

OpenManage Integration for VMware vCenter version 4.2

Web Client User's Guide (Guide de l'utilisateur du client
Web)

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.

© 2011 - 2018 Dell Inc. ou ses filiales. Tous droits réservés. Dell, EMC et d'autres marques sont des marques de Dell Inc. ou de ses filiales. Les autres marques peuvent être des marques de leurs propriétaires respectifs.

Table des matières

1 Introduction.....	9
Nouveautés de cette version.....	9
Fonctions OpenManage Integration for VMware vCenter.....	9
2 À propos de la Console Administration.....	11
Utilisation du Portail Administration.....	11
Enregistrement d'un vCenter Server par un utilisateur non-administrateur.....	11
Enregistrement d'un serveur vCenter.....	13
Chargement d'une licence sur le Portail Administration.....	15
Gestion de l'appliance virtuelle.....	15
Configuration des alertes globales.....	20
Gestion des sauvegardes et restaurations.....	20
À propos de la vSphere Client Console.....	22
3 Gestion de plusieurs appliances.....	24
4 Accès à OpenManage Integration à partir du client Web.....	25
Navigation dans le client Web VMware vCenter.....	25
Icônes dans le client Web.....	25
Localisation de la version logicielle.....	26
Actualisation du contenu de l'écran.....	26
Affichage des hôtes Dell EMC.....	26
Affichage de l'onglet des licences OpenManage Integration for VMware vCenter.....	27
Accès à l'aide et au support.....	27
Téléchargement du lot de dépannage.....	28
Réinitialisation d'iDRAC.....	28
Ouverture de l'aide en ligne.....	29
Lancement de la Console Administration.....	29
Affichage de l'historique des journaux.....	29
Affichage des journaux.....	30
Exportation des fichiers journaux.....	30
5 Gestion des licences d'OpenManage Integration for VMware vCenter.....	31
Achat et chargement d'une licence logicielle.....	31
6 Configuration d'appliance pour VMware vCenter.....	33
Tâches de configuration via l'Assistant Configuration.....	33
Affichage de la boîte de dialogue de bienvenue de l'Assistant Configuration.....	33
Sélection de vCenters.....	33
Création d'un profil de connexion.....	34
Planification des tâches d'inventaire.....	36
Exécution de tâches de récupération de la garantie.....	36
Configuration des événements et alarmes.....	37
Tâches de configuration via l'onglet Paramètres.....	37

Paramètres d'appliance.....	38
Paramètres vCenter.....	40
7 Utilisation de l'onglet Ligne de base.....	42
Profil de logithèque.....	42
Création d'un profil de logithèque.....	43
Modification d'un profil de logithèque.....	43
Suppression d'un profil de logithèque.....	44
Profil de cluster.....	44
Création d'un profil de cluster.....	45
Modification du profil de cluster.....	45
Suppression d'un profil de cluster.....	46
8 Profils.....	47
À propos des profils de connexion.....	47
Affichage d'un profil de connexion.....	47
Création d'un profil de connexion.....	47
Modification d'un profil de connexion.....	49
Suppression d'un profil de connexion.....	51
Test d'un profil de connexion.....	51
À propos du profil de châssis.....	52
Affichage des profils de châssis.....	52
Création d'un profil de châssis.....	52
Modification d'un profil de châssis.....	53
Suppression de profils de châssis.....	53
Test d'un profil de châssis.....	54
9 - Gestion de l'inventaire et de la garantie.....	55
Tâches d'inventaire.....	55
Affichage de l'inventaire de l'hôte.....	55
Affichage de l'inventaire du châssis.....	56
Modification des planifications de tâche d'inventaire.....	57
Exécution de tâches d'inventaire.....	57
Exécution immédiate d'une tâche d'inventaire du châssis.....	58
Tâches relatives à la garantie.....	58
Affichage de l'historique de garantie.....	58
Affichage de la garantie du châssis.....	59
Modification des planifications de tâche de garantie.....	59
Exécution immédiate d'une tâche de garantie des hôtes.....	60
Exécution immédiate d'une tâche de garantie du châssis.....	60
Surveillance d'un seul hôte.....	60
Affichage des détails récapitulatifs de l'hôte.....	60
Affichage des détails matériels d'un seul hôte.....	63
Affichage des détails de stockage d'un seul hôte.....	64
À propos des journaux des événements système dans le client Web.....	66
Affichage des détails matériels complémentaires pour un seul hôte.....	67
Surveillance des hôtes sur des clusters et centres de données.....	68
Affichage de la présentation des datacenters et clusters.....	68
Affichage des détails matériels des datacenters et clusters.....	70

Affichage des détails de stockage des datacenters et clusters.....	71
Affichage des détails matériels complémentaires pour les datacenters et clusters.....	73
Configuration du clignotement du voyant d'un serveur physique.....	75
Configuration du mode de verrouillage du système.....	75
10 Surveillance d'événements, d'alarmes et de l'intégrité.....	77
À propos des événements et alarmes pour les hôtes.....	77
À propos des événements et alarmes pour le châssis.....	78
Affichage des événements de châssis.....	78
Affichage des alarmes de châssis.....	78
Événements relatifs à la virtualisation.....	79
Événements Proactive HA.....	87
Affichage des paramètres d'alarme et événement.....	88
Affichage des événements.....	88
Intégrité de la redondance des composants matériels - Proactive HA.....	89
Configuration de Proactive HA pour les serveurs rack et tour	89
Activation de Proactive HA sur des clusters.....	90
Remplacement de la gravité des notifications de mise à jour de l'intégrité.....	91
Lancement des consoles de gestion.....	91
Lancement de la console Remote Access.....	91
Lancement de la console OMSA.....	92
Lancement de la console Chassis Management Controller	92
11 À propos des mises à jour de micrologiciel.....	93
Exécution de la mise à jour du micrologiciel pour un hôte non vSAN.....	93
Exécution de l'Assistant Mise à jour du micrologiciel pour un hôte vSAN.....	95
Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters non vSAN.....	97
Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters vSAN.....	99
12 Gestion de châssis.....	102
Affichage des détails récapitulatifs du châssis.....	102
Affichage des informations d'inventaire matériel du châssis.....	103
Affichage de la configuration du matériel supplémentaire du châssis.....	105
Affichage de l'hôte associé à un châssis.....	106
13 Déploiement d'hyperviseur.....	108
Détection de périphériques.....	109
Détection manuelle.....	109
Détection automatique dans OpenManage Integration for VMware vCenter.....	109
Suppression d'un serveur sans système d'exploitation.....	113
Provisioning.....	113
Profils système.....	113
Création d'un profil système.....	114
Gestion des profils système.....	116
Configuration d'un profil matériel.....	116
Activation de CSIOR sur un serveur de référence.....	117
Création ou personnalisation d'un profil matériel.....	117
Création ou clonage de profil matériel.....	119
Gestion des profils matériels.....	119

Création d'un profil d'hyperviseur.....	120
Gestion des profils d'hyperviseur.....	120
Création de modèles de déploiement.....	121
Gestion des modèles de déploiement.....	121
À propos de l'Assistant Déploiement.....	121
Prise en charge de la technologie VLAN.....	122
Exécution de l'Assistant Déploiement.....	123
Gestion des tâches de déploiement à l'aide de la file d'attente des tâches :.....	124
Gestion des tâches de mise à jour de micrologiciel -	126
Synchronisation de la tâche de déploiement.....	127
Téléchargement d'images ISO EMC Dell personnalisées.....	128
14 À propos de la conformité des hôtes, des serveurs sans système d'exploitation et des iDRAC.....	129
Rapport et résolution de conformité des hôtes vSphere.....	129
Résolution de la conformité de la licence iDRAC des hôtes vSphere.....	131
Affichage de la conformité de ligne de base.....	131
Utilisation d'OMSA avec les serveurs de 11e génération.....	132
Déploiement de l'agent OMSA sur un système ESXi.....	132
Configuration d'une destination d'interruption OMSA.....	133
Rapports et correction de conformité pour les serveurs sans système d'exploitation.....	133
Résolution de la conformité de la licence iDRAC des serveurs sans système d'exploitation.....	134
Actualisation d'un serveur sans système d'exploitation.....	134
15 Autorisations et rôles de sécurité.....	135
Intégrité des données.....	135
Rôles, autorisation et authentification de contrôle d'accès.....	135
Rôle opérationnel Dell.....	136
Rôle de déploiement de l'infrastructure Dell.....	136
À propos des privilèges.....	136
16 Questions fréquemment posées (FAQ).....	138
Questions fréquemment posées (FAQ).....	138
Le bouton Exporter tout ne permet pas d'exporter vers un fichier .CSV dans Google Chrome.....	138
La description et le type de licence iDRAC s'affichent de façon incorrecte pour les hôtes vSphere non conformes.....	138
L'icône Dell EMC ne s'affiche pas après l'annulation de l'enregistrement de vCenter sur une version d'OMIVV précédente et son enregistrement avec une version OMIVV ultérieure.....	138
Le fournisseur Dell ne s'affiche pas en tant que fournisseur de mise à jour d'intégrité.....	139
Échec de l'inventaire lors de la réalisation d'une tâche de mise à jour du micrologiciel sur un hôte ESXi 5.x.....	139
La connexion test ou l'inventaire d'hôte échoue en raison d'une adresse IP non valide ou inconnue de l'iDRAC.....	139
Lors de l'exécution de l'assistant de correction des hôtes vSphere non conformes, l'état d'un hôte spécifique s'affiche comme étant Inconnu.....	140
Les privilèges Dell attribués lors de l'enregistrement de l'appliance OMIVV ne sont pas supprimés après le désenregistrement d'OMIVV.....	140
OMIVV n'affiche pas tous les fichiers log pertinents lors des tentatives de filtrage d'une catégorie de gravité.....	140
Comment puis-je résoudre le code d'erreur 2000000 provoqué par VMware Certificate Authority (VMCA) ?.....	140

Dans l'Administration Console, le chemin d'accès vers l'espace de stockage des mises à jour est défini sur la valeur par défaut après que j'ai rétabli les paramètres d'usine.....	144
La planification de garantie et d'inventaire pour tous les vCenters ne s'applique pas lorsqu'elle est sélectionnée dans la page de file d'attente des tâches.....	144
Que faire lorsqu'une erreur de communication Web dans le client Web vCenter s'affiche après la modification des paramètres DNS dans OMIVV ?.....	145
La page Paramètres ne se charge pas, si je la quitte avant d'y revenir.....	145
Le message d'erreur « Une tâche ne peut pas être planifiée pour une heure dans le passé » s'affiche dans la page de planification d'inventaire et de garantie de l'Assistant Configuration initiale.....	145
La date d'installation s'affiche sous la forme 12-31-1969 pour certains micrologiciels sur la page du micrologiciel.....	145
Une actualisation globale répétée génère une exception dans la fenêtre de tâches récentes.....	145
Pourquoi l'interface utilisateur du client Web est-elle déformée dans quelques écrans Dell dans IE 10 ?.....	146
Je ne vois pas l'icône OpenManage Integration dans le client Web, même si l'enregistrement du plug-in auprès de vCenter a réussi.....	146
La mise à jour du micrologiciel du système 11G montre qu'il n'existe aucun des lots conçus pour une telle mise à jour, même si le référentiel contient les bons lots.....	146
Pourquoi est-ce que les paramètres de configuration du DNS sont restaurés à leurs valeurs d'origine après le redémarrage de l'appliance lorsque les paramètres de DNS et d'adresse IP de l'appliance sont écrasés par les valeurs DHCP.....	146
L'utilisation d'OMIVV pour mettre à jour la carte réseau Intel avec la version 13.5.2 du micrologiciel n'est pas prise en charge.....	147
L'utilisation d'OMIVV pour mettre à jour une carte réseau Intel de la version 14.5 ou 15.0 vers la version 16.x échoue en raison de la préparation exigée par le DUP.....	147
Lors d'une tentative de mise à jour du micrologiciel avec un progiciel DUP non valide, l'état de la tâche de mise à jour matérielle sur la console vCenter ne présente ni un échec ni un temps d'attente pendant des heures, même si l'état de la tâche dans LC est ÉCHEC. Pourquoi ?.....	147
Pourquoi le portail d'administration affiche-t-il un emplacement de référentiel des mises à jour inaccessible ?.....	147
Pourquoi le système n'est pas passé en mode maintenance lorsque j'ai effectué la mise à jour du micrologiciel de un à plusieurs ?.....	148
L'intégrité globale du châssis reste en bon état lorsqu'une partie de l'état du bloc d'alimentation passe à l'état critique.....	148
La version du processeur s'affiche comme « Non applicable » dans la vue du processeur de la page de présentation du système.....	148
OMIVV prend-il en charge vCenter en mode lié ?.....	148
Quels sont les paramètres de port requis pour OMIVV ?.....	148
Le mot de passe utilisé pour la découverte sans système d'exploitation ne change pas pour l'utilisateur après l'application réussie du profil matériel ou du profil système comportant le même utilisateur doté de nouvelles données d'identification modifiées dans la liste d'utilisateurs d'iDRAC.....	151
Impossible d'afficher les détails des nouvelles versions de l'iDRAC répertoriés dans la page des hôtes et des clusters vCenter.....	151
Comment puis-je tester les paramètres d'événements en utilisant OMSA pour simuler un défaut matériel de température ?.....	151
Bien que l'agent OMSA soit installé sur le système hôte OMIVV, je reçois un message d'erreur indiquant qu'OMSA n'est pas installé.....	152
OMIVV peut-il prendre en charge l'ESXi avec le mode de verrouillage activé ?.....	152
Quand j'essaie d'utiliser le mode de verrouillage, celui-ci échoue.....	152
La création du profil matériel échoue si j'utilise un serveur de référence.....	152
Les tentatives de déploiement d'ESXi sur un serveur échouent.....	152
Échec des déploiements d'hyperviseur sur les machines Dell PowerEdge R210 II.....	153
Les systèmes détectés automatiquement s'affichent sans information de modèle dans l'assistant Déploiement.....	153

Le partage NFS est configuré avec l'ISO ESXi, mais le déploiement échoue avec des erreurs de montage de l'emplacement du partage.....	153
Comment puis-je forcer la suppression de l'appliance virtuelle de vCenter.....	153
La saisie d'un mot de passe sur l'écran Backup Now (Sauvegarder maintenant) produit un message d'erreur.....	153
Dans le client Web vSphere, si vous cliquez sur le portlet Dell Server Management ou sur l'icône Dell, l'erreur 404 est retournée.....	154
Que dois-je faire en cas d'échec d'une mise à jour de micrologiciel ?.....	154
Que dois-je faire en cas d'échec de l'enregistrement de vCenter ?.....	154
Performances au cours de la lecture des informations d'identification du test de profil de connexion ralenties ou absence de réponse.....	154
Est-ce qu'OMIVV prend en charge l'appliance VMware vCenter Server ?.....	155
Le niveau de micrologiciel n'est pas à jour lorsque j'ai effectué la mise à jour du micrologiciel à l'aide de l'option Appliquer au redémarrage suivant et que le système a été redémarré.....	155
L'hôte s'affiche sous le châssis, même après la suppression de l'hôte de l'arborescence de vCenter.....	155
Dans l'Administration Console, le chemin d'accès vers l'espace de stockage des mises à jour est défini sur la valeur par défaut après que j'ai rétabli les paramètres d'usine.....	155
Après la sauvegarde et la restauration d'OMIVV, les paramètres de l'alarme ne sont pas restaurés.....	155
Échec du déploiement de l'hyperviseur lorsqu'un NPAR est activé sur un nœud cible et désactivé sur le profil système.....	155
La version disponible de l'appliance virtuelle affiche des informations erronées lorsque la version disponible est inférieure à la version actuelle.....	156
L'exception 267027 est générée lors de l'ajout d'un serveur sans système d'exploitation de 12e génération avec une licence Express	156
Lors du déploiement du système d'exploitation sur les serveurs de 14e génération, l'application du profil matériel échoue en raison d'une erreur iDRAC.....	156
La mise à niveau RPM OMIVV échoue si le proxy est configuré avec une authentification d'utilisateur de domaine.....	156
Impossible d'appliquer un profil système si la carte PCIe est dans le châssis FX.....	156
Problèmes de déploiement de serveurs sans système d'exploitation.....	157
Activation de la découverte automatique sur un système acheté récemment.....	157
17 Documentation connexe	158
Accès aux documents à partir du site de support Dell EMC.....	158
Annexe A : Attributs spécifiques au système	159
Annexe B : Attributs de personnalisation	162
Annexe C : Informations supplémentaires	163
Annexe D : Matrice de comparaison de la version du composant avec la version de ligne de base	164

Introduction

Les administrateurs informatiques utilisent VMware vCenter en tant que console principale pour gérer et surveiller les hôtes VMware vSphere ESX/ESXi. OpenManage Integration for VMware vCenter (OMIVV) vous permet de mieux gérer les hôtes Dell à partir du client Web VMware en fournissant des capacités améliorées de déploiement, de gestion, de surveillance et de mise à niveau.

