOUTER UN NOUVEAU PÉRIPHÉRIQUE**, sélectionnez **Adaptateur réseau**.

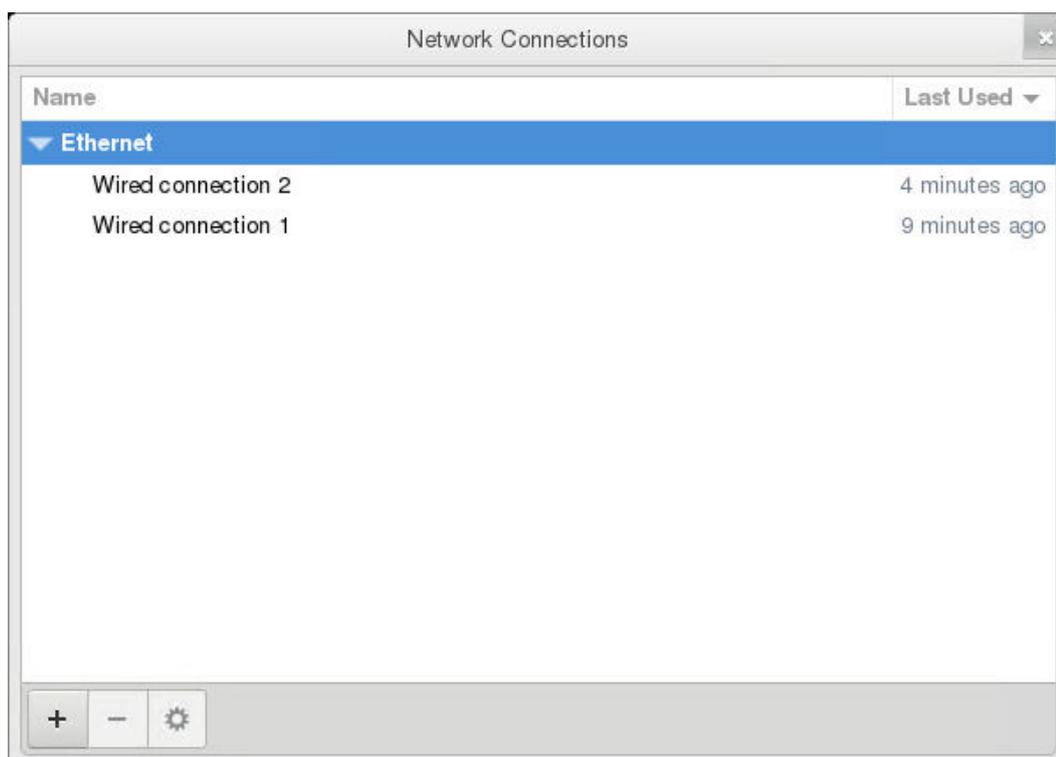


- a. Sélectionnez le réseau approprié pour l'adaptateur réseau, puis cochez la case **Connecter à la mise sous tension**.
- b. Sélectionnez l'adaptateur de type **E1000** dans le menu déroulant. OMIVV ne prend en charge que les adaptateurs réseau de type E1000.



4. Mettez la machine virtuelle sous tension. Connectez-vous en tant qu'administrateur (le nom d'utilisateur par défaut est Admin), puis appuyez sur **Entrée**.
5. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration for VMware vCenter**, cliquez sur **Configuration réseau**.

La page **Connexions réseau** affiche deux cartes réseau.



**⚠ AVERTISSEMENT : N'utilisez pas le signe « + » pour ajouter une nouvelle interface réseau. Vous devez utiliser les paramètres de modification de vSphere pour pouvoir ajouter une carte réseau.**



6. Sélectionnez la carte réseau que vous voulez configurer, puis cliquez sur .
7. Pour identifier la carte réseau appropriée, utilisez l'identifiant MAC affiché sous l'onglet **Ethernet**, puis comparez-le à l'identifiant MAC affiché dans le client vSphere (HTML-5).

Assurez-vous de ne pas modifier l'adresse MAC par défaut qui est indiquée sous l'onglet **Ethernet**.

8. Cliquez sur l'onglet **Général**, puis cochez la case **Se connecter automatiquement à ce réseau lorsqu'il est disponible**.
9. Cliquez sur l'onglet **Paramètres IPv4** et procédez comme suit :

Editing Wired connection 1

Connection name:

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method:

**Addresses**

Address	Netmask	Gateway
192.168.40.20	24	192.168.40.1

DNS servers:

Search domains:

DHCP client ID:

Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

- a. Sélectionnez **Manuel** ou **Automatique (DHCP)** à partir de la liste déroulante **Méthode**.
- b. Si vous sélectionnez la méthode **Manuel**, cliquez sur **Ajouter**, puis saisissez l'adresse IP valide, le masque de réseau (au format CIDR) et les détails de la passerelle. Il est recommandé d'utiliser l'IP statique si vous voulez contrôler la priorité des serveurs DNS (entrées DNS primaires et secondaires).

Généralement, les éléments vSphere du datacenter tels que vCenter et les hôtes ESXi sont gérés à l'aide du nom d'hôte ou du FQDN. iDRAC, CMC et OME-Modular sont gérés à l'aide d'adresses IP. Dans ce cas, Dell EMC vous recommande de configurer les paramètres DNS uniquement pour le réseau vSphere.

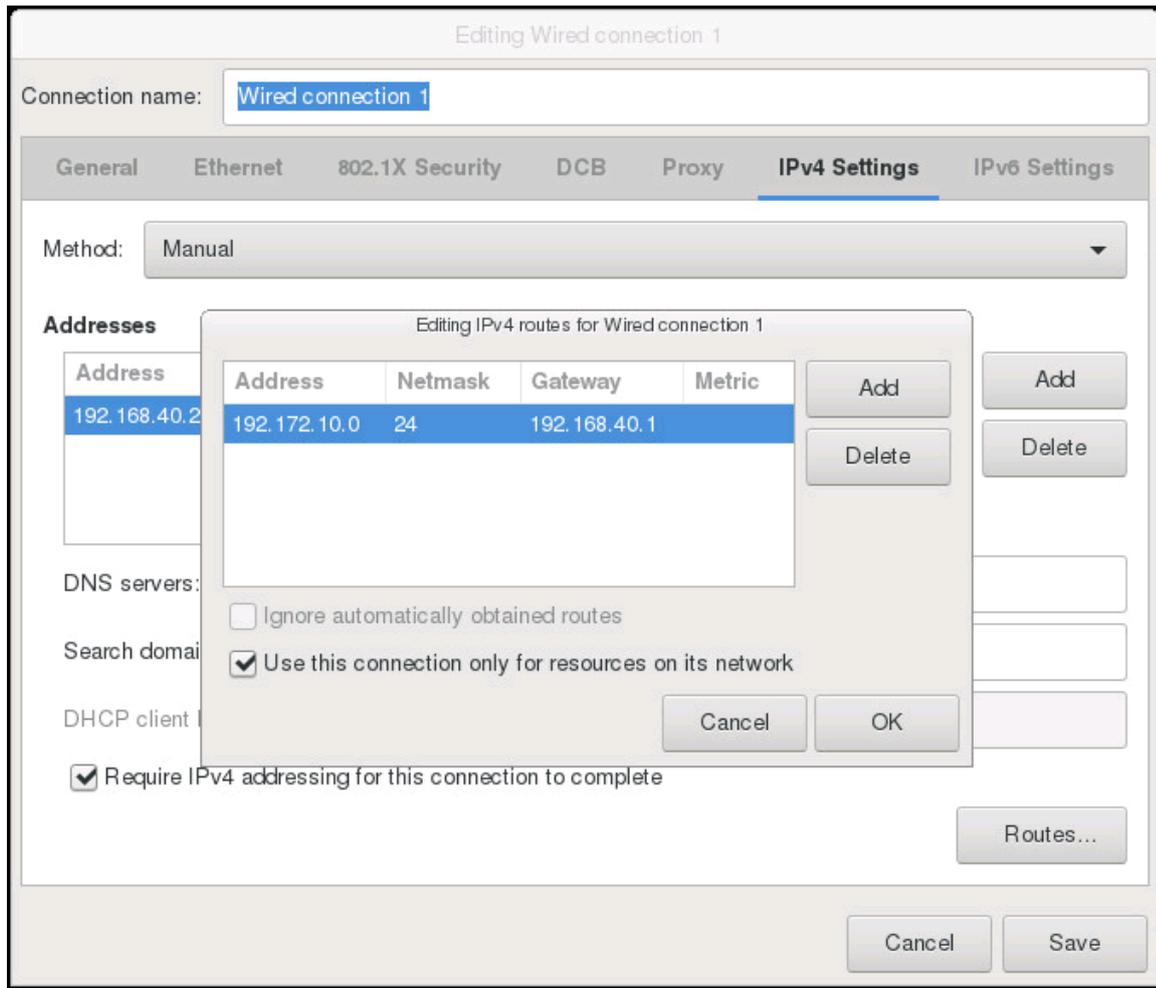
Si le réseau vSphere et le réseau de gestion iDRAC sont gérés à l'aide du nom d'hôte ou du FQDN, le serveur DNS doit être configuré de manière à résoudre le nom d'hôte ou le FQDN des deux réseaux. Pour plus d'informations, consultez la documentation CentOS.

**REMARQUE** : Le dernier serveur DNS configuré devient le DNS primaire quel que soit le réseau pour lequel le DNS est configuré.

- c. Saisissez l'adresse IP du serveur DNS et les domaines à rechercher dans les champs **Serveurs DNS** et **Domaines de recherche** respectivement.
- d. Cochez la case **Adressage IPv4 requis pour pouvoir établir cette connexion**, puis cliquez sur **ENREGISTRER**.
- e. Si vous ne voulez pas utiliser ce réseau comme réseau par défaut (passerelle), cliquez sur **Routes**, puis cochez la case **Utiliser cette connexion uniquement pour les ressources de son réseau**.

**REMARQUE** : L'ajout de plusieurs réseaux comme passerelles par défaut peut entraîner des problèmes de réseau et les fonctions OMIVV peuvent être affectées.

- f. Si vous souhaitez accéder à un réseau externe à l'aide des passerelles connues, cliquez sur **Ajouter** sur la même page, puis ajoutez l'adresse IP du réseau, le masque réseau (au format CIDR) et les détails de la passerelle.



En règle générale, le réseau que vous avez configuré comme passerelle par défaut ne nécessite aucune configuration manuelle du routage car la passerelle est capable de fournir l'accessibilité. Toutefois, pour les réseaux pour lesquels la passerelle par défaut n'est pas configurée (la case **Utiliser cette connexion uniquement pour les ressources de son réseau** est cochée), une configuration manuelle du routage peut être nécessaire. Puisque la passerelle par défaut n'est pas configurée pour que ce réseau atteigne les réseaux externes, des configurations de routage manuelles sont nécessaires.

**REMARQUE :** Une configuration de routage incorrecte peut brusquement empêcher l'interface réseau de répondre. Assurez-vous de configurer les entrées de routage de manière appropriée.

- g. Cliquez sur **OK**.
10. Cliquez sur Enregistrer. Pour configurer une autre carte réseau, répétez les tâches 6 à 10.
11. Accédez à l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration for VMware vCenter**, puis cliquez sur **Redémarrer l'appliance**. La configuration réseau n'est terminée qu'après le redémarrage de l'appliance OMIVV.

**REMARQUE :**

Après le redémarrage de l'appliance, les cartes réseau commencent à fonctionner comme configuré. L'état des cartes réseau peut être consulté en se connectant en tant qu'utilisateur **readonly**, et en exécutant les commandes suivantes : `ifconfig`, `ping` et `route -n`.

## Génération d'une requête de signature de certificat (CSR)

Avant d'enregistrer une appliance OMIVV dans un serveur vCenter, assurez-vous de télécharger la CSR.

La génération d'une nouvelle CSR empêche le chargement sur l'appliance des certificats créés avec la CSR générée antérieurement. Pour générer une CSR, procédez comme suit :

1. Sur la page **GESTION DE L'APPLIANCE**, cliquez sur **Générer une requête de signature de certificat** dans la zone **CERTIFICATS HTTPS**.  
Un message s'affiche indiquant que si une nouvelle requête est générée, les certificats créés à l'aide de la CSR précédente ne peuvent plus être chargés sur l'appliance. Pour poursuivre la requête, cliquez sur **Continuer**.
2. Si vous poursuivez la requête, dans la boîte de dialogue **GÉNÉRER UNE REQUÊTE DE SIGNATURE DE CERTIFICAT**, saisissez des informations sur le nom commun, l'organisation, la localité, l'état, le pays et l'adresse e-mail. Cliquez sur **Continuer**.
3. Cliquez sur **Télécharger**, puis sauvegardez la CSR résultant dans un emplacement accessible.

## 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 OMIVV et les systèmes hôtes. Pour configurer ce type de communications sécurisées, envoyez le certificat CSR à un signataire autorisé, puis téléchargez le certificat CSR résultant en utilisant la console d'administration. Il existe aussi un certificat par défaut qui est auto-signé et qui peut être utilisé pour sécuriser les communications. Ce certificat est unique à chaque installation.

1. Sur 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 charger le certificat, cliquez sur **Parcourir**, puis sur **Charger**.

**REMARQUE :** Si vous souhaitez charger un certificat CSR personnalisé vers OMIVV, assurez-vous de télécharger le nouveau certificat avant l'enregistrement de vCenter. Si vous chargez le nouveau certificat personnalisé après l'enregistrement dans vCenter, des erreurs de communication s'affichent dans le client vSphere (HTML-5). Pour résoudre ce problème, annulez l'enregistrement et recommencez l'enregistrement de l'appliance dans vCenter. Pour plus d'informations, reportez-vous à la [Gestion du désenregistrement et du réenregistrement](#), page 37.

Une fois que la tâche de téléchargement du certificat HTTPS est terminée, fermez la session de navigateur et accédez au portail d'administration dans une nouvelle session de navigateur.

## Restauration du certificat HTTPS par défaut

1. Sur 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**.

Une fois la tâche de restauration de certificat HTTPS par défaut terminée, fermez la session du navigateur en cours et accédez au portail d'administration dans une nouvelle session.

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

Assurez-vous que vos licences sont prêtes à être téléchargées sur [Dell Digital Locker](#). 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 [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 vSphere (HTML-5). Pour résoudre ce problème, annulez l'enregistrement et recommencez l'enregistrement de l'appliance dans vCenter. Pour plus d'informations, voir [Gestion du désenregistrement et du réenregistrement](#), page 37.

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

Pour ouvrir la **Console d'administration**, ouvrez un navigateur Web et saisissez `https://<IPAppliance ou Nom d'hôte de l'appliance ou FQDN>`.

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.

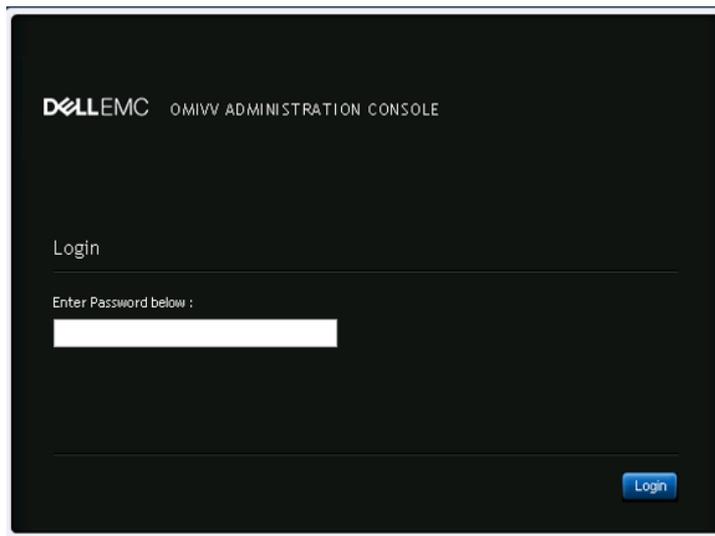


Figure 1. Console Administration

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

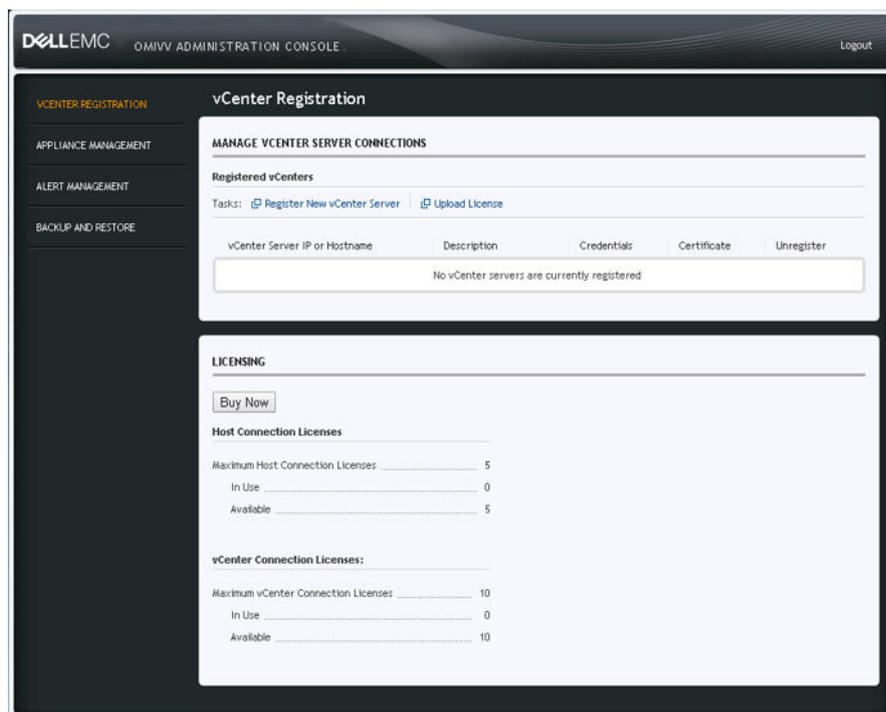


Figure 2. Fenêtre d'enregistrement vCenter provenant de la Console d'administration

3. Dans la fenêtre **Enregistrement vCenter**, cliquez sur **Enregistrer un nouveau serveur vCenter**.
4. 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**, saisissez l'adresse IP ou le FQDN du serveur, puis dans la zone de texte **Description**, saisissez 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. Pour plus d'informations, voir [Enregistrement d'un serveur vCenter par un utilisateur non-administrateur](#), page 30.