Sujets :

- [Nouveautés de cette version](#)
- [Fonctions OpenManage Integration for VMware vCenter](#)

Nouveautés de cette version

Cette version d'OpenManage Integration for VMware vCenter fournit les fonctionnalités suivantes :

- La fonction existante de mise à jour compatible avec le système de cluster a été améliorée pour prendre en charge les clusters VSAN. Elle prend en charge les mises à jour de pilotes et de micrologiciels.
- Possibilité de référencer un cluster VSAN pour la configuration de pilote, de micrologiciel et matérielle et pour la découverte des dérivés
- Possibilité d'inclure/exclure les attributs pour le profil système
- Prise en charge des plates-formes de 14e génération
- Prise en charge des partages CIFS SMB2
- Prise en charge d'OMSA 9.1
- Prise en charge de vSphere 6.7

Fonctions OpenManage Integration for VMware vCenter

Les fonctions de l'appliance OpenManage Integration for VMware vCenter (OMIVV) sont les suivantes :

Tableau 1. Fonctions OMIVV

Fonctionnalités	Description
Inventaire	<p>La fonction d'inventaire fournit les éléments suivants :</p> <ul style="list-style-type: none"> • Les détails du serveur PowerEdge, comme la mémoire (quantité et type), la carte réseau, le PSU, les processeurs, le RAC, les informations de garantie, le serveur, le cluster et la vue du niveau du datacenter. • Les détails du châssis, comme les informations du contrôleur de gestion du châssis, le bloc d'alimentation du châssis, l'état du KVM, les détails du ventilateur/thermiques, les informations de garantie, les détails du serveur/commutateur vide.
Surveiller et envoyer des alertes	<p>La surveillance et l'envoi d'alertes comprennent les fonctionnalités suivantes :</p> <ul style="list-style-type: none"> • Détecter des défauts matériels clés et effectuer les actions qui reconnaissent la virtualisation. Par exemple, migrer les charges de traitement ou placer l'hôte en mode de maintenance. • Fournir des renseignements sur l'inventaire, les événements, les alarmes pour diagnostiquer les problèmes de serveur • Prise en charge de la fonctionnalité VMware Proactive HA.

Fonctionnalités	Description
Mises à jour du micrologiciel	<p>La mise à jour du micrologiciel comprend les éléments suivants :</p> <ul style="list-style-type: none"> · Mettre à jour le matériel Dell EMC à la version la plus récente du BIOS et du micrologiciel. · La fonction actuelle de mise à jour compatible avec le système de cluster est optimisée pour prendre en charge les clusters VSAN lorsque l'option DRS est activée. La fonction améliorée prend également en charge la mise à jour du pilote et des micrologiciels des clusters VSAN.
Déploiement et approvisionnement	<p>Créer des profils matériels (serveurs PowerEdge de la 11e à la 13e génération), des profils système (serveurs de 14e génération), des profils d'hyperviseur et déployer à distance des systèmes d'exploitation sur les serveurs PowerEdge sans système d'exploitation à l'aide de VMware vCenter sans utiliser PXE.</p>
Informations de service	<p>Récupérer les informations de garantie pour les serveurs Dell EMC et leurs châssis associés à partir de la base de données des garanties de Dell et permettre une mise à niveau de la garantie facile en ligne.</p>
Rôles et autorisations de sécurité	<p>Les rôles de sécurité et autorisations comprennent les fonctionnalités suivantes :</p> <ul style="list-style-type: none"> · S'intègre avec les règles, autorisations et l'authentification vCenter standard. · Prise en charge du mode de verrouillage de l'iDRAC à la 14e génération de serveurs.

REMARQUE : À partir d'OMIVV 4.0 et versions ultérieures, seul le client Web VMware vSphere est pris en charge et le bureau client vSphere n'est pas pris en charge.

REMARQUE : Pour vCenter 6.5 et versions ultérieures, l'appliance OMIVV est disponible uniquement pour la version Flash. L'appliance OMIVV n'est pas disponible pour la version HTML5.

À propos de la Console Administration

Vous pouvez assurer l'administration d'OpenManage Integration for VMware vCenter et de son environnement virtuel à l'aide des deux portails d'administration suivants :

- Administration Console Web
- Vue de console pour un serveur particulier (la console de la machine virtuelle de l'appliance OMIVV)

Sujets :

- [Utilisation du Portail Administration](#)

Utilisation du Portail Administration

Vous pouvez utiliser le portail d'administration pour effectuer les tâches suivantes :

- Enregistrer un serveur vCenter. Voir [Enregistrement d'un serveur vCenter](#).
- Modifier des informations d'identification pour la connexion à vCenter. Voir [Modification des informations d'identification de connexion à vCenter](#).
- Mettre à jour des certificats SSL. Voir [Mise à jour des certificats SSL des serveurs vCenter enregistrés](#).
- Charger ou acheter une licence. Si vous utilisez une licence d'évaluation, le lien **Acheter un logiciel** s'affiche. En cliquant sur ce lien, vous pouvez acheter une licence de version complète afin de gérer plusieurs hôtes. Voir [Chargement d'une licence sur le Portail d'Administration](#).
- Mettre à jour OMIVV. Voir [Mise à jour de l'appliance virtuelle et de l'emplacement de son référentiel](#).
- Générer un lot de dépannage. Voir [Téléchargement du lot de dépannage](#).
- Redémarrer OMIVV. Voir [Redémarrage de l'appliance virtuelle](#).
- Effectuer des sauvegardes et des restaurations. Voir [Mise à jour de l'appliance via des sauvegardes et restaurations](#).
- Configurer des alertes. Voir [Configuration des alertes globales](#).
- Configurer le mode de déploiement, voir [Configuration du mode de déploiement](#).

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

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

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

1. Pour modifier les privilèges sélectionnés pour un rôle, ajoutez le rôle et sélectionnez les privilèges requis pour celui-ci, ou modifiez un rôle existant.
Pour connaître les étapes à suivre afin de créer ou de modifier un rôle et sélectionner des privilèges dans le client Web vSphere, voir la documentation de VMware vSphere. Pour sélectionner tous les privilèges requis pour le rôle, voir la section [Privilèges requis pour les utilisateurs non administrateurs](#).
REMARQUE : L'administrateur vCenter doit ajouter ou modifier un rôle.
2. Après avoir créé et défini un rôle, attribuez-lui un utilisateur et sélectionnez les privilèges correspondants.
Pour plus d'informations sur l'attribution d'autorisations dans le client Web vSphere, reportez-vous à la documentation de VMware vSphere.
REMARQUE : L'administrateur vCenter doit affecter des autorisations dans vSphere Client.
Un utilisateur non-administrateur du serveur vCenter disposant des privilèges requis peut désormais enregistrer ou désenregistrer des serveurs vCenter, modifier les données d'identification ou mettre à jour le certificat.
3. Enregistrez un serveur vCenter à l'aide d'un utilisateur non-administrateur disposant des privilèges requis. Voir [Enregistrement d'un serveur vCenter par un utilisateur non-administrateur disposant des privilèges requis](#).
4. Attribuez les privilèges Dell au rôle créé ou modifié à l'étape 1. Voir [Attribution de privilèges Dell au rôle dans le client Web vSphere](#).

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

Privilèges requis pour les utilisateurs non administrateurs

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

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

- Alarmes
 - Créer l'alarme
 - Modifier l'alarme
 - Supprimer l'alarme
- Poste
 - Enregistrer le poste
 - Annuler l'enregistrement du poste
 - Mettre à jour le poste
- Global
 - Annuler la tâche
 - Événement journal
 - Paramètres

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

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

i **REMARQUE : Attribuez les privilèges suivants si vous utilisez VMware vCenter 6.5 ou si vous opérez une mise à niveau vers vCenter 6.5 ou version ultérieure :**

- **Host.Config**
 - **Paramètres avancés**
 - **Connexion**
 - **Maintenance**
 - **Configuration réseau**
 - **Demander un correctif**
 - **Profil de sécurité et pare-feu**

- Inventaire
 - Ajouter un hôte au cluster
 - Ajouter un hôte autonome
 - Modifier le cluster

i **REMARQUE : Assurez-vous que vous attribuez le privilège de modification du cluster si vous utilisez vCenter 6.5 ou si vous opérez une mise à niveau vers vCenter 6.5 ou version ultérieure.**

- Profil d'hôte
 - Modifier
 - Afficher
- Droits
 - Modifier les droits
 - Modifier le rôle
- Sessions
 - Valider la session
- Tâche
 - Créer une tâche
 - Mettre à jour la tâche

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


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

Vous pouvez enregistrer un serveur vCenter pour l'appliance OMIVV en tant qu'utilisateur non administrateur doté des privilèges appropriés. Reportez-vous [Enregistrement d'un serveur vCenter](#) pour en savoir plus sur l'enregistrement d'un serveur vCenter en tant qu'utilisateur non administrateur ou en tant qu'administrateur.

Attribution de privilèges Dell à un rôle existant

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

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

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

Pour plus d'informations sur les rôles OMIVV disponibles dans vCenter, voir la section [Rôles et autorisations de sécurité](#).

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

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

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

Enregistrement d'un serveur vCenter

Vous pouvez enregistrer l'appliance OMIVV une fois qu'OpenManage Integration for VMware vCenter est installé. OpenManage Integration for VMware vCenter utilise le compte utilisateur administrateur ou un compte utilisateur non-administrateur disposant des privilèges nécessaires pour les opérations vCenter. Une seule instance de l'appliance OMIVV peut prendre en charge un total de 10 serveurs vCenter et jusqu'à 1 000 hôtes ESXi.

Pour enregistrer un nouveau serveur vCenter, effectuez les étapes suivantes :

1. Ouvrez le **Portail Administration** depuis un navigateur pris en charge.
Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console d'administration** ou démarrez un navigateur Web et renseignez l'URL `https://<ApplianceIP|hostname>`.
2. Dans le volet gauche, cliquez sur **ENREGISTREMENT DE VCENTER**, puis cliquez sur **Enregistrer un nouveau serveur vCenter**.
3. Dans la boîte de dialogue **ENREGISTRER UN NOUVEAU SERVEUR VCENTER**, sous **Nom du serveur vCenter**, procédez comme suit :
 - a) Dans la zone de texte **Nom d'hôte ou IP du serveur vCenter**, entrez l'adresse IP du vCenter ou le FQDN de l'hôte.

REMARQUE : Dell recommande l'enregistrement d'OMIVV avec VMware vCenter en utilisant le nom de domaine complet (FQDN). Pour tous les enregistrements, le nom d'hôte du vCenter doit pouvoir être correctement résolu par le serveur DNS. Les pratiques suivantes sont recommandées pour l'utilisation du serveur DNS :

 - **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.**
 - b) Dans la zone de texte **Description**, entrez une description (facultatif).
4. Sous **Compte utilisateur vCenter**, procédez comme suit :
 - a) Dans la zone de texte **Nom d'utilisateur vCenter**, saisissez le nom d'utilisateur de l'administrateur ou un nom d'utilisateur non administrateur disposant des privilèges requis.
 - b) Dans la zone de texte **Mot de passe**, entrez le mot de passe.
 - c) Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe.
5. Cliquez sur **S'inscrire**.

Après l'enregistrement du serveur vCenter, OMIVV est enregistré en tant que plug-in vCenter et l'icône Dell EMC OpenManage Integration est visible dans le client Web vSphere à partir duquel vous pouvez accéder aux fonctionnalités OMIVV.

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

L'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.

Modification des informations d'identification pour la connexion à vCenter

Les informations d'identification de connexion à vCenter peuvent être modifiées par un utilisateur doté de privilèges d'administration ou un utilisateur non administrateur doté des privilèges nécessaires.

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe, puis cliquez sur **Se connecter**.
3. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**.
Les serveurs vCenter enregistrés sont affichés dans le volet de droite de la fenêtre **GÉRER LES CONNEXIONS DE SERVEUR VCENTER**. Pour ouvrir la fenêtre **MODIFIER LE COMPTE UTILISATEUR**, sous **Références**, cliquez sur **Modifier** pour un vCenter enregistré.
4. Entrez le **Nom d'utilisateur** et le **Mot de passe** vCenter, puis **Confirmer le mot de passe**. Les mots de passe doivent concorder.
5. Pour changer le mot de passe, cliquez sur **Appliquer**. Pour annuler le changement, cliquez sur **Annuler**.

REMARQUE : Un message d'erreur s'affiche si l'utilisateur indiqué ne dispose pas des privilèges nécessaires.

Mise à jour des certificats SSL des serveurs vCenter enregistrés

L'OpenManage Integration for VMware vCenter utilise l'API OpenSSL pour créer la requête de signature de certificat (RSC) à l'aide de la norme de cryptage standard RSA, dotée d'une longueur de clé de 2 048 bits. La RCS générée par OMIVV obtient un certificat signé numériquement, provenant d'une autorité de certification de confiance. L'OpenManage Integration for VMware vCenter utilise ce certificat numérique pour activer SSL sur le serveur Web pour sécuriser la communication.

Si le certificat SSL est modifié sur un serveur vCenter, suivez les étapes ci-dessous afin d'importer le nouveau certificat pour OpenManage Integration for VMware vCenter.

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
2. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**.
Les serveurs vCenter enregistrés s'affichent dans le volet droit.
3. Pour mettre à jour le certificat du nom d'hôte ou de l'adresse IP d'un serveur vCenter, cliquez sur **Mettre à jour**.

Désinstallation d'OpenManage Integration for VMware vCenter

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

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

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
2. Dans la page ENREGISTREMENT DE VCENTER, accédez au tableau **Nom d'hôte ou adresse IP du serveur vCenter**, puis cliquez sur **Désenregistrer**.

REMARQUE : Étant donné qu'il peut y avoir plusieurs serveurs vCenter, veillez à sélectionner le serveur vCenter approprié.

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 : 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**, décochez la case située à côté du fournisseur Dell Inc.

Chargement d'une licence sur le Portail Administration

Vous pouvez charger une licence OMIVV pour modifier le nombre d'instances vCenter et d'hôtes gérés pris en charge et enregistrés simultanément. Vous pouvez également ajouter des licences si vous avez besoin d'ajouter plus d'hôtes en effectuant les étapes suivantes :

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `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 droit.
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**.

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

Gestion de l'appliance virtuelle

La gestion de l'appliance virtuelle vous permet de gérer le réseau, la version, le protocole NTP et les informations HTTPS concernant OpenManage Integration for VMware vCenter. En outre, cette gestion permet à un administrateur de :

- Redémarrer l'appliance virtuelle. Voir [Redémarrage de l'appliance virtuelle](#).
- Mettre à jour l'appliance virtuelle et configurer un emplacement pour la logithèque de mise à jour. [Mise à jour de l'appliance virtuelle et de l'emplacement de son espace de stockage](#).
- Configurer des serveurs NTP. Voir [Configuration des serveurs NTP \(Network Time Protocol\)](#).
- Téléverser des certificats HTTPS. Voir [Chargement d'un certificat HTTPS](#).

Dans Dell OpenManage Integration for VMware vCenter, effectuez les étapes suivantes pour accéder à la page **GESTION DE L'APPLIANCE** via le Portail Administration :

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe.
3. Pour configurer la section GESTION DE L'APPLIANCE, accédez au volet gauche, puis cliquez sur **GESTION DE L'APPLIANCE**.

Redémarrage de l'appliance virtuelle

1. Dans la page **GESTION DE L'APPLIANCE**, cliquez sur **Redémarrer l'appliance virtuelle**.
2. Pour redémarrer l'appliance virtuelle, accédez à la boîte de dialogue **Redémarrer l'appliance virtuelle** et cliquez sur **Appliquer** (ou sur **Annuler**, si vous souhaitez annuler cette action).

Modification du nom d'hôte de l'appliance virtuelle

Effectuez les opérations suivantes :

1. Sur la page **Gestion de l'appliance**, cliquez sur **Modifier le nom d'hôte**.
2. Saisissez un nom d'hôte mis à jour.
Saisissez le nom de domaine au format suivant : `<nomd'hôte>`.
3. Cliquez sur **Mettre à jour le nom d'hôte**.
Le nom d'hôte de l'appliance est mis à jour et vous revenez au menu principal.
4. Pour redémarrer l'appliance, cliquez sur **Redémarrer l'appliance**.

REMARQUE : Si vous aviez enregistré des serveurs vCenter avec l'appliance, désenregistrez et enregistrez de nouveau les instances vCenter.

REMARQUE : Assurez-vous de mettre à jour manuellement toutes les références à l'appliance virtuelle sur son environnement, telles que le serveur d'approvisionnement dans l'iDRAC, DRM.

Mise à jour de l'appliance virtuelle et de l'emplacement de son référentiel

Pour garantir la protection de toutes les données, sauvegardez la base de données OMIVV avant de mettre à jour l'appliance virtuelle. Voir [Gestion des sauvegardes et restaurations](#).

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

REMARQUE : L'appliance 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. Selon les paramètres du réseau, activez l'utilisation de serveurs proxy et fournissez les paramètres proxy si le réseau nécessite un serveur proxy. Voir [Configuration du proxy HTTP](#).

REMARQUE : Vérifiez que le Chemin d'accès au référentiel de mise à jour est valide.