- c. Sous **Mot de passe**, saisissez le mot de passe.  
d. Dans **Vérifier le mot de passe**, entrez à nouveau le mot de passe.

5. Cliquez sur **S'inscrire**.

**REMARQUE :** OpenManage Integration for VMware vCenter prend actuellement en charge jusqu'à 2 000 hôtes pour un mode de déploiement extra large avec une seule instance vCenter ou plusieurs serveurs vCenter en utilisant le mode lié.

6. Effectuez l'une des actions suivantes :

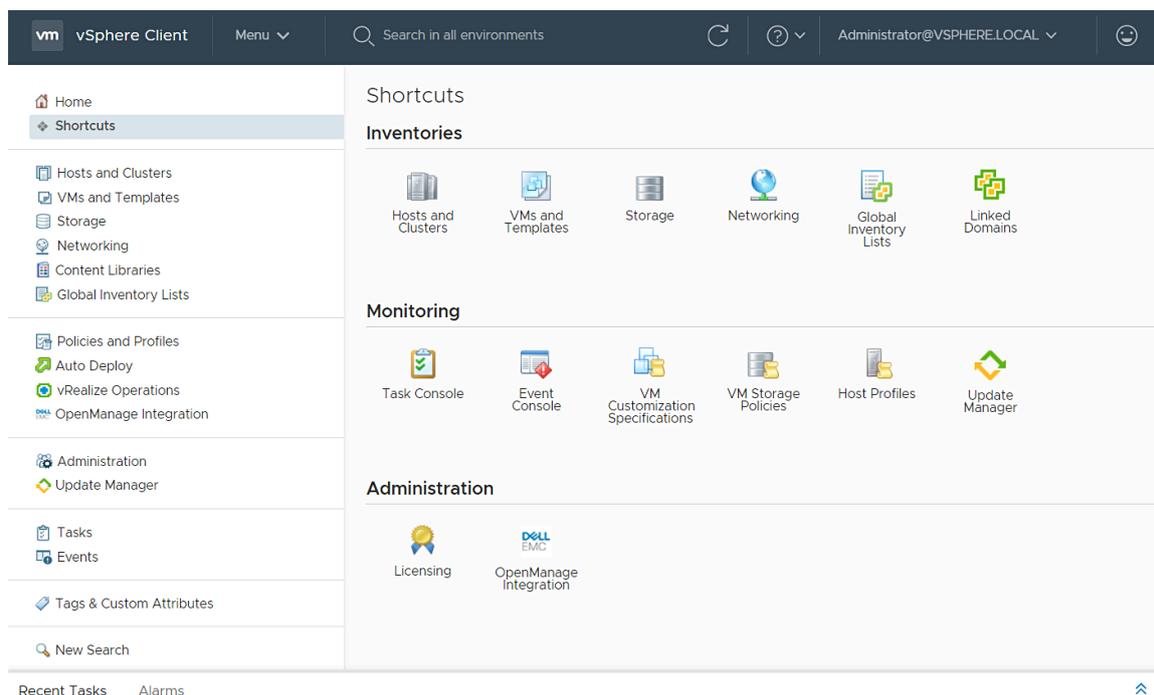
- Si vous utilisez la version d'essai d'OMIVV, vous pouvez afficher l'icône OMIVV.
- Si vous utilisez la version de produit intégrale, le fichier de licence peut être téléchargé à partir de Dell Digital Locker sur [Dell Digital Locker](#) et vous pouvez importer cette licence vers votre appliance virtuelle. Pour importer le fichier de licence, cliquez sur **Charger la licence**.

7. 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 vous rendant sur [Contact Technical Support](#) pour trouver le numéro de téléphone du service de support Dell de votre zone géographique pour votre produit.

Une fois l'OMIVV enregistré, l'icône OMIVV s'affiche sur la page d'accueil du client vSphere (HTML-5).

Pour vérifier l'installation, voir [Vérification de l'installation](#), page 32.



**Figure 3. 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.

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

Pour effectuer les tâches suivantes, assurez-vous que vous disposez des privilèges d'administrateur vCenter.

Vous pouvez enregistrer des vCenter Server 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 serveur vCenter, procédez comme suit :

1. Créez un rôle ou modifiez le rôle existant avec les privilèges obligatoires pour le rôle.  
Pour plus d'informations sur la liste des privilèges obligatoires pour le rôle, voir [Privilèges obligatoires pour les utilisateurs non-administrateurs](#).  
Pour connaître les étapes obligatoires à suivre pour créer ou modifier un rôle et sélectionner des privilèges dans le client vSphere (HTML-5), reportez-vous à la documentation de VMware vSphere.
2. Après avoir créé et défini un rôle, attribuez-lui un utilisateur et sélectionnez les privilèges correspondants.  
Pour plus d'informations sur l'attribution de privilèges à un rôle, reportez-vous à la documentation VMware vSphere.  
Un utilisateur non-administrateur du vCenter Server doté des privilèges requis peut alors enregistrer et/ou annuler l'enregistrement du vCenter Server, modifier les informations d'identification ou procéder à la mise à jour du certificat.
3. Enregistrez un serveur vCenter à l'aide d'un utilisateur non-administrateur disposant des privilèges requis.
4. Une fois l'enregistrement terminé, attribuez les privilèges Dell au rôle créé ou modifié à l'étape 1. Voir la section [Attribution de privilèges Dell à un rôle existant](#) , page 31.

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 :

Lorsqu'un utilisateur non-administrateur ne disposant pas des privilèges ci-dessous enregistre un serveur vCenter auprès d'OMIVV, un message 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
    - Modifier les paramètres
    - Connexion

- Maintenance
- Configuration réseau
- Demander un correctif
- Profil de sécurité et pare-feu



**REMARQUE :** Si vous utilisez vCenter 6.5 ou une mise à niveau vers vCenter 6.5 ou une version ultérieure, assurez-vous d'attribuer le privilège de modification du cluster.

- 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 :** Si vous utilisez vCenter 6.5 ou une mise à niveau vers vCenter 6.5 ou une version ultérieure, assurez-vous d'attribuer le privilège de modification du cluster.

- 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 serveur vCenter est enregistré à l'aide d'un utilisateur non administrateur pour accéder à des fonctionnalités OMIVV, l'utilisateur non-administrateur doit disposer des privilèges Dell. Pour en savoir plus sur l'affectation de privilèges Dell, voir [Attribution de privilèges Dell à un rôle existant](#), page 31.

## Attribution de privilèges Dell à un rôle existant

Si certaines pages d'OMIVV sont accessibles sans les privilèges Dell qui sont affectés à l'utilisateur connecté, l'erreur 2000000 s'affiche.

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

1. Connectez-vous au client vSphere (HTML-5) avec des droits d'administrateur.
2. Dans le client vSphere (HTML-5), développez **Menu**, puis cliquez sur **Administration** → **Rôles**.
3. Dans la liste déroulante **Fournisseur de rôles**, sélectionnez un serveur vCenter.
4. Dans la liste **Rôles**, sélectionnez **Dell-Operational**, puis cliquez sur **PRIVILÈGES**.
5. Pour attribuer les privilèges Dell, cliquez sur l'icône Modifier [✎]. La page **Modifier le rôle** s'affiche.
6. Dans le volet de gauche, cliquez sur **Dell**, sélectionnez les privilèges Dell suivants pour le rôle sélectionné, puis cliquez sur **SUIVANT** :
  - Dell.Configuration
  - Dell Deploy-Provisioning
  - Dell.Inventory
  - Dell.Monitoring
  - Dell.Reporting

Pour plus d'informations sur les rôles OMIVV disponibles au sein du vCenter, voir la section sur les rôles et les autorisations de sécurité du Guide d'utilisation.

7. Modifiez le nom du rôle et saisissez une description pour le rôle sélectionné, le cas échéant.
8. Cliquez sur **TERMINER**.  
Déconnectez-vous, puis connectez-vous depuis vCenter. L'utilisateur disposant des privilèges requis peut désormais effectuer les opérations OMIVV.

## Reconfiguration d'OMIVV après la mise à niveau d'une version vCenter enregistrée

Après la mise à niveau d'un vCenter enregistré, effectuez les tâches suivantes :

- Pour les utilisateurs non-administrateurs :
  1. Attribuez des privilèges supplémentaires aux utilisateurs non-administrateurs, si nécessaire. Voir la section [Privilèges requis pour les utilisateurs non administrateurs](#) , page 30.  
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 du client vSphere et démarrez un nouveau client vSphere (HTML-5).
2. 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.
3. Dans le client vSphere, développez **Menu**, puis cliquez sur **Administration** > **Solutions** > **Plug-ins du client**.  
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.
4. À la page **Plug-ins du client**, vérifiez la version et assurez-vous qu'OMIVV est installé et activé.  
Si l'OMIVV n'est pas activé, patientez quelques instants, puis déconnectez-vous et reconnectez-vous depuis vCenter.
5. Pour confirmer que l'icône OMIVV s'affiche dans le client vSphere (HTML-5), développez **Menu** dans le client vSphere. L'icône OpenManage Integration s'affiche.

## Gestion des sauvegardes et restaurations

La console d'administration vous permet d'effectuer des tâches de sauvegarde et de restauration.