Pour la version disponible de l'appliance virtuelle, les mécanismes de mise à niveau des appliances virtuelles OMIVV et OVF qui conviennent sont accompagnés d'une coche. Vous trouverez ci-dessous les options de mécanisme de mise à niveau possibles, et vous pouvez effectuer l'une de ces tâches pour le mécanisme de mise à niveau :

- 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 [Mise à niveau d'une version existante à la dernière version](#).
- 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'appliance disponible. Voir [Mise à jour de l'appliance via des sauvegardes et restaurations](#).
- 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'appliance virtuelle, effectuez les tâches ci-dessus pour les mécanismes de mise à niveau adéquats à partir de la version d'OMIVV.

REMARQUE : N'oubliez pas de vous déconnecter de toutes les sessions client Web avec les serveurs vCenter enregistrés.

REMARQUE : 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.

3. Cliquez sur **GESTION DE L'APPLIANCE** et vérifiez les mécanismes de mise à niveau.

Mise à niveau d'OMIVV d'une version existante vers la version actuelle

1. Sur la page **GESTION DE L'APPLIANCE**, selon les paramètres de votre réseau, activez le proxy et fournissez les paramètres de proxy, si votre réseau nécessite un proxy. Voir [Configuration de proxy HTTP](#).
2. Pour mettre à niveau le plug-in OpenManage Integration d'une version existante vers la version actuelle, 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 : <http://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 <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> dans la zone de texte **chemin d'accès à l'espace de stockage de mise à jour**. Pour enregistrer les valeurs, cliquez sur **Appliquer**.
 - Pour effectuer une mise à niveau avec les derniers dossiers ou fichiers RPM téléchargés si vous ne disposez pas d'une connectivité Internet, téléchargez tous les fichiers et dossiers à partir du chemin <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> et copiez-les sur un espace de partage HTTP. Dans la section **MISE À JOUR DE L'APPLIANCE** de la fenêtre **Gestion de l'appliance**, cliquez sur **Modifier**. Ensuite, dans la zone de texte **Chemin d'accès au référentiel de mise à jour**, incluez le chemin de l'espace de partage HTTP hors ligne, puis cliquez sur **Appliquer**.
3. Comparez la version de l'appliance virtuelle disponible avec la version de l'appliance virtuelle actuelle et assurez-vous que la version de l'appliance virtuelle disponible est ultérieure à la version de l'appliance virtuelle actuelle.
4. Pour appliquer la mise à jour à l'appliance virtuelle, 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 **CONSOLE ADMINISTRATION**.
6. Fermez le navigateur Web.

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

REMARQUE : Une fois l'appliance mise à niveau via RPM, assurez-vous d'effectuer les opérations suivantes :

- Effacez le cache du navigateur avant de vous connecter au portail d'administration Dell.
 - Réinstallation de VMWare Tools.
- Pour réinstaller VMware Tools :**
1. Effectuez un clic droit sur l'appliance OMIVV.
 2. Placez le pointeur de la souris sur **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 **Tâches récentes**.

REMARQUE : Une fois la mise à niveau RPM terminée, vous pouvez afficher l'écran de connexion de la console OMIVV. Ouvrez un navigateur, entrez le lien `https://<IpAppliance/NomHôte>`, puis naviguez jusqu'à la zone **MISE À JOUR DE L'APPLIANCE**. Vous pouvez vérifier si les versions de l'appliance virtuelle 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. Par conséquent, 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 jour de l'appliance via des sauvegardes et restaurations

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

1. Effectuez une sauvegarde de la base de données de l'ancienne version.
2. Mettez l'ancienne appliance OMIVV hors tension depuis le vCenter.
 - REMARQUE :** N'annulez pas l'enregistrement du plug-in OMIVV sur le serveur vCenter. Cela entraînerait la suppression de toutes les alarmes enregistrées sur le serveur vCenter par le plug-in OMIVV ainsi que de toutes les personnalisations effectuées sur les alarmes, telles que les actions.
3. Déployez la nouvelle appliance OVF OpenManage Integration.
4. Mettez la nouvelle appliance OpenManage Integration sous tension.
5. Configurez le réseau, le fuseau horaire, et ainsi de suite, pour la nouvelle appliance.

REMARQUE : Assurez-vous que la nouvelle appliance OpenManage Integration a la même adresse IP que l'ancienne appliance.

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

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](#) et [Chargement d'un certificat HTTPS](#). 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. Voir la section Vérification de l'installation du document *OpenManage Integration for VMware vCenter Install Guide (Guide d'installation d'OpenManage Integration for VMware vCenter)*, disponible à l'adresse Dell.com/support/manuals.
9. Exécutez l'**Inventaire** sur tous les serveurs vCenter enregistrés.

REMARQUE : Une fois la mise à niveau effectuée, Dell EMC vous recommande d'exécuter à nouveau l'inventaire sur tous les hôtes gérés par le plug-in. Pour exécuter l'inventaire sur demande, voir [Planification des tâches d'inventaire](#).

REMARQUE : Si l'adresse IP de la nouvelle version d'OMIVV y est modifiée depuis la version x d'OMIVV, la destination des interruptions SNMP doit être configurée de sorte à pointer vers la nouvelle appliance. Pour les serveurs de 12e génération et de générations ultérieures, ce problème est réglé en exécutant l'inventaire sur ces hôtes. Lors de l'exécution de l'inventaire sur les hôtes de 12e génération, si des interruptions SNMP ne pointent pas vers la nouvelle adresse IP, ces hôtes sont répertoriés comme non conformes. Avec les hôtes antérieurs à la 12e génération qui étaient compatibles avec les versions antérieures, le changement d'adresse IP s'affiche comme non compatible et vous oblige à configurer Dell EMC OpenManage Server Administrator (OMSA). Pour corriger les problèmes de conformité des hôtes vSphere, voir [Exécution de l'Assistant Correction des hôtes vSphere non conformes](#).

Téléchargement de l'ensemble de dépannage

1. Sur la page **GESTION DE L'APPLIANCE**, cliquez sur **Générer un ensemble de dépannage**.
2. Cliquez sur le lien **Télécharger un ensemble de dépannage**.
3. Cliquez sur **Fermer**.

Configuration du proxy HTTP

1. Dans la page **GESTION DE L'APPLIANCE**, faites défiler vers le bas jusqu'à **PARAMÈTRES DU PROXY HTTP** et cliquez sur **Modifier**.
2. Effectuez les étapes suivantes pour activer le mode Édition :
 - a) Sélectionnez **Activé** pour activer l'utilisation des paramètres du proxy HTTP.
 - b) Entrez l'adresse du serveur proxy dans **Adresse du serveur proxy**.
 - c) Entrez le port du serveur proxy dans **Port du serveur proxy**.
 - d) Sélectionnez **Oui** pour utiliser les informations d'identification pour le proxy.
 - e) Si vous utilisez les informations d'identification pour le proxy, entrez le nom d'utilisateur dans **Nom d'utilisateur**.
 - f) Saisissez le mot de passe dans le champ **Mot de passe**.
 - g) Cliquez sur **Appliquer**.

Configuration des serveurs NTP (Network Time Protocol)

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

1. Dans la page **GESTION DE L'APPLIANCE**, cliquez sur **Modifier** dans la zone **Paramètres NTP**.
2. Sélectionnez **Activé**. Entrez le nom d'hôte ou l'adresse IP d'un serveur NTP Privilégié et Secondaire, puis cliquez sur **Appliquer**.

REMARQUE : La synchronisation des horloges de l'appliance virtuelle avec le serveur NTP dure environ 10 minutes.

Configuration du mode de déploiement

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

Tableau 2. Configuration requise pour les modes de déploiement

Modes de déploiement	Nombre d'hôtes	Nombre de processeurs	Mémoire (en Go)	Stockage minimal
Small (Petite)	Jusqu'à 250	2	8	44 Go
Moyen	Jusqu'à 500	4	16	44 Go
Large (Importante)	Jusqu'à 1000	8	32	44 Go

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

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

1. Dans 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 comme **Petit**, **Moyen**, ou **Grand** s'affichent. Par défaut, le mode de déploiement est défini sur **Petit**.
2. Cliquez sur **Modifier** si vous souhaitez mettre à jour le mode de déploiement en fonction de l'environnement.
3. Dans le mode **Modifier**, sélectionnez le mode de déploiement de votre choix après avoir vérifié que les conditions requises sont respectées.
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 l'une des situations suivantes se produit :
 - 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. Si le mode de déploiement est modifié, confirmez les modifications, puis redémarrez l'appliance OMIVV 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 jusqu'à l'écran de connexion. Pour démarrer l'appliance OMIVV, mettez-la hors tension, 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 de mode de déploiement

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

Génération d'une requête de signature de certificat

Veillez à charger le certificat avant d'enregistrer OMIVV auprès du serveur vCenter.

La génération d'une requête de signature de certificat (CRS, Certificate Signing Request) empêche le chargement sur l'appliance des certificats créés avec la CSR générée antérieurement. Pour générer une CSR, procédez comme suit :

1. Dans 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**, pour annuler, cliquez sur **Annuler**.
2. Si vous confirmez la requête, renseignez les champs de requête suivants dans la boîte de dialogue **GÉNÉRER UNE REQUÊTE DE SIGNATURE DE CERTIFICAT** : **Nom commun**, **Nom de l'organisation**, **Unité d'organisation**, **Localité**, **Nom de l'état**, **Pays** et **E-mail**. Cliquez sur **Continuer**.

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

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

1. Dans la page GESTION DE L'APPLIANCE, cliquez sur **Charger le certificat** dans la zone **CERTIFICATS HTTPS**.
2. Cliquez sur **OK** dans la boîte de dialogue **CHARGER LE CERTIFICAT**.
3. Pour sélectionner le certificat à charger, cliquez sur **Parcourir**, puis sur **Charger**.
4. Si vous souhaitez annuler le téléchargement, cliquez sur **Annuler**.

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

Restauration du certificat HTTPS par défaut

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

Configuration des alertes globales

La gestion des alertes vous permet de configurer les paramètres globaux de stockage des alertes de toutes les instances de vCenter.

1. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DES ALERTES**. Pour entrer de nouveaux paramètres d'alertes vCenter, cliquez sur **Modifier**.
4. Entrez les valeurs numériques des champs suivants :
 - **Nombre maximum d'alertes**
 - **Nombre de jours de conservation des alertes**
 - **Délai d'expiration des alertes en double (en secondes)**
5. Pour enregistrer vos paramètres, cliquez sur **Appliquer** (ou sur **Annuler**, si vous souhaitez annuler).

Gestion des sauvegardes et restaurations

La gestion des sauvegardes et des restaurations s'effectue depuis la console d'administration. Les tâches de cette page comprennent :

- 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

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. Pour ouvrir le Portail Administration, dans l'onglet **Aide et support** d'OpenManage Integration for VMware vCenter, cliquez sur le lien situé sous **Console Administration** ou démarrez un navigateur Web et fournissez l'URL `https://<ApplianceIP|hostname>`.
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 à partir duquel elle peut être restaurée à une date ultérieure. Les profils, modèles et informations sur l'hôte sont inclus dans la sauvegarde. Dell 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. Dans 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) Dans la zone de texte **Mot de passe**, saisissez le mot de passe.
 - d) Dans la zone de texte **Entrer le mot de passe utilisé pour crypter les sauvegardes**, saisissez le mot de passe crypté dans la zone de texte.
Le mot de passe de cryptage 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. Dans 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 la sauvegarde.
4. Dans le champ **Heure de sauvegarde (24 heures, HH:mm)**, entrez 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. Dans 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 **SAUVEGARDER MAINTENANT**.
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 cryptage peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#\$\$%* ». Il n'y a aucune limite quant à la longueur du mot de passe.
4. Cliquez sur **Sauvegarder**.

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

L'opération de restauration entraîne le redémarrage de l'appliance virtuelle à la fin de la restauration.

1. Ouvrez la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**. Reportez-vous à la [gestion de sauvegarde, et restaurer](#).
2. Dans la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Restaurer maintenant**.
3. Dans la boîte de dialogue **RESTAURER MAINTENANT**, entrez le chemin d'accès de l'**Emplacement du fichier** et du fichier .gz au format CIFS/NFS.
4. 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 cryptage peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#\$\$%* ». Il n'y a pas de restriction de longueur.
5. Pour enregistrer les modifications, cliquez sur **Appliquer**.
L'appliance redémarre.

 **REMARQUE :** Assurez-vous d'enregistrer à nouveau l'appliance OMIVV si l'appliance est réinitialisée sur les paramètres d'usine.

À propos de la vSphere Client Console

La vSphere Client Console se trouve dans le client vSphere d'une machine virtuelle et fonctionne de pair avec l'Administration Console. Elle permet d'effectuer les tâches suivantes :

- Configurer des paramètres réseau
- Changer le mot de passe de l'appliance virtuelle
- Configurer le NTP et les paramètres du fuseau horaire local
- Redémarrer l'appliance virtuelle
- Réinitialisation de l'appliance virtuelle aux paramètres d'usine
- Se déconnecter à partir de la console
- Utiliser un rôle utilisateur en lecture seule

Ouverture de la console de la machine virtuelle OMIVV

1. Depuis l'**Accueil** du client Web vSphere, cliquez sur **vCenter**.
2. Dans **Listes d'inventaire**, cliquez sur **Machines virtuelles**, puis sélectionnez l'appliance virtuelle OMIVV.
3. Effectuez l'une des opérations suivantes :
 - Dans l'onglet **Objet**, sélectionnez **Action** → **Ouvrir la console**.
 - Cliquez-droit sur la machine virtuelle que vous avez sélectionnée, puis sélectionnez **Ouvrir la console**.

Après avoir ouvert la console de la machine virtuelle et fourni les informations d'identification (nom d'utilisateur : admin et mot de passe : mot de passe défini lors du déploiement de l'appliance), vous pouvez configurer la console.

Configurer des paramètres réseau

Vous pouvez modifier les paramètres réseau dans la vSphere Client Console.

1. Ouvrez la console de la machine virtuelle. Voir la section [Ouverture de la vSphere Client Console](#).
2. Dans la fenêtre **Console**, sélectionnez **Configurer le réseau**, puis appuyez sur **<ENTRÉE>**.
3. Entrez les paramètres réseau souhaités sous **Modifier des périphériques** ou **Modifier DNS**, puis cliquez sur **Enregistrer et quitter**. Pour abandonner les modifications, cliquez sur **Quitter**.

Modification du mot de passe de l'appliance virtuelle

Vous pouvez modifier le mot de passe de l'appliance virtuelle dans le client Web vSphere à l'aide de la console.

1. Ouvrez la console de la machine virtuelle. Voir la section [Ouverture de la vSphere Client Console](#).
2. Dans la fenêtre **Console**, servez-vous des flèches pour sélectionner **Changer le mot de passe Admin** et appuyez sur **ENTRÉE**.
3. Dans **Mot de passe Admin actuel**, entrez la valeur et appuyez sur **ENTRÉE**.
Le mot de passe Admin doit comporter au moins huit caractères et inclure un caractère spécial, un chiffre, une majuscule et une minuscule.
4. Entrez un nouveau mot de passe dans **Entrer le nouveau mot de passe Admin** et appuyez sur **ENTRÉE**.
5. Saisissez de nouveau le nouveau mot de passe dans **Confirmer le mot de passe Admin**, puis appuyez sur **Entrée**.

Configuration de NTP et du fuseau horaire local

1. Ouvrez la console de la machine virtuelle. Voir [Ouverture de la console client vSphere](#).
2. Pour configurer les informations de fuseau horaire d'OMIVV, cliquez sur **Propriétés Date/Heure**.
3. Dans l'onglet **Date et heure**, sélectionnez l'option **Synchroniser la date et l'heure sur le réseau**.
La fenêtre **Serveurs NTP** s'affiche.
4. Pour ajouter le nom d'hôte ou l'adresse IP du serveur NTP, cliquez sur le bouton **Ajouter**, puis appuyez sur la touche **TABULATION**.
5. Cliquez sur **Fuseau horaire** et sélectionnez le fuseau horaire applicable, puis cliquez sur **OK**.

Redémarrage de l'appliance virtuelle

1. Ouvrez la console de la machine virtuelle. Voir la section [Ouverture de la vSphere Client Console](#).
2. Cliquez sur **Redémarrer l'appliance**.
3. Pour redémarrer l'appliance, cliquez sur **Oui** ou sur **Non** pour annuler.

Réinitialisation de l'appliance virtuelle aux paramètres d'usine

1. Ouvrez la console de la machine virtuelle. Voir la section [Ouverture de la vSphere Client Console](#).
2. Cliquez sur **Paramètres de réinitialisation**.

Le message suivant s'affiche :

```
All the settings in the appliance will be Reset to Factory Defaults and the appliance will be rebooted. Do you still wish to continue?
```

3. Pour réinitialiser l'appliance, cliquez sur **Oui** ou sur **Non** pour annuler.
Si vous cliquez sur **Oui**, l'appliance OMIVV est réinitialisée aux paramètres d'usine d'origine et tous les autres paramètres et données existantes sont perdus.