- [Configuration des sauvegardes et restaurations](#)
- [Planification des sauvegardes automatiques](#)
- [Exécution d'une sauvegarde immédiate](#)
- [Restauration de la base de données à partir d'une sauvegarde](#)
- [Réinitialisation des paramètres de sauvegarde et de restauration](#) , page 34

Dans Dell OpenManage Integration for VMware vCenter, effectuez les étapes suivantes pour accéder à la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION** via la Console Administration :

1. Accédez à `https://<IPAppliance/nomhôte/>`.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe.
3. Dans le volet gauche, cliquez sur **SAUVEGARDE ET RESTAURATION**.

## Configuration des sauvegardes et restaurations

La fonction de sauvegarde et restauration sauvegarde la base de données OMIVV à un emplacement distant (NFS et CIFS) à partir duquel elle peut être restaurée à une date ultérieure. Les profils, la configuration et les informations sur l'hôte sont dans la sauvegarde. Dell EMC vous recommande de planifier des sauvegardes automatiques pour se prémunir contre la perte de données.

 **REMARQUE** : Les paramètres NTP ne sont pas sauvegardés et restaurés.

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Modifier**.
  2. Dans la zone en surbrillance **PARAMÈTRES ET DÉTAILS**, procédez comme suit :
    - a. Dans la zone de texte **Emplacement de sauvegarde**, saisissez le chemin d'accès aux fichiers de sauvegarde.
    - b. Dans la zone de texte **Nom d'utilisateur**, saisissez le nom de l'utilisateur.
    - c. Sous **Mot de passe**, saisissez le mot de passe. Le signe % n'est pas pris en charge à la fin du mot de passe.
    - d. Dans la zone de texte **Saisir le mot de passe utilisé pour crypter les sauvegardes**, saisissez le mot de passe chiffré dans la zone.

Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#\$\$%\* ».
    - e. Dans la zone de texte **Confirmer le mot de passe**, saisissez à nouveau le mot de passe crypté.
  3. Pour enregistrer ces paramètres, cliquez sur **Appliquer**.
  4. Configurez la planification des sauvegardes. Voir [Planification des sauvegardes automatiques](#).
- À l'issue de cette procédure, configurez une planification de sauvegarde.

## Planification des sauvegardes automatiques

Pour plus d'informations sur la configuration de l'emplacement de sauvegarde et des informations d'identification, reportez-vous à la section [Configuration des sauvegardes et restaurations](#).

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Modifier les sauvegardes automatiques planifiées**.

Les champs pertinents sont activés.
2. Pour activer les sauvegardes, cliquez sur **Activer**.
3. Cochez les cases **Jours de sauvegarde** correspondant aux jours de la semaine où vous voulez exécuter les tâches de sauvegarde.
4. Dans le champ **Heure de sauvegarde (24 heures, HH:mm)**, saisissez l'heure au format HH: mm.

Le champ **Prochaine sauvegarde** est renseigné avec la date et l'heure de la prochaine sauvegarde planifiée.
5. Cliquez sur **Appliquer**.

## Exécution d'une sauvegarde immédiate

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Sauvegarder maintenant**.
2. Pour utiliser l'emplacement et le mot de passe de cryptage des paramètres de sauvegarde, dans la boîte de dialogue **SAUVEGARDER MAINTENANT**, cochez la case **Utiliser l'emplacement et le mot de passe de cryptage des paramètres de sauvegarde**.
3. Entrez des valeurs pour l'**Emplacement de la sauvegarde**, le **Nom d'utilisateur**, le **Mot de passe** et le **Mot de passe de cryptage**.

Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#\$\$%\* ». Il n'existe aucune limite de caractères pour former un mot de passe.
4. Cliquez sur **Sauvegarder**.

## Restauration de la base de données OMIVV à partir d'une sauvegarde

Après avoir restauré OMIVV à partir d'une version précédente :

- Les serveurs 11G sans système d'exploitation ne sont pas pris en charge. Seuls les serveurs 12G et les générations ultérieures sont conservés après restauration.
- Les profils matériels et les modèles de déploiement ne sont pas pris en charge. Dell EMC vous recommande d'utiliser le profil système pour le déploiement.
- Les tâches de déploiement planifiées sur des serveurs 11G et/ou utilisant des modèles de déploiement basés sur les profils matériels sont annulées.
- Tous les serveurs 11G sont supprimés des profils d'identification et les licences consommées sont abandonnées.
- Les profils de logithèque n'utiliseront que des ensembles 64 bits.
-  **REMARQUE** : Si vous exécutez des sauvegardes et des restaurations depuis une version 4.x vers une 5.x, un symbole d'avertissement s'affiche en regard du nom du profil de cluster, car OMIVV ne prend pas en charge le lot de firmwares 32 bits dans les versions 5.x. Pour utiliser les dernières modifications apportées au profil de cluster, modifiez le profil de cluster.
- Les tâches de mise à jour du firmware planifiées sur les serveurs 11G sont annulées.

L'opération de restauration entraîne le redémarrage de l'apppliance OMIVV à la fin de la restauration.

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Restaurer maintenant**.
2. Dans la boîte de dialogue **RESTAURER MAINTENANT**, saisissez le chemin d'accès de l'**Emplacement du fichier** et du fichier .gz au format CIFS ou NFS.
3. Entrez un **Nom d'utilisateur**, un **Mot de passe** et un **Mot de passe de cryptage** pour le fichier de sauvegarde. Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#\$\$%\* ».
4. Pour enregistrer les modifications, cliquez sur **Appliquer**.  
L'apppliance est redémarrée. Pour vérifier l'installation, voir [Vérification de l'installation](#) , page 32. .

Une fois la restauration terminée, fermez le navigateur puis effacez son cache avant de vous connecter au portail d'administration.

## Réinitialisation des paramètres de sauvegarde et de restauration

À l'aide de la fonction de réinitialisation des paramètres, vous pouvez réinitialiser les paramètres sur l'état non configuré.

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Réinitialiser les paramètres**.
2. Dans la boîte de dialogue **Réinitialiser les paramètres**, cliquez sur **Appliquer**.  
L'apppliance est redémarrée.

## Mise à jour de l'apppliance OMIVV et de l'emplacement de la logithèque

- Pour garantir la protection de toutes les données, sauvegardez la base de données OMIVV avant de mettre à jour l'apppliance OMIVV. Voir la section [Gestion des sauvegardes et restaurations](#) , page 32.
- L'apppliance OMIVV nécessite une connexion Internet pour afficher les mécanismes de mise à niveau disponibles et effectuer la mise à niveau RPM. Assurez-vous que votre appliance OMIVV dispose d'une connexion Internet. Si vous avez besoin d'un réseau proxy, en fonction des paramètres réseau de l'environnement, activez les paramètres proxy et saisissez les données proxy. Voir la rubrique Configuration du proxy HTTP du Guide d'utilisation..
- Vérifiez que le **Chemin d'accès au référentiel de mise à jour** est valide.
- N'oubliez pas de vous déconnecter de toutes les sessions du client vSphere (HTML-5) avec les serveurs vCenter enregistrés.
- Avant de vous connecter à l'un des serveurs vCenter enregistrés, pensez à mettre simultanément à jour toutes les appliances appartenant au même contrôleur PSC (Platform Service Controller) avant de vous connecter à l'un des serveurs vCenter enregistrés. Sinon, vous êtes susceptible de voir des informations incohérentes sur les instances d'OMIVV.

1. Dans la section **MISE À JOUR DE L'APPLIANCE** de la page **GESTION DE L'APPLIANCE**, vérifiez les versions OMIVV actuelle et disponible.

Pour la version disponible de l'apppliance OMIVV, les mécanismes de mise à niveau des appliances RPM, OMIVV et OVF qui

conviennent sont accompagnés d'une coche [  ].

Vous trouverez ci-dessous les options de mécanisme de mise à niveau disponibles pour l'exécution de l'une ou l'autre des tâches de ce même mécanisme :

Option	Description
1	Si une coche s'affiche en regard de RPM, vous pouvez effectuer une mise à niveau RPM de la version existante à la dernière version disponible. Voir la section <a href="#">Mise à niveau de l'apppliance OMIVV à l'aide de RPM</a> , page 35.
2	Si une coche s'affiche en regard d'OVF, vous pouvez sauvegarder la base de données OMIVV depuis la version existante et la restaurer dans la dernière version d'apppliance disponible. Voir la section <a href="#">Mise à niveau de l'apppliance OMIVV à l'aide des sauvegardes et restaurations</a> , page 35.
3	Si une coche s'affiche en regard de RPM et OVF, vous pouvez effectuer l'une des tâches ci-dessus pour mettre à niveau votre appliance. Dans ce cas, la tâche recommandée est une mise à niveau RPM.

2. Pour mettre à jour l'apppliance OMIVV, exécutez les tâches ci-dessus pour les mécanismes de mise à niveau adéquats à partir de la version d'OMIVV.

# Mise à niveau de l'appliance OMIVV à l'aide de RPM

Assurez-vous que vous effectuez une mise à niveau vers une version de l'appliance qui est ultérieure à la version actuelle.

1. Sur la page **GESTION DE L'APPLIANCE**, en fonction de vos paramètres réseau, activez le proxy et saisissez les données de configuration du proxy, si nécessaire. Voir la rubrique .

Pour la version disponible de l'appliance OMIVV, les mécanismes de mise à niveau des appliances RPM, OMIVV et OVF qui conviennent sont accompagnés d'une coche [  ].

2. Pour mettre à niveau le plug-in OMIVV à partir d'une version existante vers la version disponible, effectuez l'une des opérations suivantes :
  - Pour effectuer une mise à niveau avec RPM, disponible dans **Chemin d'accès au référentiel de mise à jour**, assurez-vous que le chemin défini dans **Chemin d'accès au référentiel de mise à jour** est : <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>  
Si le chemin est différent, dans la fenêtre **Gestion de l'appliance**, dans la zone **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Modifier** pour mettre à jour le chemin d'accès vers <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> dans la zone de texte **Chemin d'accès au référentiel de mise à jour** et cliquez sur **Appliquer**.
3. Comparez la version de l'appliance OMIVV disponible avec la version actuelle.
4. Pour appliquer la mise à jour à l'appliance OMIVV, sous **Paramètres d'appliance**, cliquez sur **Mettre à jour l'appliance virtuelle**.
5. Dans la boîte de dialogue **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Mettre à jour**.  
En cliquant sur **Mettre à jour**, vous vous déconnectez de la fenêtre **CONSOLE ADMINISTRATION**.
6. Fermez le navigateur Web.  
Une fois que l'appliance est mise à niveau avec RPM, assurez-vous d'effacer le cache du navigateur avant de vous connecter au portail Administration Dell.

 **REMARQUE :** Au cours du processus de mise à niveau, l'appliance redémarre une ou deux fois.

 **REMARQUE :** Une fois la mise à niveau RPM terminée, vous pouvez afficher l'écran de connexion de la console OMIVV. Ouvrez un navigateur, saisissez le lien `https://<IPAppliance>/nomhôte`, puis accédez à la zone **MISE À JOUR DE L'APPLIANCE**. Vous pouvez vérifier si les versions de l'appliance OMIVV et de l'appliance disponible sont identiques. 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 la mise à niveau. Les mises à jour d'intégrité pour les hôtes Dell EMC ne sont pas disponibles tant que la mise à niveau n'est pas terminée.

## Mise à niveau des outils VMware

1. Effectuez un clic droit sur l'appliance OMIVV.
2. Placez le pointeur de la souris sur **Système d'exploitation invité**, puis cliquez sur **Installer/Mettre à niveau VMware Tools**.
3. Dans la boîte de dialogue **Installer/Mettre à niveau VMware Tools**, cliquez sur **Mise à jour automatique des outils**, puis sur **OK**.  
Vous pouvez afficher l'état de l'installation dans la section **Tâches récentes**.

## Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations

Dell EMC recommande de ne pas modifier ou supprimer un cluster ou un hôte géré par l'OMIVV après avoir effectué une sauvegarde et avant de restaurer le fichier de sauvegarde. Si le cluster ou l'hôte géré par l'OMIVV est modifié ou supprimé, reconfigurez les profils (par exemple le profil d'informations d'identification d'hôte ou le profil de cluster) associés à ces clusters et ces hôtes après la restauration.

N'annulez pas l'enregistrement du plug-in OMIVV sur le serveur vCenter. Le désenregistrement du plug-in depuis vCenter supprime le fournisseur de mise à jour d'intégrité Dell pour les clusters Proactive HA enregistrés sur vCenter par le plug-in OMIVV.

Pour mettre à jour l'appliance OMIVV depuis une version antérieure vers la version actuelle, effectuez les opérations suivantes :

1. Sauvegardez les données des versions antérieures.
2. Mettez l'ancienne appliance OMIVV hors tension depuis le vCenter.

3. Déployez la nouvelle appliance OVF OpenManage Integration.
4. Mettez la nouvelle appliance OpenManage Integration sous tension.
5. Configurez le réseau et le fuseau horaire de la nouvelle appliance.

**REMARQUE :** Dell EMC recommande de conserver l'identité (IP ou FQDN) de l'appliance OMIVV précédente pour la nouvelle appliance OMIVV.

**REMARQUE :** Si l'adresse IP de la nouvelle appliance est différente de l'adresse IP de l'ancienne appliance, la fonctionnalité Proactive HA peut ne pas fonctionner correctement. Dans un tel cas de figure, désactivez et activez la fonctionnalité Proactive HA pour chaque cluster sur lequel l'hôte Dell EMC est présent.

6. L'appliance OMIVV est livrée avec le certificat par défaut. Si vous souhaitez obtenir un certificat personnalisé pour votre appliance, mettez à jour les mêmes éléments. Reportez-vous aux sections [Génération d'une requête de signature de certificat \(CSR\)](#), page 26 et [Chargement d'un certificat HTTPS](#), page 27. Sinon, ignorez cette étape.
7. Restaurez la base de données sur la nouvelle appliance OMIVV. Voir [Restauration de la base de données OMIVV à partir d'une sauvegarde](#).
8. Vérifiez l'appliance. Pour plus d'informations, voir [Vérification de l'installation](#), page 32.
9. Après la mise à niveau, Dell EMC recommande d'exécuter à nouveau l'inventaire sur tous les hôtes gérés par le plug-in OMIVV. Les paramètres des événements et alarmes ne sont pas activés après la restauration de l'appliance. Vous pouvez réactiver les paramètres Événements et alarmes depuis l'onglet **Paramètres**.

Si vous effectuez une mise à niveau à partir d'une version antérieure d'OMIVV vers la version disponible, toutes les tâches planifiées continueront de s'exécuter.

**REMARQUE :** Si l'identité (IP ou FQDN) de la nouvelle version Y d'OMIVV est modifiée depuis la version X d'OMIVV, la destination des traps SNMP doit être configurée de sorte à pointer vers la nouvelle appliance. Pour les serveurs 12G et de générations ultérieures, ce problème est réglé en exécutant l'inventaire sur ces hôtes. Lors de l'exécution de l'inventaire sur les hôtes 12G, si des traps SNMP ne pointent pas vers la nouvelle adresse IP, ces hôtes sont répertoriés comme non conformes. Pour corriger les problèmes de conformité de l'hôte, voir la section Gestion de la conformité du Guide d'utilisation.

Après la sauvegarde et la restauration d'une version antérieure d'OMIVV par une version mise à jour, si vous constatez que le message 200000 s'affiche ou que le logo Dell EMC ne s'affiche pas, ou que l'interface utilisateur d'OMIVV ne répond pas sur l'interface utilisateur de vCenter, procédez comme suit :

- Redémarrez les services clients vSphere pour le client vSphere (HTML-5) et le client Web vSphere (FLEX) sur le serveur vCenter.
- Si le problème persiste :
  - Pour l'appliance VMware vCenter Server : accédez à `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`. Pour Windows vCenter, accédez aux dossiers suivants de l'appliance vCenter et vérifiez si les anciennes données correspondant aux anciennes versions existent :  
dossier C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity dans l'appliance vCenter.

Voici un exemple d'anciennes données : `com.dell.plugin.OpenManage—  
com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`.

- Supprimez manuellement le dossier correspondant à la version précédente d'OMIVV et redémarrez les services clients vSphere pour le client vSphere (HTML-5) et le client Web (FLEX).

## Annulation de l'enregistrement de Dell OpenManage Integration for VMware vCenter

Assurez-vous de ne pas annuler l'enregistrement d'OMIVV à partir du serveur vCenter lorsqu'une tâche d'inventaire, de garantie ou de déploiement est en cours d'exécution.

Si Proactive HA est activé sur des clusters, veillez à désactiver Proactive HA sur les clusters. Pour désactiver Proactive HA, accédez à l'écran **Proactive HA pannes et réponses** d'un cluster en sélectionnant **Configurer > Services > Disponibilité vSphere**, puis cliquez sur **Modifier**. Pour désactiver Proactive HA, sur l'écran **Échecs et réponses de Proactive HA**, désactivez la case située à côté du fournisseur **Dell Inc**.

Pour supprimer OpenManage Integration for VMware vCenter, annulez l'enregistrement d'OMIVV auprès du serveur vCenter à l'aide de la Console Administration.

1. Accédez à <https://<ApplianceIP/hostname/>>.
2. Sur la page **ENREGISTREMENT DE VCENTER**, puis dans le tableau **Nom d'hôte ou adresse IP du serveur vCenter**, cliquez sur **Annuler l'enregistrement**.  
**REMARQUE** : Assurez-vous de sélectionner le bon serveur vCenter car OMIVV peut être associé à plusieurs serveurs vCenter.
3. Pour confirmer l'annulation de l'enregistrement du serveur vCenter sélectionné, accédez à la boîte de dialogue **DÉSENREGISTRER UN VCENTER**, puis cliquez sur **Désenregistrer**.  
**REMARQUE** : Une fois le désenregistrement d'OMIVV effectué, déconnectez-vous, puis connectez-vous à partir du client vSphere (HTML-5). Si l'icône OMIVV est toujours visible, redémarrez les services clients pour le client vSphere (HTML-5) et le client Web (FLEX).

## Restauration d'OMIVV après le désenregistrement

### 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 qui ont été mises en œuvre sur les alarmes enregistrées et le fournisseur de mise à jour d'intégrité Dell pour le cluster PHA. Les étapes suivantes ne restaurent pas les personnalisations, mais elles enregistrent à nouveau les alarmes dans leur état par défaut.
- REMARQUE** : Dell EMC recommande de conserver l'identité (IP ou FQDN) de l'appliance OMIVV précédente pour la nouvelle appliance OMIVV.
- REMARQUE** : Si l'adresse IP de la nouvelle appliance est différente de l'adresse IP de l'ancienne appliance, la fonctionnalité Proactive HA peut ne pas fonctionner correctement. Dans un tel cas de figure, désactivez et activez la fonctionnalité PHA pour chaque cluster sur lequel l'hôte Dell est présent.