REMARQUE : Lorsque l'appliance virtuelle est réinitialisée aux paramètres d'usine, toutes les mises à jour apportées à la configuration réseau sont conservées ; ces paramètres ne sont pas réinitialisés.

Déconnexion de la console vSphere

Pour vous déconnecter de la console vSphere, cliquez sur **Fermer la session**.

Rôle utilisateur en lecture seule

Il existe un rôle utilisateur non privilégié en lecture seule disposant d'un accès à l'interpréteur de commandes à des fins de diagnostic. Cet utilisateur en lecture seule dispose de privilèges limités pour exécuter le montage. Le mot de passe de cet utilisateur est défini comme étant **en lecture seule**. Dans les précédentes versions d'OMIVV (versions 1.0 à 2.3.1), le mot de passe du rôle utilisateur en lecture seule correspondait au mot de passe administrateur, ce qui pouvait poser des problèmes de sécurité ; par conséquent, à partir de la version 3.0 d'OMIVV, ces mots de passe doivent être différents.

Gestion de plusieurs appliances

Vous pouvez gérer et surveiller plusieurs appliances OMIVV enregistrées auprès de serveurs vCenter appartenant au même PCS (Platform Service Controller) ou à un autre PSC. Dell EMC recommande d'utiliser des versions similaires de vCenter.

Si la page est mise en cache, Dell EMC vous recommande d'effectuer une actualisation globale.

1. Dans la page d'accueil du VMware vCenter, cliquez sur l'icône **OpenManage Integration**.
2. Dans **Navigateur**, accédez au groupe **Dell EMC** et cliquez sur **Appliances OMIVV**.
3. Dans l'onglet **Appliances OMIVV**, affichez les informations suivantes et surveillez les appliances :

REMARQUE : Dans l'onglet **Appliances Dell**, la priorité des appliances répertoriées est prédéterminée et l'appliance en surbrillance correspond à l'appliance active.

- **Nom** : affiche un lien contenant l'adresse IP ou le nom de domaine complet (FQDN) de chaque appliance OMIVV. Pour afficher et surveiller les informations d'une appliance spécifique, cliquez sur le lien correspondant. Vous accédez alors au volet de contenu principal de l'appliance OMIVV. Vous pouvez gérer les opérations OMIVV et surveiller les hôtes, les datacenters et les clusters de l'appliance.

REMARQUE : Si vous utilisez plusieurs appliances, lorsque vous cliquez sur **Nom**, un message s'affiche pour vous inviter à effectuer une actualisation globale des pages mises en cache.

Pour identifier l'appliance sur laquelle vous gérez les opérations OMIVV, procédez comme suit :

- a. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Aide et support**.
- b. Sous Console Administration, affichez l'adresse IP de l'appliance OMIVV spécifique.

- **Version** : affiche la version de chaque appliance OMIVV.
- **État de conformité** : indique si l'appliance est conforme au plug-in chargé.

REMARQUE : La mention **Non conforme** s'affiche lorsque l'appliance OMIVV n'est pas conforme au plug-in et que le lien **Nom** est désactivé.

- **État de disponibilité** : affiche un état indiquant si vous avez accès à l'appliance depuis le plug-in et si les services Web requis sont exécutés dans l'appliance OMIVV.

REMARQUE : Vous pouvez sélectionner une appliance lorsqu'elle est Conforme et que son état de disponibilité est OK.

- **Serveurs vCenter enregistrés** : affiche tous les serveurs vCenter auxquels vous avez accès pendant la session de connexion et qui sont enregistrés auprès des appliances. Si vous enregistrez une appliance auprès de plusieurs serveurs vCenter, ces derniers sont répertoriés dans une liste que vous pouvez développer et réduire. Lorsque vous cliquez sur le lien d'un serveur vCenter, vous accédez à la page **Serveurs vCenter** du volet **Navigateur** où tous les serveurs vCenter sont répertoriés.

Accès à OpenManage Integration à partir du client Web

Lorsque vous vous connectez à VMware vCenter après l'installation d'OMIVV, accédez à l'onglet **Accueil**. L'icône **OpenManage Integration** se trouve dans la zone de contenu principale, sous le groupe **Administration**. Vous pouvez utiliser l'icône **OpenManage Integration** pour accéder à la page **OpenManage Integration for VMware vCenter**. Le groupe **Dell EMC** s'affiche dans le volet **Navigateur**.

La disposition de VMware vCenter présente les trois volets principaux suivants :

Tableau 3. Volets relatifs à OpenManage Integration for VMware vCenter

Volets	Description
Navigateur	Permet d'accéder aux différents affichages de la console. L'OpenManage Integration for VMware vCenter possède un groupe spécial sous le menu vCenter qui sert de point d'accès principal pour OpenManage Integration for VMware vCenter.
Contenu principal	Affiche les vues sélectionnées dans le volet Navigateur. Le volet de contenu principal est l'endroit où s'affiche la majeure partie du contenu.
Notifications	Affiche les alarmes, les tâches et le travail en cours. OpenManage Integration for VMware vCenter s'intègre aux systèmes d'alarmes, d'événements et de tâches concernant vCenter pour afficher les informations dans le volet Notification.

Sujets :

- [Navigation dans le client Web VMware vCenter](#)
- [Icônes dans le client Web](#)
- [Localisation de la version logicielle](#)
- [Actualisation du contenu de l'écran](#)
- [Affichage des hôtes Dell EMC](#)
- [Affichage de l'onglet des licences OpenManage Integration for VMware vCenter](#)
- [Accès à l'aide et au support](#)
- [Affichage de l'historique des journaux](#)

Navigation dans le client Web VMware vCenter

OpenManage Integration for VMware vCenter se trouve dans un groupe **Dell EMC** spécial au sein du VMware vCenter.

1. Connectez-vous au VMware vCenter.
2. Dans la page d'accueil de VMware vCenter, cliquez sur l'icône **OpenManage Integration**.














Vous pouvez alors effectuer les opérations suivantes :

- Gérer les profils de connexion et les paramètres produit OpenManage Integration for VMware vCenter, afficher la page récapitulative et effectuer d'autres opérations dans les onglets du volet de contenu principal.
- Surveiller les hôtes, les datacenters, et les clusters dans le volet Navigateur, sous **Listes d'inventaire vCenter**. Sélectionnez l'hôte, le datacenter, ou le cluster à examiner, puis cliquez sur l'objet à surveiller dans l'onglet **Objets**.

Icônes dans le client Web

L'interface utilisateur produit utilise plusieurs boutons d'action en forme d'icônes pour les actions que vous effectuez.

Tableau 4. Boutons d'icône définis

Boutons d'icône	Définition
	Ajouter ou créer un nouvel élément
	Ajouter un serveur à un profil de connexion, un datacenter et un cluster
	Abandonner une tâche
	Réduire une liste
	Développer une liste
	Supprimer un objet
	Modifier une planification
	Modifier
	Purger une tâche
	Exporter un fichier
	Afficher un profil système
	Filtre
	Exécuter maintenant

Localisation de la version logicielle

La version logicielle se trouve dans l'onglet **Mise en route** d'OpenManage Integration for VMware vCenter.

1. Dans la page d'accueil du VMware vCenter, cliquez sur l'icône **OpenManage Integration**.
2. Dans l'onglet **Mise en route** d'OpenManage Integration for VMware vCenter, cliquez sur **Informations sur la version**.
3. La boîte de dialogue **Informations sur la version** affiche les informations souhaitées.
4. Pour fermer la boîte de dialogue, cliquez sur **OK**.

Actualisation du contenu de l'écran

Actualisez l'écran à l'aide de l'icône **Actualiser** de VMware vCenter.

1. Sélectionnez la page à actualiser.
2. Sur la barre de titre de VMware vCenter, cliquez sur l'icône **Actualiser (Ctrl+Alt+R)**.
L'icône **Actualiser** se trouve à droite de la zone Recherche et ressemble à une flèche tournant dans le sens des aiguilles d'une montre.

Affichage des hôtes Dell EMC

Si vous souhaitez uniquement afficher les hôtes Dell EMC, sélectionnez **Hôtes Dell EMC** dans le volet Navigateur d'OpenManage Integration for VMware vCenter.

1. Dans la page d'accueil du VMware vCenter, cliquez sur l'icône **OpenManage Integration**.
2. Dans **Navigateur**, sous **OpenManage Integration**, cliquez sur **Hôtes Dell EMC**.
3. Dans l'onglet **Hôtes Dell EMC**, affichez les informations suivantes :
 - **Nom d'hôte** : affiche un lien utilisant l'adresse IP de chaque hôte Dell EMC. Pour afficher les informations sur un hôte Dell EMC, cliquez sur le lien de cet hôte.
 - **vCenter** : affiche l'adresse IP du vCenter correspondant à cet hôte Dell EMC.
 - **Cluster** : affiche le nom du cluster, si l'hôte Dell EMC est dans un cluster.

- **Profil de connexion** : affiche le nom du profil de connexion.

Affichage de l'onglet des licences OpenManage Integration for VMware vCenter

Lors de l'installation de la licence OpenManage Integration for VMware vCenter, le nombre d'hôtes et de serveurs vCenter pris en charge s'affiche dans cet onglet. La version d'OpenManage Integration for VMware vCenter s'affiche également au haut de la page.

La page sous Gestion des licences affiche le lien **Acheter une licence**.

La section **Gestion des licences** affiche :

- **Portail des licences de produit (Locker numérique)**
- **Portail des licences iDRAC**
- **Console Administration**

L'onglet **Licences** d'OpenManage Integration for VMware vCenter affiche les éléments suivants :

Informations sur l'onglet Gestion des licences	Description
Licences hôtes	<ul style="list-style-type: none"> · Licences disponibles Affiche le nombre de licences disponibles · Licences utilisées Affiche le nombre de licences en cours d'utilisation
Licences vCenter	<ul style="list-style-type: none"> · Licences disponibles Affiche le nombre de licences disponibles · Licences utilisées Affiche le nombre de licences en cours d'utilisation

Accès à l'aide et au support

L'onglet **Aide et support** d'OpenManage Integration for VMware vCenter fournit des informations utiles sur votre produit. Vous y trouvez les informations suivantes :

Tableau 5. Informations indiquées dans l'onglet Aide et support

Nom	Description
Aide relative au produit	Fournit les liens suivants : <ul style="list-style-type: none"> · Aide d'OpenManage Integration for VMware vCenter - Fournit un lien vers l'aide du produit, qui se trouve à l'intérieur du produit. Utilisez la table des matières ou recherchez les informations souhaitées. · À propos : ce lien affiche la boîte de dialogue Informations sur la version. Vous pouvez voir le numéro de version du produit ici.
Manuels Dell EMC	Fournit des liens actifs aux éléments suivants : <ul style="list-style-type: none"> · Manuels de serveur · Manuels OpenManage Integration for VMware vCenter
Console Administration	Fournit un lien vers la Console Administration.
Aide et support supplémentaires	Fournit des liens actifs aux éléments suivants :

Nom	Description
	<ul style="list-style-type: none"> · Manuels iDRAC avec Lifecycle Controller · Documentation Dell VMware · Page de produits OpenManage Integration for VMware vCenter · Accueil de l'Aide et du support Dell · Dell TechCenter
Conseils concernant les appels au service de support	Offre des conseils sur la façon de contacter Dell Support et l'acheminement correct des appels.
Ensemble de dépannage	Fournit un lien permettant de créer et télécharger l'ensemble de dépannage. Vous pouvez fournir ou afficher ce lot lorsque vous contactez le support technique. Pour plus d'informations, voir Téléchargement du lot de dépannage .
Dell EMC recommande	Fournit un lien vers Dell EMC Repository Manager (DRM). Utiliser DRM pour rechercher et télécharger toutes les mises à jour du micrologiciel disponibles pour votre système.
Réinitialisation d'iDRAC	Fournit un lien de réinitialisation d'iDRAC à utiliser lorsque l'iDRAC ne répond pas. Cette réinitialisation entraîne un redémarrage normal du contrôleur iDRAC.

Téléchargement du lot de dépannage

REMARQUE : Pour générer le lot de dépannage, assurez-vous que vous vous connectez à vSphere Web Client en tant qu'utilisateur avec autorisation d'accès en écriture sur OMIVV.

Vous pouvez utiliser les informations du lot de dépannage pour vous aider au dépannage ou envoyer les informations au support technique. Pour afficher les informations de dépannage, procédez comme suit :

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Aide et support**.
2. Sous **Lot de dépannage**, cliquez sur **Créer et télécharger un lot de dépannage**.
3. Cliquez sur le bouton **Créer**.
4. Pour enregistrer le fichier, cliquez sur **Télécharger**.
5. Dans la boîte de dialogue **Téléchargement de fichier**, cliquez sur **Enregistrer**.
6. Dans la boîte de dialogue **Enregistrer sous**, naviguez jusqu'à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.
7. Pour quitter, cliquez sur **Fermer**.

Réinitialisation d'iDRAC

Le lien de réinitialisation du contrôleur iDRAC se trouve dans l'onglet **Aide et support**. La réinitialisation du contrôleur iDRAC entraîne un redémarrage normal de celui-ci. Ce redémarrage n'entraîne cependant pas le redémarrage de l'hôte. Il faut jusqu'à 2 minutes pour que le bon fonctionnement soit rétabli après une réinitialisation. Utilisez cette réinitialisation lorsque le contrôleur iDRAC ne répond pas dans OpenManage Integration for VMware vCenter.

REMARQUE : Dell vous recommande de placer l'hôte en mode Maintenance avant de réinitialiser l'iDRAC. Vous pouvez effectuer la réinitialisation sur un hôte qui fait partie d'un profil de connexion et a été inventorié au moins une fois. L'action de réinitialisation peut ne pas rendre l'iDRAC de nouveau utilisable. Dans un tel scénario, une réinitialisation matérielle est obligatoire. Pour en savoir plus sur la réinitialisation matérielle, voir la documentation de l'iDRAC.

Lors de la réinitialisation de l'iDRAC, vous pouvez afficher les éléments suivants :

- Un léger délai ou une erreur de communication alors que l'OpenManage Integration for VMware vCenter obtient son état d'intégrité.
- La fermeture de toutes les sessions ouvertes avec l'iDRAC.
- La modification de l'adresse DHCP pour l'iDRAC.

Si l'iDRAC utilise DHCP pour son adresse IP, l'adresse IP peut changer. Si l'adresse IP change, réexécutez la tâche d'inventaire des hôtes pour capturer la nouvelle adresse IP d'iDRAC dans les données d'inventaire.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Aide et support**.
2. Sous Réinitialisation d'iDRAC, cliquez sur **Réinitialiser l'iDRAC**.
3. Dans la boîte de dialogue **Réinitialiser l'iDRAC**, sous Réinitialiser l'iDRAC, saisissez l'adresse IP/le nom de l'hôte.
4. Pour confirmer que vous comprenez bien le processus de réinitialisation de l'iDRAC, sélectionnez l'option **Je comprends la réinitialisation d'iDRAC. Poursuivre la réinitialisation de l'iDRAC**.
5. Cliquez sur **Réinitialiser l'iDRAC**.

Ouverture de l'aide en ligne

Vous pouvez ouvrir l'aide en ligne à partir de l'onglet **Aide et support**. Vous pouvez rechercher le document d'aide pour comprendre un sujet ou pour trouver une procédure.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Aide et support**, sous **Aide relative aux produits**, cliquez sur **Aide relative à OpenManage Integration for VMware vCenter**.
Le contenu de l'aide en ligne s'affiche dans la fenêtre du navigateur.
2. Utilisez la table des matières du volet gauche ou recherchez le sujet souhaité.
3. Pour fermer l'aide en ligne, cliquez sur **X** dans le coin supérieur droit de la fenêtre du navigateur.

Lancement de la Console Administration

Vous pouvez démarrer OpenManage Integration for VMware vCenter à partir du client Web VMware vCenter et ouvrir la Console Administration à partir de l'onglet **Aide et support**.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Aide et support** puis, sous **Console Administration**, cliquez sur le lien vers la console.
2. Dans la boîte de dialogue de connexion **Console Administration**, utilisez le mot de passe de l'administrateur pour ouvrir une session.
Vous pouvez effectuer les opérations suivantes dans la Console Administration :
 - Enregistrer ou annuler l'enregistrement d'un vCenter, modifier des informations d'identification ou mettre à jour un certificat.
 - Télécharger la licence.
 - Afficher le récapitulatif indiquant le nombre de vCenters enregistrés et disponibles ainsi que le nombre maximum de licences d'hôtes en cours d'utilisation et disponibles.
 - Redémarrer l'appliance virtuelle.
 - Effectuer une mise à jour ou une mise à niveau vers la version la plus récente.
 - Afficher les paramètres réseau (mode lecture seule).
 - Configurer les paramètres de proxy HTTP qui permettent de se connecter au serveur Dell EMC pour mettre à niveau l'appliance ou à des fins de connectivité à <http://downloads.dell.com/published/Pages/index.html>.
 - Configurer des paramètres NTP, qui vous permettent d'activer ou de désactiver le serveur NTP et de configurer des serveurs NTP préférés et secondaires.
 - Générer une requête de signature de certificat (CSR), télécharger un certificat ou restaurer le certificat par défaut pour les certificats HTTPS.
 - Configurer les paramètres globaux afin de définir le stockage des alertes pour toutes les instances de vCenter. Vous pouvez configurer le nombre maximal d'alertes à stocker, le nombre de jours de conservation de ces alertes et le délai de duplication des alertes.
 - Configurer les paramètres globaux afin de définir le stockage des alertes pour toutes les instances de vCenter.
 - Lancer une sauvegarde ou une restauration.
 - Configurer l'emplacement de sauvegarde sur un partage réseau et le mot de passe de cryptage des fichiers sauvegardés (ainsi que le test de la connexion réseau).
 - Planifier une sauvegarde récurrente.