Exécutez les tâches 3 à 9 répertoriées dans [Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations](#) , page 35.

## Gestion du désenregistrement et du réenregistrement

Dell EMC recommande d'effectuer une sauvegarde avant de procéder au désenregistrement.

- REMARQUE** : Le désenregistrement du plug-in supprime toutes les personnalisations qui ont été mises en œuvre sur les alarmes enregistrées et le fournisseur de mise à jour d'intégrité Dell pour le cluster PHA. Les étapes suivantes ne restaurent pas les personnalisations, mais elles enregistrent à nouveau les alarmes dans leur état par défaut.

1. Effectuez une sauvegarde d'OMIVV.
2. Désenregistrez vCenter à partir d'OMIVV.
3. Exécutez toute modification de configuration planifiée. Par exemple, une modification du nom d'hôte ou une nouvelle modification de la configuration.
4. Redémarrez l'appliance OMIVV.
5. Restaurez le fichier de sauvegarde. Pour plus d'informations, voir [Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations](#) , page 35.

# Configuration de l'appliance pour VMware vCenter

Vous pouvez configurer l'appliance OMIVV à l'aide de l'une des méthodes suivantes :

- Avec l'**Assistant Configuration initiale**.

Une fois l'installation de base de l'OMIVV et l'enregistrement des vCenters terminés, l'Assistant Configuration initiale s'affiche automatiquement pour la première fois lorsque vous lancez l'OMIVV dans vCenter.

Si vous souhaitez lancer l'Assistant Configuration initiale ultérieurement, accédez à :

- **Paramètres > Assistant Configuration initiale > DÉMARRER L'ASSISTANT CONFIGURATION INITIALE**
- **Tableau de bord > Références rapides > DÉMARRER L'ASSISTANT CONFIGURATION INITIALE**

- Avec l'onglet **Paramètres**.

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

## Sujets :

- [Tâches de configuration à l'aide de l'Assistant Configuration initiale](#)
- [Tâches de configuration sur la page Paramètres](#)

## Tâches de configuration à l'aide de l'Assistant Configuration initiale

 **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 vSphere (HTML-5), puis reconnectez-vous.

À l'aide de l'Assistant Configuration initiale, vous pouvez afficher et effectuer les tâches suivantes :

- Sélection de vCenters
- Création du profil d'identification d'hôte. Pour plus d'informations, voir [Création du profil d'identification d'hôte](#) , page 39.
- Configuration des événements et alarmes. Pour plus d'informations, voir [Configuration des événements et alarmes](#) , page 42.
- Planification des tâches d'inventaire. Pour plus d'informations, voir [Planification d'une tâche d'inventaire](#) , page 41.
- Planification des tâches de récupération de la garantie. Pour plus d'informations, voir [Planification des tâches de récupération de la garantie](#) , page 41.

## Configuration initiale

Une fois l'installation de base de l'OMIVV et l'enregistrement des vCenters terminés, l'Assistant Configuration initiale s'affiche automatiquement pour la première fois lorsque vous lancez l'OMIVV dans vCenter.

Si vous souhaitez lancer l'Assistant Configuration initiale ultérieurement, accédez à :

- **Paramètres > Assistant Configuration initiale > DÉMARRER L'ASSISTANT CONFIGURATION INITIALE**
- **Tableau de bord > Références rapides > DÉMARRER L'ASSISTANT CONFIGURATION INITIALE**

1. Sur la page **Bienvenue**, lisez les instructions, puis cliquez sur **DÉMARRER**.
2. Sur la page **Sélectionner un vCenter**, dans le menu déroulant **vCenters**, sélectionnez un vCenter spécifique ou **Tous les vCenters enregistrés**, puis cliquez sur **SUIVANT**.

 **REMARQUE** : Si vous disposez de plusieurs serveurs vCenter faisant partie du même PSC et enregistrés avec la même appliance OMIVV, et si vous choisissez de configurer un seul serveur vCenter, l'étape 2 doit être répétée jusqu'à ce que chaque vCenter soit configuré.

3. Sur la page **Créer un profil d'identification d'hôte**, cliquez sur **CRÉER UN PROFIL D'IDENTIFICATION D'HÔTE**.  
Pour plus d'informations sur la création d'un profil d'identification d'hôte, voir [Création du profil d'identification d'hôte](#), page 39.  
  
Une fois les hôtes ajoutés au profil d'informations d'identification d'hôte, l'adresse IP d'OMIVV est automatiquement définie en tant que destination d'interruption SNMP pour l'iDRAC de l'hôte. 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 de trap SNMP échoue et/ou l'activation du service WBEM échoue pour certains hôtes, ceux-ci sont répertoriés comme non conformes. Pour afficher et corriger la non-conformité, voir la section Gestion de la conformité du Guide d'utilisation.
4. Sur la page **Configurer des paramètres supplémentaires**, procédez comme suit :
  - a. Planification des tâches d'inventaire. Pour plus d'informations sur la planification de la tâche d'inventaire, voir [Planification d'une tâche d'inventaire](#), page 41.
  - b. Planification des tâches de récupération de la garantie. Pour plus d'informations sur la planification de la tâche de récupération de la garantie, voir [Planification des tâches de récupération de la garantie](#), page 41.  
Si vous souhaitez modifier la planification de la tâche d'inventaire, accédez à **Paramètres > Paramètres vCenter > Planification de récupération des données > Récupération d'inventaire** ou **Tâches > Inventaire**.  
Si vous souhaitez modifier la planification de la tâche de récupération de la garantie, accédez à **Paramètres > Récupération de la garantie > Tâches > Garantie**.
  - c. Configuration des événements et alarmes. Pour plus d'informations sur la configuration des événements et alarmes, voir [Configuration des événements et alarmes](#), page 42.
  - d. Pour appliquer des paramètres individuels, cliquez sur le bouton **Appliquer** séparément, puis cliquez sur **SUIVANT**.  
Il est vivement recommandé d'activer tous les paramètres supplémentaires. Si l'un des paramètres supplémentaires n'est pas appliqué, un message s'affiche pour indiquer que tous les paramètres supplémentaires sont obligatoires.
5. Sur la page **Étapes suivantes**, lisez les instructions, puis cliquez sur **TERMINER**.  
Dell EMC recommande d'associer vos hôtes OMIVV à une ligne de base de configuration, car cela vous permet de surveiller étroitement les modifications de configuration qui se produisent dans les hôtes et les clusters associés. Une configuration de base peut être créée pour n'importe quel cluster une fois que les hôtes sont gérés avec succès par OMIVV. Pour créer une ligne de base de configuration, procédez comme suit :
  - Créez un profil de logithèque de firmware et de pilote : cela vous aide à définir des versions de firmware et de pilote sur ligne de base.
  - Créez un profil système : cela vous permet de définir des configurations matérielles sur ligne de base pour les hôtes.
  - Créez un profil de cluster : pour créer une ligne de base réussie, sélectionnez des clusters, puis associez le firmware, les pilotes et les configurations matérielles.
  - Les hôtes présents dans un châssis PowerEdge MX équipé d'un iDRAC IPv4 désactivé doivent être gérés à l'aide d'un profil d'identification de châssis.

## Création du profil d'identification d'hôte

Si le nombre d'hôtes ajoutés dépasse la limite définie par la licence pour créer un profil d'identification d'hôte, vous ne pouvez pas créer un profil de ce type.

Avant d'utiliser les informations d'identification Active Directory (AD) pour un profil d'identification d'hôte, assurez-vous que :

- Le compte d'utilisateur existe dans AD.
- Le contrôleur iDRAC ou l'hôte est configuré pour l'authentification basée sur Active Directory.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement > Profil d'identification d'hôte**.
2. Sur la page **Créer un profil d'identification d'hôte**, cliquez sur **CRÉER UN NOUVEAU PROFIL**.
3. Sur la page **Profil d'identification d'hôte**, lisez les instructions, puis cliquez sur **DÉMARRER**.
4. Sur la page **Nom et références**, effectuez les opérations suivantes :
  - a. Saisissez le nom et la description du profil. Il n'est pas obligatoire de renseigner le champ de description.
  - b. Dans la liste **Nom du vCenter**, sélectionnez une instance de vCenter sur laquelle vous souhaitez créer le profil d'identification d'hôte.
 

**i REMARQUE :** Si vous sélectionnez **Tous les vCenters enregistrés** lors de la création du profil d'identification d'hôte, la connexion test échoue pour tous les hôtes exécutant ESXi 6.5 ou ultérieur pour lesquels le service WBEM est désactivé. Dans ce cas, Dell EMC recommande de terminer les actions de l'Assistant de création du profil d'identification d'hôte, d'exécuter l'inventaire sur les hôtes, puis de retester le profil d'identification d'hôte.
  - c. Dans le champ **Informations d'identification**, saisissez les informations d'identification locales d'iDRAC ou AD.

- Pour saisir les informations d'identification locales d'iDRAC, exécutez les tâches suivantes :
    - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur**. Le nom d'utilisateur ne doit pas comporter plus de 16 caractères. Pour plus d'informations sur la définition des noms d'utilisateur, consultez le *Guide d'utilisation d'iDRAC* disponible sur le site [dell.com/support](http://dell.com/support).
    - Saisissez le mot de passe. Pour plus d'informations sur les caractères recommandés dans les noms d'utilisateur et mots de passe, reportez-vous au *Guide d'utilisation d'iDRAC* disponible sur [dell.com/support](http://dell.com/support).
    - Pour télécharger et stocker le certificat iDRAC et le valider lors de toutes les connexions futures, cochez la case **Activer la vérification du certificat**.
  - Pour saisir les informations d'identification d'un iDRAC déjà configuré et activé pour AD, cochez la case **Utiliser Active Directory**.
    - **REMARQUE :** Le compte iDRAC exige que l'utilisateur détienne des droits d'administration pour mettre à jour le firmware et déployer un système d'exploitation.
    - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**. Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la *documentation Microsoft Active Directory* pour connaître les conventions de nom d'utilisateur.
    - Saisissez le mot de passe.  
Les informations d'identification Active Directory du contrôleur iDRAC et de l'hôte peuvent être identiques ou distinctes.
    - Pour télécharger et stocker le certificat iDRAC et le valider lors de toutes les connexions futures, cochez la case **Activer la vérification du certificat**.
- d. Dans le champ **Hôte racine**, saisissez les informations d'identification locales d'hôte ou AD.
- Pour saisir les informations d'identification locales d'hôte ESXi, exécutez les tâches suivantes :
    - Le nom d'utilisateur par défaut est **root**. Vous ne pouvez pas modifier celui-ci.
    - Saisissez le mot de passe.
    - Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, cochez la case **Activer la vérification du certificat**.
  - Pour saisir les informations d'identification des hôtes déjà configurés et activés pour AD, cochez la case **Utiliser Active Directory**.
    - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**. Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la *documentation Microsoft Active Directory* pour connaître les conventions de nom d'utilisateur.
    - Saisissez le mot de passe.
    - Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, cochez la case **Activer la vérification du certificat**.
- **REMARQUE :** Pour les hôtes exécutant ESXi 6.5 U2 et versions ultérieures, OMIVV peut obtenir les informations de l'iDRAC même si des informations d'identification incorrectes sont saisies.
5. Cliquez sur **Suivant**.  
La page **Sélectionner les hôtes** s'affiche.
- **REMARQUE :** Si vous tentez de gérer tous les hôtes associés à OMIVV dans un seul profil d'identification d'hôte, l'affichage de la notification d'inventaire Dell peut prendre quelques minutes dans vCenter. Ce délai peut se produire lorsque vous ajoutez un grand nombre d'hôtes à un profil d'identification d'hôte pour la première fois. L'inventaire suivant s'exécutera normalement.
6. Sur la page **Sélectionner les hôtes**, développez l'arborescence et sélectionnez les hôtes, puis cliquez sur **OK**.
- Cliquez sur **AJOUTER UN HÔTE** pour ajouter ou supprimer des hôtes de la page **Hôtes associés**.
  - **REMARQUE :** N'ajoutez pas un serveur MX PowerEdge avec un iDRAC IPv4 désactivé à un profil d'identification d'hôte. Ces serveurs sont gérés à l'aide d'un profil d'identification de châssis.
- Les hôtes sélectionnés sont affichés sur la page **Hôtes associés**.
7. Pour tester la connexion, sélectionnez un ou plusieurs hôtes, puis cliquez sur **DÉMARRER LE TEST**. Dell EMC recommande de tester la connexion pour tous les hôtes configurés.
- **REMARQUE :** Même après avoir saisi des informations d'identification valides, l'opération de test de la connexion peut échouer pour l'hôte et un message s'affiche indiquant que des informations d'identification non valides ont été saisies. Ce problème survient si ESXi bloque l'accès. Plusieurs tentatives de connexion à ESXi à l'aide d'informations d'identification incorrectes vous empêchent d'accéder à ESXi pendant 15 minutes. Patientez 15 minutes, puis réessayez.
- Pour arrêter le processus de test de connexion, cliquez sur **ANNULER LE TEST**.

Vous pouvez consulter les résultats du test de la connexion dans la section **RÉSULTATS DU TEST**.

**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 la connexion ou pendant l'inventaire sur ces hôtes.

**REMARQUE :** Tester la connectivité iDRAC dans un profil d'identification d'hôte à l'aide d'un mot de passe incorrect verrouille l'accès d'iDRAC à l'appliance jusqu'à ce que le temps de pénalité configuré dans iDRAC soit atteint. Réessayez avec le mot de passe correct après le temps de pénalité spécifié dans les paramètres de filtrage et de blocage IP dans iDRAC.

8. Cliquez sur **Terminer**.

## Planification d'une tâche d'inventaire

Pour afficher les données d'inventaire les plus récentes sur OMIVV, vous devez planifier une tâche d'inventaire pour qu'elle s'exécute périodiquement afin de s'assurer que les informations d'inventaire des hôtes ou des châssis sont à jour. Dell EMC recommande d'exécuter la tâche d'inventaire sur une base hebdomadaire.

**REMARQUE :** Le châssis est géré dans le contexte OMIVV. Il n'existe aucun contexte de vCenter dans la gestion du châssis. Une fois l'inventaire de l'hôte planifié, l'inventaire du châssis est déclenché pour tous les châssis gérés à l'aide d'OMIVV.

**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. Sur la page d'accueil de OMIVV, cliquez sur **Paramètres > > Paramètres vCenter > > Planification de récupération des données > > Récupération de la garantie**.

2. Cochez la case **Activer la récupération des données d'inventaire (Recommandé)**.

Dans un environnement PSC disposant de plusieurs serveurs de vCenter, si la planification de chaque vCenter est différente et si vous sélectionnez l'option **Tous les vCenters inscrits** pour mettre à jour la planification de l'inventaire, la page Paramètres de planification de l'inventaire affiche la planification par défaut.

3. Sélectionnez le jour et l'heure d'extraction des données d'inventaire, puis cliquez sur **APPLIQUER**.

**REMARQUE :** Dans un environnement PSC doté de plusieurs serveurs vCenter, si vous mettez à jour la planification de l'inventaire de **Tous les vCenters inscrits**, la mise à jour remplace les paramètres de planification d'inventaire vCenter individuel.

## Planification des tâches de récupération de la garantie

1. Assurez-vous que l'inventaire est exécuté avec succès sur les hôtes et les châssis.

2. Pour utiliser les fonctions de garantie d'OMIVV, vous devez disposer d'une connexion Internet. Si votre environnement requiert un proxy pour accéder à Internet, veillez à configurer les paramètres de proxy dans le portail d'administration.

Les informations sur la garantie du matériel sont récupérées à partir de Dell Online et sont affichées par OMIVV. Seul le numéro de série est envoyé, mais celui-ci n'est pas stocké par Dell Online.

Dans un environnement PSC avec plusieurs serveurs vCenter, la garantie du châssis s'exécute automatiquement pour chaque vCenter lorsque la garantie de n'importe lequel d'entre eux est exécutée. Toutefois, la garantie ne s'exécute pas automatiquement si elle n'est pas ajoutée au profil d'identification de 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 la garantie, veillez à répliquer la tâche de récupération de la garantie précédente dans cette page avant de suivre les fonctions de l'assistant afin que la tâche précédente ne soit pas remplacée par les paramètres par défaut.

1. Sur la page d'accueil de OMIVV, cliquez sur **paramètres > vCenter paramètres > planification de récupération des données > récupération de la garantie**.

2. Cochez la case **Activer la récupération des données de garantie (Recommandé)**.

Dans un environnement PSC disposant de plusieurs serveurs de vCenter, si la planification de chaque vCenter est différente et que vous sélectionnez l'option **Tous les vCenters inscrits** pour mettre à jour la planification de la garantie, la page Paramètres de planification de la garantie affiche la planification par défaut.

3. Sélectionnez le jour et l'heure d'extraction des données de garantie, puis cliquez sur **APPLIQUER**.

**REMARQUE :** Dans un environnement PSC doté de plusieurs serveurs vCenter, si vous mettez à jour la planification de la garantie de **Tous les vCenters inscrits**, la mise à jour remplace les paramètres de planification de garantie vCenter individuels.

## Configuration des événements et alarmes

Pour recevoir des événements des serveurs, vérifiez que la destination du trap SNMP est définie dans le contrôleur iDRAC. L'OMIVV prend en charge les alertes SNMP v1 et v2.