Affichage de l'historique des journaux

La page des journaux vous permet de consulter les journaux générés par OMIVV.

Vous pouvez filtrer et trier le contenu de cette page à l'aide des deux listes déroulantes disponibles. La première liste déroulante vous permet de filtrer et d'afficher les détails des journaux en fonction des types suivants :

- Toutes les catégories
- Informatif
- Avertissement

- Erreur

La seconde liste déroulante vous permet de trier les détails des journaux selon la fréquence :

- La semaine dernière
- Le mois dernier
- L'année dernière
- Plage personnalisée
 - Si vous sélectionnez **Plage personnalisée**, vous pouvez préciser la date de début et de fin en fonction de ce que vous souhaitez filtrer, puis cliquer sur **Appliquer**.

Le tableau de grille présente les informations suivantes :

- Catégorie : affiche le type de catégorie de journal.
- Date et heure : affiche les date et heure des actions utilisateur.
- Description : affiche la description de l'action utilisateur.

Vous pouvez trier les colonnes de la grille de données par ordre ascendant ou descendant en cliquant sur l'en-tête de la colonne. Utilisez la zone de texte **Filtre** pour effectuer des recherches dans le contenu. Les informations suivantes s'affichent en bas de la grille des pages :

Tableau 6. Historique du journal


Informations de journal	Description
Nombre total d'éléments	Affiche le nombre total de tous les éléments de journal
Éléments par écran	Affiche le nombre d'éléments de journal sur la page affichée. Utilisez la zone déroulante pour définir le nombre d'éléments par page.
Page	Affiche la page sur laquelle vous vous trouvez. Vous pouvez également saisir un numéro de page dans la zone de texte ou utiliser les boutons Précédent et Suivant pour accéder à la page de votre choix.
Boutons Précédent et Suivant	Vous guide vers les pages précédentes ou suivantes
Icône Exporter tout	Exporte le contenu du journal dans un fichier CSV

Affichage des journaux

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Dans l'onglet **Journal**, affichez les journaux des actions utilisateur impliquant OpenManage Integration for VMware vCenter. Pour plus d'informations sur les journaux affichés, reportez-vous à l'[Historique du journal](#).
3. Pour trier les données de la grille, cliquez sur un en-tête de colonne.
4. Pour trier par catégorie ou bloc de temps, utilisez les listes déroulantes précédant la grille.
5. Pour naviguer d'une page des éléments du journal à l'autre, utilisez les boutons **Précédent** et **Suivant**.

Exportation des fichiers journaux

L'OpenManage Integration for VMware vCenter utilise un fichier de valeurs séparées par des virgules (CSV) pour l'exportation d'informations depuis les tables de données.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Pour exporter le contenu des journaux au format CSV, cliquez dans le coin inférieur droit de l'écran sur l'icône .
3. Dans la boîte de dialogue **Sélectionner l'emplacement de téléchargement**, naviguez jusqu'à l'emplacement d'enregistrement des informations de journal.
4. Dans la zone de texte **Nom de fichier**, acceptez le nom par défaut `ExportList.csv` ou saisissez le nom de fichier de votre choix suivi de l'extension `.CSV`.
5. Cliquez sur **Enregistrer**.

Gestion des licences d'OpenManage Integration for VMware vCenter

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

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

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

Les licences offrent les informations suivantes :

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

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

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

Sujets :


- [Achat et chargement d'une licence logicielle](#)

Achat et chargement d'une licence logicielle

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

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

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

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

Configuration d'appliance pour VMware vCenter

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

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

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

REMARQUE : Les deux méthodes utilisent une interface utilisateur similaire.

Sujets :

- [Tâches de configuration via l'Assistant Configuration](#)
- [Tâches de configuration via l'onglet Paramètres](#)

Tâches de configuration via l'Assistant Configuration

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

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

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

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

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

1. Dans le client Web vSphere, cliquez sur **Accueil**, puis sur l'icône **OpenManage Integration**.
Pour accéder à l'Assistant Configuration initiale, vous pouvez utiliser l'une des méthodes suivantes :
 - Lorsque vous cliquez sur l'icône **OpenManage Integration** pour la première fois, l'**Assistant Configuration initiale** s'affiche automatiquement.
 - Depuis **OpenManage Integration > Mise en route**, cliquez sur **Démarrer l'Assistant Configuration initiale**.
2. Dans la boîte de dialogue **Accueil**, examinez les étapes, puis cliquez sur **Suivant**.

Sélection de vCenters

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

- un vCenter particulier
- Tous les vCenters enregistrés

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

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

Sélectionnez un vCenter parmi ceux qui ne sont pas encore configurés ou sélectionnez un vCenter que vous venez d'ajouter à votre environnement. La page Sélection de vCenter vous permet de sélectionner un ou plusieurs vCenters pour en configurer les paramètres.

3. Pour continuer et afficher la boîte de dialogue **Description du profil de connexion**, cliquez sur **Suivant**.

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

Création d'un profil de connexion

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

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

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

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

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

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

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

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

- Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
- Pour ne pas stocker le certificat iDRAC et en effectuer la vérification au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.

4. Dans **Racine hôte**, effectuez l'une des opérations suivantes :

- Dans le cas des hôtes déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, sélectionnez **Utiliser Active Directory** et effectuez les opérations suivantes ; sinon, configurez les informations d'identification de l'hôte :

- a. Dans **Nom d'utilisateur** Active Directory, saisissez le nom de l'utilisateur. Saisissez le nom d'utilisateur au format `domaine \nom_utilisateur` ou `nom_utilisateur@domaine`. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères.

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

Exigences pour le nom d'utilisateur d'hôte :

- **Entre 1 et 64 caractères**
- **Aucun caractère non imprimable**
- **Pas de caractères non valides, tels que " / \ [] ; | = , + * ? < > @**

Exigences pour le domaine d'hôte :

- **Entre 1 et 64 caractères**
- **Le premier caractère doit être alphabétique.**
- **Ne peut pas contenir d'espace.**
- **Pas de caractères non valides, tels que " / \ [] ; | = , + * ? < > @**

- b. Dans **Mot de passe** Active Directory, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.

- c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.

- d. Effectuez l'une des actions suivantes :

- Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
- Pour ne pas stocker le certificat iDRAC et en effectuer la vérification au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.

- Pour configurer les informations d'identification de l'hôte sans Active Directory, procédez comme suit :

- a. Dans **Nom d'utilisateur**, le nom d'utilisateur est `root`. Il s'agit du nom d'utilisateur par défaut et vous ne pouvez pas le modifier. Toutefois, si l'option Active Directory est configurée, vous pouvez choisir n'importe quel utilisateur Active Directory au lieu de racine.

- b. Dans la zone de texte **Mot de passe**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.

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

- c. Dans **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.

- d. Effectuez l'une des actions suivantes :

- Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
- Pour ne pas stocker le certificat iDRAC et effectuer la vérification du certificat au cours de toutes les futures connexions, désélectionnez **Activer la vérification du certificat**.

5. Cliquez sur **Suivant**.

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

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

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

REMARQUE : Le test de connexion échoue pour tous les hôtes exécutant ESXi 6.5 et/ou une version ultérieure dont le service WBEM est désactivé. Pour ces hôtes, le service WBEM est automatiquement activé lorsque vous effectuez l'inventaire sur ces hôtes. Bien que le test de connexion échoue, nous vous recommandons de terminer les actions de l'Assistant Profil de connexion, d'exécuter l'inventaire sur les hôtes, puis d'effectuer à nouveau le test de profil de connexion.

8. Pour terminer la création du profil, cliquez sur **Suivant**.

Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis l'Assistant. Vous pouvez modifier ou créer d'autres profils de connexion pour ce serveur vCenter depuis la page **Gérer > Profils de connexion** après avoir exécuté l'Assistant Configuration. Voir la rubrique **Modification d'un profil de connexion** dans ce guide..

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

Une fois les hôtes ajoutés au profil de connexion, l'adresse IP d'OMIVV est automatiquement définie sur la destination d'interruption SNMP de l'iDRAC de l'hôte et OMIVV active automatiquement le service WBEM pour les hôtes ESXi 6.5. OMIVV utilise le service WBEM pour synchroniser correctement les relations de l'hôte ESXi et du contrôleur iDRAC. Si la configuration de la destination d'interruption SNMP échoue et/ou l'activation du service WBEM échoue pour certains hôtes, ceux-ci sont répertoriés comme non conformes. Pour afficher les hôtes non conformes qui nécessitent une destination d'interruption SNMP pour être reconfigurés et/ou des services WBEM pour être activés, voir la rubrique [Rapport et résolution de conformité des hôtes vSphere](#).

Planification des tâches d'inventaire

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

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

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

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

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

Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis cet Assistant. Vous pouvez modifier les détails de planification de l'inventaire des hôtes depuis l'onglet **Gérer > Paramètres** après avoir terminé la configuration depuis l'Assistant Configuration. Voir [Modification des planifications de tâche d'inventaire](#)

Exécution de tâches de récupération de la garantie

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

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

1. Dans la boîte de dialogue **Planification de garantie**, sélectionnez **Activer la récupération des données de garantie**.
2. Dans **Planification de la récupération des données de garantie**, procédez comme suit :
 - a) Cochez la case en regard de chaque jour de la semaine pendant lequel vous voulez exécuter l'inventaire.
 - b) Entrez l'heure au format HH:MM.
L'heure entrée est votre heure locale. Par conséquent, si vous voulez exécuter l'inventaire dans le fuseau horaire de l'appliance virtuelle, calculez le décalage horaire entre votre fuseau horaire local et celui de l'appliance virtuelle, puis entrez l'heure de manière appropriée.
3. Pour enregistrer vos modifications et continuer, cliquez sur **Suivant** afin de poursuivre le paramétrage des **Événements et alarmes**. Une fois que vous avez cliqué sur Suivant, tous les détails que vous fournissez sont enregistrés et vous ne pouvez pas les modifier depuis l'Assistant. Vous ne pourrez modifier les planifications de tâches de garantie qu'à l'issue de l'exécution de l'Assistant de configuration, à partir de l'onglet **Paramètres**. Voir [Modification des planifications de tâche de garantie](#)

Configuration des événements et alarmes

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

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

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

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

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

REMARQUE : Cette opération ne peut être effectuée que si vous sélectionnez **Activer les alarmes d'hôtes Dell EMC**.
4. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell EMC, cliquez sur **Restaurer les alarmes par défaut**.
Il peut s'écouler une minute avant que le changement prenne effet.

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

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

Tâches de configuration via l'onglet Paramètres

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

- Activer le lien OMSA. Voir [Activation du lien OMSA](#).
- Configurer les paramètres de notification d'expiration de la garantie. Voir [Configuration des paramètres de notification d'expiration de la garantie](#).
- Configurer l'espace de stockage de mise à jour du micrologiciel. Voir [Configuration de l'espace de stockage de mise à jour du micrologiciel](#).
- Configurer les notifications de la dernière version de l'appliance. Voir [Configuration des notifications de la dernière version de l'appliance](#).


- Configurer et afficher les événements et alarmes. Voir [Configuration des événements et alarmes](#).
- Afficher les planifications de récupération des données pour l'inventaire et la garantie. Voir [Affichage des planifications de récupération des données pour l'inventaire et la garantie](#).

Paramètres d'appliance

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


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


Configuration des paramètres de notification d'expiration de la garantie


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


Configuration du référentiel de mise à jour du micrologiciel

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

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

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

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

 **REMARQUE** : Assurez-vous que vous utilisez la version la plus récente de Dell EMC Repository Manager (DRM) version (3.0) et versions ultérieures.
3. Si vous sélectionnez **Dossier de réseau partagé**, renseignez le champ **Emplacement du fichier de catalogue** en respectant le format suivant :

- Partage NFS pour le fichier XML : host:/share/filename.xml
- Partage NFS pour le fichier gz : host:/share/filename.gz
- Partage CIFS pour le fichier XML : \\host\share\filename.xml
- Partage CIFS pour le fichier gz : \\host\share\filename.gz

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


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

4. Une fois le téléchargement terminé, cliquez sur **Appliquer**.

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

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


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

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

Configuration des informations d'identification pour le déploiement

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

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

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer** > **Paramètres**, sous **Paramètres d'appliance** à droite de **Informations d'identification pour le déploiement**, puis cliquez sur l'icône  .
2. Dans **Informations d'identification pour déployer un serveur sans système d'exploitation**, sous **Informations d'identification**, saisissez les valeurs suivantes :
 - Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
Le nom d'utilisateur doit comporter 16 caractères maximum (uniquement des caractères ASCII imprimables)
 - Dans la zone de texte **Mot de passe**, entrez le mot de passe.
Le mot de passe doit comporter 20 caractères maximum (uniquement des caractères ASCII imprimables)
 - Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe.

Assurez-vous que les mots de passe sont identiques.

3. Pour enregistrer les informations d'identification spécifiées, cliquez sur **Appliquer**.

Paramètres vCenter


Dans cette section, configurez les paramètres vCenter suivants :

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

Activation du lien OMSA

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

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

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

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


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

Configuration des événements et alarmes



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

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

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

1. Dans l'onglet **Gérer > Paramètres** sous **Paramètres vCenter** d'OpenManage Integration for VMware vCenter, développez **Événements et alarmes**.
Les **Alarmes vCenter concernant les hôtes Dell EMC** actuelles (activées ou désactivées) ou toutes les alarmes vCenter et le **Niveau de publication d'événement** sont affichés.
2. Cliquez sur l'icône  située à droite de l'en-tête **Événements et alarmes**.
3. Pour activer tous les événements et alarmes relatifs au matériel, sélectionnez **Activer les alarmes pour tous les hôtes Dell EMC**.
REMARQUE : Les hôtes Dell EMC pour lesquels des alarmes sont activées répondent aux événements critiques en passant en mode maintenance, et vous pouvez alors modifier l'alarme si nécessaire.
4. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell gérés, cliquez sur **Restaurer les alarmes par défaut**.



Cette étape peut prendre jusqu'à une minute avant que le changement soit appliqué. Par ailleurs, elle est uniquement disponible si **Activer les alarmes d'hôtes Dell EMC** est sélectionné.

5. Dans **Niveau de publication d'événement**, sélectionnez soit « Ne pas publier d'événements », « Publier tous les événements », « Publier uniquement les événements de type Critique et Avertissement » ou « Publier uniquement les événements de type Critique et Avertissement concernant la virtualisation ». Pour plus d'informations, voir la section sur la [surveillance des événements, des alarmes et de l'intégrité](#).
6. Pour appliquer ces paramètres à tous les vCenters, sélectionnez **Appliquer ces paramètres à tous les vCenters**.
 -  **REMARQUE :** Si vous sélectionnez cette option, tous les paramètres existants pour tous les vCenters sont ignorés.
 -  **REMARQUE :** Cette option n'est pas disponible si vous avez déjà sélectionné Tous les vCenters enregistrés dans la liste déroulante dans l'onglet Paramètres.
7. Pour enregistrer les valeurs, cliquez sur **Appliquer**.

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

1. Dans OpenManage Integration for VMware vCenter, sous l'onglet **Gérer > Paramètres**, sous **Paramètres vCenter**, cliquez sur **Planification de récupération des données**.
En cliquant sur Planification de récupération des données, vous développez l'affichage et les options de modification des données d'inventaire et de garantie apparaissent.
2. Cliquez sur l'icône  en regard de **Récupération des données d'inventaire** ou de **Récupération des données de garantie**. La boîte de dialogue **Récupération des données d'inventaire/de garantie** vous permet de consulter les informations suivantes pour la récupération des données d'inventaire ou de garantie :
 - L'option de récupération d'inventaire et/ou de garantie option est-elle activée ou désactivée ?
 - Les jours de la semaine pour lesquels l'option est activée.
 - L'heure pour laquelle l'option est activée.
3. Pour modifier les planifications de récupération des données, voir [Modification des planifications de tâches d'inventaire](#) ou [Modification des planifications de tâches de garantie](#).
4. Cliquez de nouveau sur **Planification de récupération des données** pour masquer les planifications d'inventaire et de garantie et afficher une seule ligne.