1. Sur la page d'accueil OMIVV, cliquez sur **Paramètres > Paramètres vCenter > Événements et alarmes**.
2. Pour activer les alarmes pour tous les hôtes et leur châssis, cliquez sur **Activer les alarmes pour tous les hôtes et leur châssis**. La page **Activation des avertissements d'alarmes Dell EMC** affiche les clusters et l'hôte non mis en cluster qui peuvent être affectés après l'activation des alarmes Dell EMC.
  - REMARQUE :** Les hôtes Dell EMC pour lesquels les alarmes sont activées répondent à certaines événements critiques en entrant en mode de maintenance. Vous pouvez modifier l'alarme, si nécessaire.
  - REMARQUE :** Dans vCenter 6.7 U1 et 6.7 U2, l'option de modification échoue. Pour modifier les définitions d'alarme, Dell EMC recommande d'utiliser le client Web (FLEX).
  - REMARQUE :** Les interruptions BMC n'ont pas d'ID de message, de sorte que les alertes ne possèdent pas ces détails dans OMIVV.
3. Pour accepter la modification, cliquez sur **CONTINUER**. Les alarmes pour tous les hôtes et leurs châssis sont activées.
4. Sélectionnez un des niveaux de publication d'événement suivants :
  - **Ne pas publier d'événements :** ne pas transférer d'événements ou d'alertes dans ses vCenters associés.
  - **Publier tous les événements :** publier tous les événements, y compris les événements d'information et les événements reçus des hôtes et du châssis et gérés dans ses vCenters associés. Dell EMC vous recommande de sélectionner l'option Publier tous les événements comme niveau de publication d'événement.
  - **Publier uniquement les événements de type Critique et Avertissement :** publier uniquement les événements de niveau critique et d'avertissement dans ses vCenters associés.
  - **Publier uniquement les événements relatifs à la virtualisation :** publier les événements liés à la virtualisation reçus des hôtes dans ses vCenters associés. Les événements liés à la virtualisation sont ceux qui sont les plus critiques pour les hôtes exécutant des machines virtuelles.
5. Pour enregistrer les modifications, cliquez sur **APPLIQUER**.

Pour restaurer les paramètres d'alarme par défaut de vCenter pour tous les hôtes et leur châssis, cliquez sur **RESTAURER LES ALARMES**. Il peut s'écouler une minute avant que le changement prenne effet.

Le bouton **RESTAURER LES ALARMES** permet de restaurer simplement la configuration d'alarme par défaut sans désinstaller puis réinstaller le produit. Si des configurations d'alarme Dell EMC ont été modifiées depuis l'installation, ces changements sont annulés à l'aide de l'option **RESTAURER LES ALARMES**.

  - REMARQUE :** Les paramètres des événements et alarmes ne sont pas activés après la restauration de l'appliance. Vous devez réactiver les paramètres Événements et alarmes depuis l'onglet Paramètres.

## Tâches de configuration sur la page Paramètres

Vous pouvez effectuer les tâches suivantes sur la page **Paramètres** :

- [Configuration des notifications d'expiration de la garantie](#)
- [Configuration de la notification relative à la dernière version de l'appliance](#)
- [Configuration des informations d'identification de déploiement](#)
- [Remplacement de la gravité des notifications de mise à jour de l'intégrité](#)
- [Configuration initiale](#)

## Configuration des notifications d'expiration de la garantie

Activez la notification d'expiration de la garantie pour recevoir une notification lorsque la date d'expiration de garantie de l'un des hôtes se rapproche.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Paramètres** > **Notifications** > **Notification d'expiration de la garantie**.
2. Sélectionnez **Activer la notification d'expiration de la garantie pour les hôtes**.
3. Sélectionnez le nombre de jours avant l'expiration de la garantie pour l'envoi de la notification.
4. Cliquez sur **APPLIQUER**.

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

Pour recevoir une notification lorsqu'une version OMIVV plus récente est disponible, cochez la case **Activer la notification de la dernière version (recommandé)**. Dell EMC recommande une vérification hebdomadaire. Pour utiliser les fonctionnalités de la dernière version de l'appliance d'OMIVV, vous devez disposer d'une connexion Internet. Si votre environnement requiert un proxy pour accéder à Internet, veillez à configurer les paramètres de proxy sur le portail d'administration.

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. Sur la page d'accueil d'OMIVV, cliquez sur **Paramètres** > **Paramètres d'appliance** > **Notifications** > **Notification de la dernière version**.
2. Cochez la case **Activer la notification relative à la dernière version (Recommandé)**.
3. Pour recevoir la notification de la dernière version de l'appliance, sélectionnez la date et l'heure.
4. Cliquez sur **APPLIQUER**.

## Configuration des informations d'identification de déploiement

OMIVV fonctionne comme un serveur de provisioning. Les informations d'identification de déploiement permettent de communiquer avec l'iDRAC qui utilise le plug-in OMIVV comme serveur de configuration au cours du processus de détection automatique. Les informations d'identification de déploiement vous permettent de configurer des informations d'identification pour iDRAC afin de communiquer en toute sécurité avec un serveur sur matériel vierge découvert à l'aide de la détection automatique jusqu'à ce que le déploiement du système d'exploitation soit terminé.

Une fois le processus de déploiement de l'OS terminé, OMIVV modifie les informations d'identification du contrôleur iDRAC comme indiqué dans le profil d'identification d'hôte. Si vous modifiez les informations d'identification de déploiement, tous les systèmes nouvellement découverts automatiquement sont provisionnés avec les nouvelles informations d'identification d'iDRAC. Toutefois, les informations d'identification stockées sur les serveurs découverts avant la modification des informations d'identification de déploiement ne sont pas affectées par ce changement.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Paramètres** > **Paramètres de l'appliance** > **Informations d'identification du déploiement**.
2. Saisissez un nom d'utilisateur et un mot de passe. Le nom d'utilisateur par défaut est **root** et le mot de passe est **calvin**. Veillez à fournir uniquement les caractères et les informations d'identification locales iDRAC pris en charge.
3. Cliquez sur **APPLIQUER**.

## Remplacement de la gravité des notifications de mise à jour de l'intégrité

Vous pouvez effectuer la configuration de sorte à remplacer la gravité existante des événements Dell Proactive HA de l'hôte Dell EMC et ses composants par une gravité personnalisée, adaptée à votre environnement.

Les éléments suivants sont les niveaux de gravité qui s'appliquent à chacun des événements Proactive HA :

- **Informatif**
- **Modérément dégradé**
- **Gravement dégradé**

 **REMARQUE** : Vous ne pouvez pas personnaliser la gravité des composants Proactive HA avec le niveau de gravité **Informatif**.

1. Dans OpenManage INTEGRATION for VMware vCenter, cliquez sur **Settings** > **Appliance Settings** > **override Severity for proactive ha**.

La grille de données affiche tous les événements Proactive HA pris en charge et comprend des colonnes pour les identifiants d'événements, la description de l'événement, le type du composant, la gravité par défaut et le remplacement de la gravité pour personnaliser la gravité de l'hôte et de ses composants.

2. Pour modifier la gravité d'un hôte ou d'un de ses composants, sélectionnez l'état souhaité dans la liste déroulante sous la colonne **Remplacer la gravité**.  
Cette stratégie s'applique à tous les hôtes Proactive HA sur tous les serveurs vCenter qui sont enregistrés avec OMIVV.
3. Répétez l'étape 2 pour tous les événements devant être personnalisés.
4. Effectuez l'une des actions suivantes :
  - a. Pour enregistrer la personnalisation, cliquez sur **APPLIQUER**.
  - b. Pour annuler le remplacement des paramètres de gravité, cliquez sur **ANNULER**.  
Pour réinitialiser les paramètres de gravité par défaut, cliquez sur **RÉTABLIR LES VALEURS PAR DÉFAUT**.

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

Vous pouvez accéder aux documents requis en utilisant l'un des liens suivants :

- Pour les documents de gestion des systèmes Dell EMC Enterprise : [www.dell.com/SoftwareSecurityManuals](http://www.dell.com/SoftwareSecurityManuals)
- Pour les documents Dell EMC OpenManage : [www.dell.com/OpenManageManuals](http://www.dell.com/OpenManageManuals)
- Pour les documents de gestion des systèmes Dell EMC Enterprise à distance : [www.dell.com/esmmanuals](http://www.dell.com/esmmanuals)
- Pour les documents iDRAC : [www.Dell.com/idracmanuals](http://www.Dell.com/idracmanuals)
- Pour les documents de gestion des systèmes Dell EMC Enterprise - Connexions OpenManage : [www.dell.com/OMConnectionsEnterpriseSystemsManagement](http://www.dell.com/OMConnectionsEnterpriseSystemsManagement)
- Pour les documents Dell EMC Serviceability Tools (Outils de facilité de la gestion) : [www.dell.com/ServiceabilityTools](http://www.dell.com/ServiceabilityTools)
- 1. Rendez-vous sur [www.support.Dell.com](http://www.support.Dell.com).
- 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**
  - **Solutions du secteur public**
  - **Utilitaires**
  - **Mainframe**
  - **Outils de facilité de la gestion**
  - **Solutions de virtualisation**
  - **Systèmes d'exploitation**
  - **Compatibilité**
- 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.

## Documentation connexe

Outre ce guide, les autres manuels sont disponibles sur [dell.com/support/](https://dell.com/support/). Cliquez sur **Parcourir tous les produits**, puis sur **Logiciel > Solutions de virtualisation**. Cliquez sur **OpenManage Integration for VMware vCenter 5.0** pour accéder aux documents suivants :

- *OpenManage Integration for VMware vCenter Version 5.0 User's Guide (Guide d'utilisation d'OpenManage Integration for VMware vCenter version 5.0)*
- *OpenManage Integration for VMware vCenter Version 5.0 Release notes (Notes de mise à jour d'OpenManage Integration for VMware vCenter version 4.0)*
- *OpenManage Integration for VMware vCenter Version 5.0 Compatibility Matrix (Tableau de compatibilité d'OpenManage Integration for VMware vCenter version 4.0)*

Les ressources techniques, notamment les livres blancs, sont disponibles sur <https://www.dell.com/support>.