Configuration de la chaîne de communauté d'interruption SNMP

1. Dans la page **OpenManage Integration for VMware vCenter**, sous l'onglet **Gérer > Paramètres**, sous **Paramètres d'appliance**, cliquez sur l'icône  en regard de la **Chaîne de communauté d'interruption SNMP OMSA**. La boîte de dialogue **Paramètres de chaîne de communauté d'interruption SNMP OMSA** s'affiche. Par défaut, la chaîne de communauté d'interruption SNMP est configurée sur **public**.
2. Vous pouvez modifier le texte **public** comme vous le voulez, puis cliquez sur **Appliquer**.
 -  **REMARQUE :** La configuration de la chaîne de communauté d'interruption SNMP pour les serveurs PowerEdge de 11e génération est définie lors de l'installation ou de la mise à niveau d'OMSA via OMIVV.

Utilisation de l'onglet Ligne de base

Vous pouvez utiliser l'onglet Ligne de base pour créer un profil de logithèque et un profil de cluster.

Sujets :



- Profil de logithèque
- Création d'un profil de logithèque
- Modification d'un profil de logithèque
- Suppression d'un profil de logithèque
- Profil de cluster
- Création d'un profil de cluster
- Modification du profil de cluster
- Suppression d'un profil de cluster

Profil de logithèque

Le profil de logithèque vous permet de créer ou de gérer plusieurs profils de logithèque de micrologiciels ou de pilotes. Ces profils de logithèque de pilotes ou de micrologiciels peuvent être utilisés dans :


- Profil de ligne de base pour identifier la dérive pour le cluster vSAN.
- Mettez à jour le pilote ou le micrologiciel pour les clusters vSAN ou les nœuds de cluster vSAN.

REMARQUE :


- **Utilisez un catalogue de micrologiciels personnalisé créé spécifiquement pour vos environnements vSAN.**
- **Un profil de logithèque de pilotes peut posséder un maximum de 10 pilotes.**
 -  **REMARQUE :** Assurez-vous de ne pas disposer de plus de 10 lots hors ligne (fichiers .zip). Si vous avez plus de 10 fichiers, la sélection de pilotes est aléatoire.
- **Pour le profil de logithèque de pilotes, seuls les pilotes asynchrones au format VIB provenant de lots hors ligne sont utilisés (fichiers .zip).**
 -  **REMARQUE :** Seuls les pilotes VIB asynchrones nécessaires validés par rapport aux exigences vSAN. Pour plus d'informations, voir la Matrice de compatibilité matérielle VMware.
- **Pour le profil de logithèque de pilotes OMIVV requiert un accès écrit au partage CIFS ou NFS.**
- **Pour le profil de logithèque de pilotes, les fichiers dans les sous-dossiers ou les fichiers d'une taille supérieure à 10 Mo sont ignorés.**
- **Une fois l'analyse réussie uniquement, les profils de logithèque sont disponibles pour être utilisés dans le Profil de ligne de base ou pour exécuter une tâche de mise à jour du pilote ou du micrologiciel vSAN.**
- **Si plusieurs versions du micrologiciel sont disponibles, la version la plus récente est toujours utilisée pour la comparaison de conformité.**


Pour lancer la page du profil de logithèque, procédez comme suit :

1. Sur la page **Intégration OpenManage pour VMware vCenter** cliquez sur l'onglet **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de logithèque**.
 - a. Sur la page **Profil de logithèque**, affichez la liste des profils de logithèque que vous avez créés.
Un tableau s'affiche, répertoriant les profils de logithèque avec le **Nom du profil**, la **Description**, le **Type**, le **Chemin de partage**, l'**Heure de la dernière mise à jour réussie** et l'**État de la dernière actualisation**.
 - b. Pour afficher plus d'informations sur un profil de logithèque, sélectionnez le profil de logithèque souhaité.
Vérifiez les informations du profil de logithèque qui s'affichent comme **Nom de profil**, **Chemin de partage**, **Date de création**, **Date de modification** et **Dernière modification par**.
 - c. Pour permuter les colonnes dans la grille de données, faites glisser les colonnes dans la grille de données.


- d. Pour filtrer ou effectuer une recherche dans le contenu de la grille de données, saisissez les critères de filtre dans le champ **Filtre**.
- e. Pour exporter les informations du profil système vers un fichier .CSV, sélectionnez un profil de logithèque, puis cliquez sur  dans le coin droit de la grille de données.



Création d'un profil de logithèque

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de logithèque**.
 2. Cliquez sur .
 3. Sur la page **d'accueil**, lisez les instructions, puis cliquez sur **Suivant** pour ajouter plus d'informations :
 - a. Dans la boîte de dialogue **Nom du profil**, saisissez le nouveau nom du profil de logithèque.
 - b. Dans le champ **Description du profil**, saisissez une description (facultatif).
 - c. Cliquez sur **Suivant**.
 4. Dans la boîte de dialogue **Paramètres du profil**, sélectionnez un des types de logithèques suivants :
 - Micrologiciel (par défaut, cette option est sélectionnée)
 - Pilote
 - a. Dans le champ **Emplacement de partage de logithèque**, saisissez l'emplacement de partage de logithèque (CIFS ou NFS).
 - b. Pour un partage CIFS, saisissez le nom d'utilisateur et le mot de passe. Les caractères qui ne sont pas autorisés pour le mot de passe sont : &, !, @, % et <.


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

 - c. Pour valider l'accès pour le chemin d'accès à la logithèque en question et l'existence du fichier de catalogue pour la logithèque de micrologiciels et de pilotes, cliquez sur **Démarrer le test**. Cette validation est obligatoire pour continuer.

 : indique que le test de la connexion a réussi.

 : indique que le test de la connexion a échoué.
 - d. Cliquez sur **Suivant**.
-  **REMARQUE : Pour la logithèque de pilotes, téléchargez les fichiers .zip du pilote hors ligne, enregistrez-les dans l'emplacement partagé et indiquez le chemin complet de l'emplacement partagé. OMIVV crée automatiquement le catalogue dans l'appliance OMIVV. Les lots de pilotes VIB sont disponibles sur <https://my.vmware.com/web/vmware/downloads>.**
5. Cliquez sur **Suivant**.
La page **Récapitulatif** s'affiche. Elle contient les informations concernant le profil de logithèque.
 6. Cliquez sur **Terminer**.
Après la création du catalogue, le téléchargement et l'analyse du catalogue commencent et l'état s'affiche sur la page d'accueil du profil de logithèque.
Les profils de logithèque analysés avec succès sont disponibles pendant la création du profil de cluster et pendant la mise à jour du micrologiciel vSAN.

Modification d'un profil de logithèque

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de logithèque**.
2. Sélectionnez un profil de logithèque à modifier, puis cliquez sur .
3. Sur l'Assistant **Profil de logithèque**, vous pouvez modifier le **nom du profil** et la **Description**, qui est facultative, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Paramètres du profil**, procédez comme suit :
 - a) Vous pouvez modifier les informations d'identification CIFS.
 - b) Pour valider l'accès pour le chemin d'accès à la logithèque en question et l'existence du fichier de catalogue pour la logithèque de micrologiciels et de pilotes, cliquez sur **Démarrer le test**. Cette validation est obligatoire pour continuer.



: indique que le test de la connexion a réussi.



: indique que le test de la connexion a échoué.

- c) Pour actualiser la logithèque avec le contenu le plus récent dans l'emplacement spécifié, cliquez sur **Synchroniser avec l'emplacement de la logithèque**.



REMARQUE : L'option *Synchroniser avec l'emplacement de la logithèque* est sélectionnée par défaut. Assurez-vous que cette option est sélectionnée si vous souhaitez recréer le catalogue à partir du dernier catalogue de pilotes ou de micrologiciels (emplacement de partage).

5. Cliquez sur **Suivant**.
La page **Récapitulatif** s'affiche. Elle contient les informations concernant le profil de logithèque.
6. Cliquez sur **Terminer**.

Suppression d'un profil de logithèque

Avant de supprimer le profil de logithèque, assurez-vous de dissocier le profil de logithèque des profils de cluster associés.

1. Sur la page **Intégration OpenManage pour VMware vCenter** cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de logithèque**.
2. Sélectionnez le profil de logithèque à supprimer, puis cliquez sur **X**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui** pour supprimer le profil ou sur **Non** pour annuler la suppression.

Profil de cluster


Le profil de cluster vous permet de capturer la configuration de base telle que la configuration matérielle (pour les serveurs de 14e génération uniquement), les versions du micrologiciel ou du pilote et de maintenir l'état souhaité des clusters vSAN en identifiant la dérive par rapport à la ligne de base.

REMARQUE :

- **Les profils de logithèque de micrologiciels et de pilotes doivent être analysés après leur création avant d'être utilisés dans une création du profil de cluster.**
- **Une fois que le profil de cluster est créé, il déclenche la tâche Détection de dérive.**
- **Lorsqu'un cluster est associé à un profil de cluster, il remplace les associations de profils de cluster précédentes.**

Pour lancer la page du profil de cluster, effectuez les étapes suivantes :

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur l'onglet **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de cluster**.
 - a. Sur la page **Profil de cluster**, affichez la liste des profils de cluster que vous avez créés.
Un tableau s'affiche, répertoriant les profils de cluster avec le **Nom du profil**, la **Description**, le **Profil système associé**, le **profil de logithèque de micrologiciels associé**, le **profil de logithèque de pilotes associé** et l'**Heure de la dernière mise à jour réussie**.

REMARQUE : Si la dernière version d'un profil de logithèque est disponible pour un profil de cluster existant, un symbole d'avertissement s'affiche à côté du profil de micrologiciel ou de pilote associé.
 - b. Pour afficher plus d'informations sur un profil de cluster, sélectionnez le profil de cluster souhaité.
Affichez les informations de profil de cluster qui affichent les détails : **Nom de profil**, **Date de création**, **Date de modification** et **Dernière modification par**.
 - c. Pour permuter les colonnes dans la grille de données, faites glisser les colonnes dans la grille de données.
 - d. Pour filtrer ou effectuer une recherche dans le contenu de la grille de données, utilisez **Filtre**.
 - e. Pour exporter les informations du profil de logithèque vers un fichier .CSV, sélectionnez un profil de logithèque, puis cliquez sur  dans le coin droit de la grille de données.

Création d'un profil de cluster

1. Profil du système, profil de logithèque pour le micrologiciel et les pilotes, modèles de serveurs homogènes pour le cluster.
2. Le cluster vSAN doit être présent dans le vCenter.
3. Le profil de connexion doit être créé pour au moins un hôte dans le cluster vSAN et l'inventaire doit être exécuté avec succès.

REMARQUE : Si plusieurs vCenters autonomes sont enregistrés auprès d'OMIVV, nous vous recommandons de créer différents profils de cluster pour chaque vCenter.

REMARQUE : Lors de la création du profil de cluster, un instantané actuel de la logithèque de micrologiciels et de pilotes associée est créé pour la ligne de base. Si les logithèques changent, le profil de cluster devra être mis à jour à nouveau pour tenir compte des changements. Dans le cas contraire, toute mise à jour effectuée sur les logithèques ne sera pas actualisée avec l'instantané de profil de cluster d'origine.

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de cluster**.
2. Cliquez sur **+**.
3. Sur la page **d'accueil**, lisez les instructions, puis cliquez sur **Suivant** pour ajouter plus d'informations :
 - a) Dans le champ **Nom du profil**, saisissez le nom du profil de cluster.
 - b) Dans le champ **Description du profil**, saisissez la description du profil de cluster. La description du profil est facultative.
 - c) Cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Paramètres du profil**, procédez comme suit :
 - a) Sélectionnez le profil système, ou le profil de logithèque (profil de logithèque de micrologiciels ou profil de logithèque de pilotes), ou ses combinaisons.

REMARQUE : Le profil du système s'applique uniquement aux serveurs de 14^e génération.


REMARQUE : Dell EMC vous recommande de créer une ligne de base avec la logithèque Profil de système, micrologiciel et pilote.
 - b) Cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Association de profil**, procédez comme suit :
 - a) Sélectionnez le serveur vCenter souhaité dans la liste déroulante.
 - b) Cliquez sur **Parcourir** pour associer les clusters vSAN requis.
 - c) Cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Programmation des détections de dérive**, définissez le jour et l'heure, puis cliquez sur **Suivant**.
La page **Récapitulatif** s'affiche. Elle contient les informations concernant le profil de cluster.
7. Cliquez sur **Terminer**.

Le profil de cluster est enregistré automatiquement et s'affiche sur la page **Profil de cluster**.

REMARQUE : La tâche de détection de dérive s'exécute immédiatement après que le profil de cluster est enregistré et s'exécute pendant la période planifiée.

Modification du profil de cluster

REMARQUE : Modifier le profil de cluster modifie la ligne de base, ce qui peut entraîner un nouveau calcul du niveau de conformité.

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de cluster**.
2. Sélectionnez un profil de cluster que vous souhaitez modifier, puis cliquez sur .
3. Sur l'Assistant **profil de cluster**, vous pouvez modifier la **Description**, qui est facultative, puis cliquer sur **Suivant**.

REMARQUE : Vous ne pouvez pas modifier le nom du profil.

4. Dans la boîte de dialogue **Paramètres de profil**, vous pouvez modifier les combinaisons du profil.
5. Dans la boîte de dialogue **Association de profil**, vous pouvez modifier les associations et configurations requises dans le profil de cluster.

6. Dans la boîte de dialogue **Configuration de profil**, vous pouvez modifier la **programmation de détection de dérive**, puis cliquer sur **Suivant**.


La page **Récapitulatif** s'affiche. Elle contient la mise à jour des informations sur le profil de cluster.

7. Cliquez sur **Terminer**.

Le profil mis à jour est enregistré automatiquement et s'affiche dans les profils de cluster.

 **REMARQUE** : La tâche de détection de dérive s'exécute immédiatement après que le profil de cluster est enregistré et s'exécute pendant la période planifiée.

Suppression d'un profil de cluster

1. Sur la page **Intégration OpenManage pour VMware vCenter**, cliquez sur **Gérer > Ligne de base**, développez **Info ligne de base**, puis cliquez sur **Profil de cluster**.
2. Sélectionnez un profil de cluster que vous souhaitez supprimer, cliquez sur .
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui** pour supprimer le profil ou sur **Non** pour annuler la suppression. Si le profil de cluster est supprimé, la tâche de détection de dérive correspondante est également supprimée.

À propos des profils de connexion

L'onglet **Profils de connexion** permet de gérer et de configurer les profils de connexion qui contiennent des informations d'identification actuellement utilisées par l'appliance virtuelle pour communiquer avec les serveurs Dell. Associez chaque serveur Dell EMC à un seul profil de connexion pour la gestion par OpenManage Integration for VMware vCenter. Vous pouvez attribuer plusieurs serveurs à un même profil de connexion. Après avoir exécuté l'**Assistant Configuration initiale**, vous pouvez gérer le profil de connexion depuis OpenManage Integration for VMware vCenter, en effectuant les tâches suivantes :

- [Affichage d'un profil de connexion](#)
- [Création d'un profil de connexion](#)
- [Modification d'un profil de connexion](#)
- [Suppression d'un profil de connexion](#)
- [Test d'un profil de connexion](#)

Affichage d'un profil de connexion

Un profil de connexion doit être créé, et/ou doit exister pour pouvoir s'afficher. Lorsqu'un ou plusieurs profils de connexion ont été créés, ils s'affichent sur la page **Profils de connexion**. OpenManage Integration for VMware vCenter utilise les informations d'identification fournies dans les profils pour communiquer avec les hôtes Dell EMC.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils** puis cliquez sur **Profils de référence**.
3. Développez la section **Profils de référence** et cliquez sur l'onglet **Profils de connexion**.

Vous pouvez afficher tous les profils de connexion que vous avez créés.

Tableau 7. Informations relatives aux profils de connexion

Champs relatifs au profil de connexion	Description
Nom du profil	Affiche le nom du profil de connexion
Description	Affiche une description, si elle est fournie.
vCenter	Affiche le nom de domaine complet (FQDN), le nom d'hôte ou l'adresse IP du vCenter, selon le contexte.
Hôtes associés	Une liste des hôtes associés au profil de connexion Si plus d'un, utilisez l'icône développer pour afficher toutes les.
Vérification de certificat iDRAC	Indique si la vérification de certificat iDRAC est activée ou non.
Vérification de certificat racine d'hôte	Indique si la vérification de certificat racine d'hôte est activée ou non.
Date de création	Affiche la date à laquelle le profil de connexion a été créé.
Date de modification	Affiche la date à laquelle le profil de connexion a été modifié.
Dernière modification par	Affiche les détails de l'utilisateur qui a modifié le profil de connexion.

Création d'un profil de connexion

Vous pouvez attribuer plusieurs serveurs à un même profil de connexion. Pour créer un profil de connexion, procédez comme suit :

REMARQUE : Les vCenters qui s'affichent pendant la procédure ont été authentifiés à l'aide de l'authentification unique (SSO). Si vous ne voyez pas d'hôte vCenter, il est possible qu'il soit sur une SSO différente ou que vous utilisiez une version de VMware vCenter antérieure à la version 5.5.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer** → **Profils** → **Profils de référence** → **Profils de connexion**, et cliquez sur **+**.
2. Lisez les instructions indiquées dans la page **Bienvenue**, puis cliquez sur **Suivant**.
3. Sur la page **Profil de connexion**, entrez les informations suivantes :

- a) Sous **Profil**, saisissez le **Nom du profil** et éventuellement une **Description**.
- b) Sous **vCenter**, sélectionnez dans la liste déroulante les serveurs vCenter dans lesquels le profil sera créé. Cette option vous permet de créer un profil de connexion pour chaque serveur vCenter.
- c) Dans la zone **Informations d'identification iDRAC**, effectuez l'une des tâches suivantes :

REMARQUE : Le compte iDRAC exige que l'utilisateur détienne des droits d'administration pour mettre à jour le micrologiciel, appliquer des profils matériels et déployer un hyperviseur.

- Dans le cas des iDRAC déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, sélectionnez **Utiliser Active Directory** ; sinon, passez à l'option suivante.
 - Dans la zone de texte **Nom d'utilisateur Active Directory**, saisissez le nom d'utilisateur. Saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine`. 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.
 - Dans la zone de texte **Mot de passe Active Directory**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
 - Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**.
 - Pour vérifier le certificat iDRAC, sélectionnez l'une des options suivantes :
 - Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
 - Pour ne procéder à aucune vérification et ne pas stocker le certificat, désélectionnez **Activer la vérification du certificat**.
- Pour configurer les informations d'identification iDRAC sans Active Directory, effectuez les opérations suivantes :
 - Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur. Le nom d'utilisateur ne doit pas comporter plus de 16 caractères. Pour en savoir plus sur les restrictions de nom d'utilisateur de votre version d'iDRAC, voir la documentation iDRAC.

REMARQUE : Le compte local iDRAC exige des droits d'administration pour la mise à jour des logiciels, l'application de profils matériels et le déploiement d'hyperviseur.

- Dans la zone de texte **Mot de passe**, entrez le mot de passe. Le mot de passe ne doit pas comporter plus de 20 caractères.
 - Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**.
 - Pour vérifier le certificat iDRAC, sélectionnez l'une des options suivantes :
 - Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
 - Pour ne procéder à aucune vérification et ne pas stocker le certificat, ne sélectionnez pas **Activer la vérification du certificat**.
- d) Dans la zone **Racine hôte**, effectuez l'une des tâches suivantes :
- Dans le cas des hôtes déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; sinon, passez à la configuration des informations d'identification de l'hôte.
 - Dans la zone de texte **Nom d'utilisateur Active Directory**, saisissez le nom d'utilisateur. Saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine`. 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.
 - Dans la zone de texte **Mot de passe Active Directory**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
 - Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**.
 - Pour vérifier le certificat, sélectionnez l'une des options suivantes :
 - Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.

- Pour ne procéder à aucune vérification et ne pas stocker le certificat de l'hôte, ne sélectionnez pas **Activer la vérification du certificat**.
 - Pour configurer les informations d'identification de l'hôte sans Active Directory, procédez comme suit :
 - Dans la zone de texte **Nom d'utilisateur**, le nom d'utilisateur est root.
- Le nom de l'utilisateur root est le nom d'utilisateur par défaut et vous ne pouvez pas le modifier.


REMARQUE : Si l'option Active Directory est configurée, vous pouvez choisir n'importe quel nom d'utilisateur Active Directory au lieu de root.

- Dans la zone de texte **Mot de passe**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
- Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**.
- Pour vérifier le certificat, sélectionnez l'une des options suivantes :
 - Pour télécharger et stocker le certificat de l'hôte et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
 - Pour ne procéder à aucune vérification et ne pas stocker le certificat de l'hôte, ne sélectionnez pas **Activer la vérification du certificat**.

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

4. Cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Sélectionner les hôtes**, choisissez les hôtes à associer à ce profil de connexion et cliquez sur **OK**.
6. Sur la page **Hôtes associés**, ajoutez un ou plusieurs hôtes au profil de connexion, si nécessaire.

Pour ajouter des hôtes, cliquez sur **+**, sélectionnez des hôtes, puis cliquez sur **OK**.

7. Pour tester le profil de connexion, sélectionnez un ou plusieurs hôtes, puis cliquez sur l'icône .

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

REMARQUE : Le test de connexion échoue pour tous les hôtes exécutant ESXi 6.5 et/ou une version ultérieure dont le service WBEM est désactivé. Pour ces hôtes, le service WBEM est automatiquement activé lorsque vous effectuez l'inventaire sur ces hôtes. Bien que le test de connexion échoue, nous vous recommandons de terminer les actions de l'Assistant Profil de connexion, d'exécuter l'inventaire sur les hôtes, puis d'effectuer à nouveau le test de profil de connexion.

8. Pour terminer la création du profil, cliquez sur **Suivant**.
Pour les serveurs non dotés de carte iDRAC Express ou Enterprise, le résultat du test de connexion iDRAC affiche **Non applicable** pour ce système.

Une fois les hôtes ajoutés au profil de connexion, l'adresse IP d'OMIVV est automatiquement définie sur la destination d'interruption SNMP de l'iDRAC de l'hôte et OMIVV active automatiquement le service WBEM pour les hôtes ESXi 6.5. OMIVV utilise le service WBEM pour synchroniser correctement les relations de l'hôte ESXi et du contrôleur iDRAC. Si la configuration de la destination d'interruption SNMP échoue et/ou l'activation du service WBEM échoue pour certains hôtes, ceux-ci sont répertoriés comme non conformes. Pour afficher les hôtes non conformes nécessitant la reconfiguration de la destination d'interruption SNMP et/ou l'activation du service WBEM, voir [Exécution de l'Assistant Correction des hôtes vSphere non conformes](#).




Modification d'un profil de connexion

Après avoir créé un profil de connexion, vous pouvez modifier le nom du profil, la description, les hôtes et l'iDRAC associés, ainsi que les informations d'identification des hôtes.

REMARQUE : Les vCenters qui s'affichent pendant la procédure ont été authentifiés à l'aide de l'authentification unique (SSO). Si vous ne voyez pas d'hôte vCenter, il est possible qu'il soit sur une SSO différente ou que vous utilisiez une version de VMware vCenter antérieure à la version 5.5.

REMARQUE : Assurez-vous de ne pas mettre à jour un profil de connexion lorsqu'une tâche d'inventaire, de garantie ou de déploiement est en cours d'exécution.

REMARQUE : Assurez-vous de ne pas déplacer un hôte associé à un profil de connexion sur un autre profil de connexion ni de supprimer un hôte d'un profil de connexion lorsqu'une tâche d'inventaire, de garantie ou de déploiement est en cours d'exécution.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
 2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.
 3. Développez **Profils de référence**, puis cliquez sur **Profils de connexion**.
 4. Sélectionnez un profil et cliquez sur .
 5. Dans l'onglet **Bienvenue** de la fenêtre **Profil de connexion**, lisez les informations, puis cliquez sur **Suivant**.
 6. Dans l'onglet **Nom et informations d'identification**, procédez comme suit :
 - a. Sous **Profil**, saisissez le **Nom du profil** et éventuellement une **Description**.
 - b. Sous **vCenter**, affichez les hôtes associés pour ce profil de connexion. Voir ci-dessus la remarque concernant l'affichage des hôtes ici.
 - c. Dans la zone **Informations d'identification pour l'iDRAC**, effectuez l'une des opérations suivantes :
 - Pour les comptes iDRAC qui sont déjà configurés et activés pour Active Directory et sur lesquels vous souhaitez utiliser Active Directory, sélectionnez **Utiliser Active Directory**.
 - Dans la zone de texte **Nom d'utilisateur Active Directory**, saisissez le nom d'utilisateur. Saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou `domaine/nom_utilisateur` ou `nom_utilisateur@domaine`. 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.
 - Dans la zone de texte **Mot de passe Active Directory**, saisissez le mot de passe. Celui-ci ne doit pas comporter plus de 127 caractères.
 - Saisissez de nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**.
 - Pour vérifier le certificat, sélectionnez l'une des options suivantes :
 - Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**.
 - Pour ne procéder à aucune vérification et ne pas stocker le certificat, ne sélectionnez pas **Activer la vérification du certificat**.
 - Pour configurer les informations d'identification iDRAC sans Active Directory, renseignez les champs suivants :
 - **Nom d'utilisateur** : saisissez le nom d'utilisateur au format `domaine\nom_utilisateur` ou `domaine@nom_utilisateur`.
Les caractères autorisés pour le nom d'utilisateur sont les suivants : / (barre oblique), & (esperluette), \ (barre oblique inverse), . (point), " (guillemet), @ (arobase), % (pourcentage) (127 caractères au maximum).
Le nom de domaine peut contenir des caractères alphanumériques, tels que - (tiret) et . (point) (254 caractères au maximum). Le premier et le dernier caractères du nom de domaine doivent être alphanumériques.
 - **Mot de passe** : saisissez le mot de passe.
Les caractères suivants sont interdits dans le mot de passe : / (barre oblique), & (esperluette), \ (barre oblique inverse), . (point), " (guillemet).
 - **Vérifier le mot de passe** : saisissez de nouveau votre mot de passe.
 - **Activer la vérification du certificat** : par défaut, la case est décochée. Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**. Pour ne procéder à aucune vérification et ne pas stocker le certificat, ne cochez pas la case **Activer la vérification du certificat**.
-  **REMARQUE : Sélectionnez Activer la vérification du certificat si vous utilisez Active Directory.**
- d. Sous **Racine de l'hôte**, procédez comme suit :
 - Pour accéder à toutes les consoles associées à Active Directory, cochez la case **Utiliser Active Directory**.
 - **Nom d'utilisateur** : le nom d'utilisateur par défaut est racine et ne peut pas être modifié. Si l'option **Utilisation d'Active Directory** est sélectionnée, utilisez n'importe quel nom d'utilisateur d'Active Directory.
 -  **REMARQUE : Le nom d'utilisateur est racine et cette entrée ne peut pas être modifiée si vous ne sélectionnez pas l'option Utilisation d'Active Directory. Il n'est pas obligatoire d'utiliser les informations d'identification racine pour l'utilisateur de l'iDRAC et il peut s'agir d'un privilège d'administrateur si Active Directory est configuré.**
 - **Mot de passe** : saisissez le mot de passe.
Les caractères suivants sont interdits dans le mot de passe : / (barre oblique), & (esperluette), \ (barre oblique inverse), . (point), " (guillemet).
 - **Vérifier le mot de passe** : saisissez de nouveau votre mot de passe.
 - **Activer la vérification du certificat** : par défaut, la case est décochée. Pour télécharger et stocker le certificat iDRAC et le valider au cours de connexions futures, sélectionnez **Activer la vérification du certificat**. Pour ne procéder à aucune vérification et ne pas stocker le certificat, ne cochez pas la case **Activer la vérification du certificat**.

 **REMARQUE :** Sélectionnez Activer la vérification du certificat si vous utilisez Active Directory.

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

 **REMARQUE :** Pour les serveurs sans carte iDRAC Express ou Enterprise, le résultat du test de connexion iDRAC affiche Non applicable pour ce système.

7. Cliquez sur **Suivant**.

8. Dans la boîte de dialogue **Sélectionner les hôtes**, choisissez les hôtes à associer à ce profil de connexion.

9. Cliquez sur **OK**.


La boîte de dialogue **Hôtes associés** vous permet de tester les informations d'identification pour l'iDRAC et les hôtes sur les serveurs sélectionnés.

10. Effectuez l'une des opérations suivantes :

- Pour créer un profil de connexion sans tester les informations d'identification, cliquez sur **Terminer**.
- Pour lancer le test, sélectionnez les hôtes à vérifier, puis cliquez sur l'icône




. Les autres options sont inactives.


 **REMARQUE :** Le test de connexion échoue pour tous les hôtes exécutant ESXi 6.5 et/ou une version ultérieure dont le service WBEM est désactivé. Pour ces hôtes, le service WBEM est automatiquement activé lorsque vous effectuez l'inventaire sur ces hôtes. Bien que le test de connexion échoue, nous vous recommandons de terminer les actions de l'Assistant Profil de connexion, d'exécuter l'inventaire sur les hôtes, puis d'effectuer à nouveau le test de profil de connexion.

Lorsque le test est terminé, cliquez sur **Terminer**.

- Pour arrêter les tests, cliquez sur **Annuler tous les tests**. Dans la boîte de dialogue **Annuler les tests**, cliquez sur **OK**, puis sur **Terminer**.

 **REMARQUE :** Les champs **Date de modification** et **Dernière modification** par incluent les modifications apportées à un profil de connexion via l'interface du client Web. Les modifications apportées au profil de connexion par l'appliance OMIVV n'affectent pas les détails de ces deux champs.

Suppression d'un profil de connexion

 **REMARQUE :** Assurez-vous de ne pas supprimer de profil de connexion associé à un hôte lorsqu'une tâche d'inventaire, de garantie ou de déploiement est en cours d'exécution.


1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.

2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.

3. Développez la section **Profils de référence**, cliquez sur l'onglet **Profils de connexion**, puis sélectionnez les profils à supprimer.

4. Cliquez sur .

5. Pour supprimer le profil, cliquez sur **Oui** pour répondre au message de confirmation de la suppression (ou sur **Non**, si vous souhaitez annuler cette action).

 **REMARQUE :** OMIVV ne gère pas les hôtes faisant partie du profil de connexion que vous avez supprimé, tant que ces hôtes ne sont pas ajoutés à un autre profil de connexion.

 **REMARQUE :** Avant de supprimer le profil de connexion, assurez-vous de supprimer la tâche de mise à jour du micrologiciel planifiée.

Test d'un profil de connexion

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.

2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.

3. Développez **Profils de référence**, cliquez sur l'onglet **Profils de connexion**, puis sélectionnez un profil de connexion.

4. Dans la boîte de dialogue **Tester le profil de connexion**, sélectionnez les hôtes à tester, puis cliquez sur l'icône .

Si vous ne sélectionnez pas de profil de connexion, l'exécution du test de connexion prendra un certain temps.

5. Pour abandonner tous les tests sélectionnés et annuler les tests, cliquez sur **Annuler tous les tests**. Dans la boîte de dialogue **Annuler les tests**, cliquez sur **OK**.
6. Pour quitter, cliquez sur **Annuler**.

À propos du profil de châssis

L'OMIVV peut surveiller tous les châssis Dell EMC associés aux serveurs Dell EMC. Un profil de châssis est requis pour surveiller le châssis. Vous pouvez gérer le profil de châssis en effectuant les tâches suivantes :

- Affichage du profil de châssis. Voir [Affichage du profil de châssis](#).
- Création d'un profil de châssis. Voir [Création d'un profil de châssis](#).
- Modification d'un profil de châssis. Voir [Modification d'un profil de châssis](#).
- Suppression d'un profil de châssis. Voir [Suppression d'un profil de châssis](#).
- Test d'un profil de châssis. Voir [Test d'un profil de châssis](#).

Affichage des profils de châssis

Avant d'afficher un profil de châssis, vérifiez qu'il existe. Si ce n'est pas le cas, créez-en un.

Lorsqu'un ou plusieurs profils de châssis ont été créés, vous pouvez les afficher sur la page Profils de châssis.


1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.
3. Développez **Profils de référence** et cliquez sur l'onglet **Profils de châssis**. Les profils de châssis s'affichent.
4. Pour afficher tous les châssis associés, cliquez sur l'icône  si plusieurs châssis sont associés au profil de châssis.
5. Dans la page **Profils de châssis**, consultez les informations sur les châssis.


Tableau 8. Informations des profils de châssis

Champs relatifs au châssis	Description
Nom du profil	Affiche le nom du profil de châssis.
Description	Affiche une description, si elle est fournie.
Adresse IP/Nom d'hôte du châssis	Affiche l'adresse IP ou le nom d'hôte du châssis.
Numéro de service du châssis	Affiche l'identificateur unique attribué à un châssis.
Date Modified (Date de modification)	Affiche la date à laquelle le profil de châssis a été modifié.

Création d'un profil de châssis

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

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

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

Dans la section **Nom et références**, sous **Profil de châssis** :

 - a. Dans la zone de texte **Nom de profil**, entrez le nom du profil.
 - b. Dans la zone de texte **Description**, entrez une description (facultatif).

Dans la section **Informations d'identification** :

 - a. Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur doté de privilèges d'administrateur, lequel est généralement utilisé pour se connecter au contrôleur CMC (Chassis Management Controller).

- b. Dans le champ **Mot de passe**, entrez le mot de passe correspondant au nom d'utilisateur spécifié.
- c. Dans la zone de texte **Vérifier le mot de passe**, entrez le même mot de passe que vous avez saisi dans la zone de texte **Mot de passe**. Les mots de passe doivent correspondre.

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

6. Cliquez sur **Suivant**.

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

REMARQUE : Les châssis ne sont détectés et associables au profil de châssis qu'après l'exécution réussie de l'inventaire d'un hôte modulaire présent sous ce châssis.

7. Pour sélectionner un châssis unique ou plusieurs châssis, cochez les cases correspondantes en regard de la colonne **Adresse IP/Nom d'hôte**.

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

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

8. Cliquez sur **OK**.


La page **Châssis associés** s'affiche.

9. Pour tester la connectivité du châssis, sélectionnez le châssis, puis cliquez sur l'icône  afin de vérifier les informations d'identification. Le résultat est indiqué dans la colonne **Résultat du test** par la mention **Réussite** ou **Échec**.

10. Pour terminer l'opération, cliquez sur **Terminer**.

Modification d'un profil de châssis


Après avoir créé un profil de châssis, vous pouvez modifier le nom du profil, la description, les châssis associés et les informations d'identification.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.
3. Développez la section **Profils de référence**, cliquez sur l'onglet **Profils du châssis**, puis sélectionnez un profil de châssis.
4. Cliquez sur l'icône  dans le menu principal. La fenêtre **Modifier le profil du châssis** s'affiche.
5. Dans la zone **Profil du châssis**, vous pouvez modifier le **Nom du profil** et, si vous souhaitez, la **Description**.
6. Dans la zone **Informations d'identification**, vous pouvez modifier les champs **Nom d'utilisateur**, **Mot de passe** et **Vérifier le mot de passe**.

Le mot de passe que vous tapez dans **Vérifier le mot** doit être identique au mot de passe saisi dans le champ **Mot de passe**. Les informations d'identification saisies doivent disposer de droits d'administrateur sur le châssis.

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

L'onglet **Châssis associé** vous permet de tester le châssis et les informations d'identification correspondant au châssis sélectionné. Effectuez l'une des opérations suivantes :




- Pour commencer le test, sélectionnez un seul ou plusieurs châssis à vérifier, puis cliquez sur l'icône . La colonne **Résultat du test** affiche si la connexion test a réussi ou non.
- Vous pouvez ajouter ou supprimer un ou plusieurs châssis dans un profil de châssis.

REMARQUE : Si les châssis ne sont pas inventoriés, seuls le nom IP/hôte et le numéro de service s'affichent. Les champs **Nom du châssis** et **Modèle** s'affichent une fois que le châssis est inventorié.


Suppression de profils de châssis

REMARQUE : Avant de supprimer le profil de châssis, assurez-vous que les instances du châssis ne font pas partie d'autres instances de vCenter, auprès desquelles est enregistré OMIVV.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.

3. Développez la section **Profils de référence**, puis cliquez sur l'onglet **Profils de châssis**.
 4. Sélectionnez le profil de châssis à supprimer, puis cliquez sur .
Un message d'avertissement s'affiche.
 5. Pour confirmer la suppression, cliquez sur **Oui**. Sinon, pour annuler la suppression, cliquez sur **Non**.
Si tous les châssis associés à un profil de châssis sont effacés ou déplacés vers d'autres profils, un message de confirmation de suppression s'affiche pour indiquer que le profil n'est plus associé à aucun châssis et qu'il va être supprimé. Pour supprimer le profil de châssis, cliquez sur **OK** dans le message de confirmation de suppression.
-  **REMARQUE : OMIVV ne surveille pas les châssis qui sont associés aux profils de châssis que vous avez supprimés, jusqu'à ce que ces châssis soient ajoutés à un autre profil de châssis.**
-  **REMARQUE : Si le profil de châssis est supprimé, ses données d'historique de garantie associées ne sont pas supprimées de l'historique de garantie.**

Test d'un profil de châssis

1. Dans OpenManage Integration for VMware vCenter, cliquez sur **Gérer**.
2. Cliquez sur **Profils**, puis cliquez sur **Profils de référence**.
3. Développez les **Profils de référence**, cliquez sur l'onglet **Profils de châssis**, puis sélectionnez un ou plusieurs profils de châssis à tester.
Cette opération peut prendre quelques minutes.
4. Dans la boîte de dialogue **Tester le profil de châssis**, sélectionnez le châssis que vous souhaitez tester et cliquez sur l'icône .
5. Pour abandonner tous les tests sélectionnés et annuler les tests, cliquez sur **Annuler tous les tests**. Dans la boîte de dialogue **Annuler les tests**, cliquez sur **OK**.
6. Pour quitter, cliquez sur **Annuler**.

- Gestion de l'inventaire et de la garantie

Une fois que vous avez configuré OMIVV, vous pouvez surveiller l'inventaire, les tâches de garantie, gérer les tâches de déploiement et de mise à jour de micrologiciel dans l'onglet **Surveiller**. L'inventaire et la garantie se définissent via l'**Assistant Configuration initiale** ou l'onglet **Paramètres**.

La page File d'attente des tâches permet de gérer les tâches suivantes :

- Affichage des tâches de mise à jour de micrologiciel ou de déploiement de serveur soumises.
- Actualisation des tâches de déploiement ou de mise à jour de micrologiciel ou des files d'attente de l'historique d'inventaire ou de garantie.
- Planification d'une tâche de garantie ou d'inventaire.
- Purge des entrées de la file d'attente des tâches de déploiement ou de mise à jour de micrologiciel.

REMARQUE : Pour veiller à ce que l'inventaire ou la garantie contienne des informations à jour, planifiez la tâche d'inventaire ou de garantie afin qu'elle s'exécute au moins une fois par semaine.

Les tâches que vous pouvez effectuer dans cette page comprennent :

- [Gestion des tâches de déploiement](#)
- [Gestion des tâches de mise à jour de micrologiciel](#)
- [Gestion des tâches d'inventaire](#)
- [Gestion des tâches de garantie](#)

REMARQUE : Pour toutes les tâches mentionnées, assurez-vous qu'elles ont été planifiées de nouveau si la date de l'apppliance a été modifiée à une date ultérieure et inversée.

REMARQUE : Pour la surveillance de l'intégrité basique, redémarrez l'apppliance OMIVV. Pour une surveillance de l'intégrité étendue, assurez-vous de désactiver la Surveillance étendue, puis activez-la à partir de la Console Administration OMIVV.

Sujets :

- [Tâches d'inventaire](#)
- [Tâches relatives à la garantie](#)
- [Surveillance d'un seul hôte](#)
- [Surveillance des hôtes sur des clusters et centres de données](#)
- [Configuration du clignotement du voyant d'un serveur physique](#)
- [Configuration du mode de verrouillage du système](#)

Tâches d'inventaire

Les tâches d'inventaire sont définies en utilisant l'onglet **Paramètres** ou l'**Assistant Configuration initiale**. Utilisez l'onglet **Historique d'inventaire** pour afficher toutes les tâches d'inventaire. Les tâches que vous pouvez effectuer dans cet onglet incluent :

- [Affichage de l'inventaire du châssis ou des hôtes](#)
- [Modification des planifications de tâche d'inventaire](#)
- [Exécution immédiate d'une tâche d'inventaire du châssis](#)

Affichage de l'inventaire de l'hôte

Un inventaire complet et réussi est nécessaire pour recueillir des données. Une fois l'inventaire terminé, vous pouvez en afficher les résultats pour l'ensemble du datacenter ou pour un système hôte particulier. Vous pouvez trier les colonnes de la vue d'inventaire dans l'ordre croissant et/ou décroissant.

REMARQUE : Il est parfois impossible de récupérer et d'afficher les données de l'hôte pour les raisons suivantes :

- L'hôte n'est associé à aucun profil de connexion, ce qui vous empêche d'exécuter la tâche d'inventaire.

- **Aucune tâche d'inventaire n'a été exécutée sur l'hôte pour collecter les données, si bien qu'il n'y a rien à afficher.**
- **Le nombre de licences hôte est dépassé, et vous devez vous procurer des licences supplémentaires pour exécuter la tâche d'inventaire.**
- **L'hôte n'a pas la licence iDRAC correcte et requise pour les serveurs PowerEdge de 12e génération et de générations ultérieures. Vous devez donc acheter les licences iDRAC adéquates.**
- **Les informations d'identification peuvent ne pas être correctes.**
- **L'hôte est peut-être inaccessible.**

Pour afficher les détails de l'inventaire de l'hôte :

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, développez **Historique d'inventaire**, puis cliquez sur **Inventaire des hôtes**. Les informations vCenter s'affichent sur la grille supérieure.
3. Pour afficher les informations d'hôte sur un vCenter sélectionné, choisissez un vCenter afin d'afficher tous les détails associés.
4. Passez en revue les informations d'inventaire de l'hôte.

Tableau 9. Informations sur l'hôte vCenter

vCenter	
vCenter	Affiche l'adresse de vCenter.
Hôtes testés OK	Affiche la liste des hôtes ayant réussi.
Dernier inventaire	Affiche la date et l'heure d'exécution de la dernière planification d'inventaire.
Inventaire suivant	Affiche la date et l'heure d'exécution de la prochaine planification d'inventaire.
Hôtes	
Hôte	Affiche l'adresse de l'hôte.
État	Affiche l'état. Les options possibles incluent : <ul style="list-style-type: none"> · Réussite · En panne · En cours · Planifié
Durée (MM:SS)	Affiche la durée de la tâche, en minutes et secondes
Date et heure de début	Affiche la date et l'heure de démarrage de la planification d'inventaire
Date et heure de fin	Affiche l'heure de fin de la planification d'inventaire

Affichage de l'inventaire du châssis

Un inventaire complet et réussi est nécessaire pour recueillir des données. Vous pouvez trier les colonnes de la vue d'inventaire dans l'ordre croissant et/ou décroissant.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, développez **Historique d'inventaire**, puis cliquez sur **Inventaire des châssis**.
3. Passez en revue les informations d'inventaire du châssis.

Tableau 10. Informations sur le châssis

Inventaire du châssis	
IP du châssis	Affiche l'adresse IP du châssis
Numéro de service	Affiche le numéro de service du châssis. Ce numéro de service est un identificateur unique fourni par le fabricant à des fins d'assistance et de maintenance

Inventaire du châssis	
État	Affiche l'état du châssis
Durée (MM:SS)	Affiche la durée de la tâche, en minutes et secondes
Date et heure de début	Affiche la date et l'heure de démarrage de la planification d'inventaire
Date et heure de fin	Affiche l'heure de fin de la planification d'inventaire

REMARQUE : L'inventaire du châssis n'est pas pris en charge sur les serveurs PowerEdge suivants : C6320P, C6320, C4130 et C6420.

Modification des planifications de tâche d'inventaire

Pour vous assurer que les informations sur les hôtes sont à jour, planifiez une tâche d'inventaire au moins une fois par semaine. Un inventaire consomme un minimum de ressources et ne dégrade pas les performances des hôtes. Vous pouvez modifier la planification des tâches d'inventaire à partir de l'**Assistant Configuration initiale** ou à partir de l'onglet **Surveiller**.

Le calendrier des tâches d'inventaire définit l'heure ou le jour d'exécution de tâches d'inventaire, telles que :

- De manière hebdomadaire, à une heure précise et certains jours.
- À un intervalle de temps défini.

Pour effectuer un inventaire sur les systèmes hôtes, créez un profil de connexion fournissant des informations de communication et d'authentification.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches, Historique d'inventaire**, puis cliquez sur **Inventaire des hôtes**.
3. Sélectionnez un vCenter, puis cliquez sur .
4. Dans la boîte de dialogue **Récupération des données d'inventaire**, procédez comme suit :
 - a) Sous **Données d'inventaire**, cochez la case **Activer la récupération des données d'inventaire**.
 - b) Sous **Planification de récupération des données d'inventaire**, sélectionnez les jours de la semaine d'exécution de votre tâche.
 - c) Dans la zone de texte **Heure de récupération des données d'inventaire**, saisissez l'heure locale de la tâche.
Il peut être nécessaire de prendre en compte le décalage horaire entre la configuration d'une tâche et la mise en œuvre d'une tâche.
5. Pour enregistrer les paramètres, cliquez sur **Appliquer**. Pour réinitialiser les paramètres, cliquez sur **Effacer**. Enfin, si vous souhaitez interrompre l'opération, cliquez sur **Annuler**.
6. Pour exécuter la tâche immédiatement à partir de l'OpenManage Integration for VMware vCenter, accédez à l'onglet **Surveiller** > **File d'attente des tâches**, puis cliquez sur **Historique d'inventaire** > **Inventaire des hôtes**.
7. Cliquez sur  puis, dans la boîte de dialogue **Succès**, cliquez sur **Fermer**.

REMARQUE : Lorsque vous exécutez l'inventaire d'hôtes modulaires, les châssis correspondants sont automatiquement détectés. L'inventaire de châssis s'exécute automatiquement après l'inventaire des hôtes si le châssis appartient déjà à un profil de châssis.

Une fois qu'une tâche d'inventaire est planifiée, cette tâche est placée dans la file d'attente. Vous ne pouvez pas exécuter un inventaire pour un seul hôte. Une tâche d'inventaire s'exécute pour tous les hôtes.

Exécution de tâches d'inventaire

1. Une fois l'**Assistant Configuration** exécuté, l'inventaire se déclenche automatiquement pour tous les hôtes ajoutés à un profil de connexion. Pour qu'un inventaire s'exécute ultérieurement, à la demande, cliquez sur **File d'attente des tâches** > **Inventaire** > **Exécuter maintenant** pour exécuter une tâche d'inventaire.
2. Pour afficher l'état de la tâche d'inventaire, cliquez sur **Actualiser**.
3. Accédez à la vue **Hôtes et clusters**, cliquez sur un **hôte Dell EMC**, puis cliquez sur l'onglet **OpenManage Integration**. Les informations suivantes devraient être disponibles :
 - Page Vue générale
 - Journal des événements système
 - Inventaire du matériel

- Stockage
- Micrologiciel
- Surveillance de l'alimentation

REMARQUE : Toute tâche d'inventaire des hôtes excédant la limite de licences sera ignorée et marquée comme **Échouée**.

Les commandes d'hôte suivantes fonctionnent au sein de l'onglet OpenManage Integration :


- Faire clignoter le voyant
- Exécuter l'Assistant Mise à jour du micrologiciel
- Lancer l'accès à distance
- Lancer OMSA
- Lancer CMC
- Configuration du mode de verrouillage du système

Exécution immédiate d'une tâche d'inventaire du châssis

Vous pouvez afficher et exécuter une tâche d'inventaire du châssis dans l'onglet **Inventaire du châssis**.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, **Historique de l'inventaire**, puis **Inventaire du châssis**.
La liste des châssis et leurs états s'affiche pour la dernière tâche d'inventaire.

REMARQUE : L'inventaire planifié du châssis est exécuté en même temps que l'inventaire planifié de l'hôte.

3. Cliquez sur .
Les listes de châssis inventoriés mis à jour sont affichées, avec, en regard de chaque châssis, leur état (**Réussite** ou **Échec**).

Tâches relatives à la garantie

Les informations sur la garantie du matériel sont récupérées en ligne auprès de Dell et sont affichées par OMIVV. Le numéro de service du serveur permet de récupérer des informations sur la garantie du serveur. Les tâches de récupération des données de garantie sont configurées à l'aide de l'**Assistant Configuration initiale**.

Les tâches que vous pouvez réaliser dans cet onglet incluent :

- [Affichage de l'historique de garantie](#)
- [Modification d'un calendrier des tâches de garantie](#)
- [Exécution immédiate d'une tâche de garantie des hôtes](#)
- [Exécution immédiate d'une tâche de garantie du châssis](#)

Affichage de l'historique de garantie

Une tâche de garantie est une tâche planifiée qui consiste à obtenir des informations de garantie depuis le site `support.dell.com` sur tous les systèmes. Vous pouvez trier les colonnes de la vue d'inventaire dans l'ordre croissant et/ou décroissant.

REMARQUE : L'appliance OMIVV nécessite une connexion Internet pour extraire les informations de garantie. Assurez-vous que votre appliance OMIVV dispose d'une connexion Internet. En fonction des paramètres réseau, les informations du proxy peuvent être requises par OMIVV pour accéder à Internet et récupérer les informations de garantie. Les détails du proxy peuvent être mis à jour dans la console d'administration. Voir la section [Configuration du proxy HTTP](#).

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, puis cliquez sur **Historique de garantie**.
3. Développez l'**historique de la garantie** pour afficher la **Garantie des hôtes** et la **Garantie du châssis**.
4. Pour afficher les informations correspondant à votre historique des tâches de garantie, sélectionnez **Garantie des hôtes**, puis choisissez un serveur vCenter afin d'afficher les détails des hôtes associés.

Tableau 11. Informations d'historique sur vCenter et les hôtes

Historique vCenter	
vCenters	Affiche la liste des vCenters

Historique vCenter	
Hôtes testés OK	Affiche le nombre d'hôtes vCenter qui ont réussi le test
Dernière garantie	Indique la date et l'heure d'exécution de la dernière tâche de garantie
Garantie suivante	Indique la date et l'heure d'exécution de la prochaine tâche de garantie
Historique des hôtes	
Hôte	Affiche l'adresse de l'hôte
État	Affiche l'état. Les options possibles incluent : <ul style="list-style-type: none"> · Réussite · En échec · En cours · Planifié
Durée (MM:SS)	Affiche la durée de la tâche de garantie, au format MM:SS
Date et heure de début	Indique la date et l'heure de démarrage de la tâche de garantie
Date et heure de fin	Indique l'heure de fin de la tâche de garantie

Affichage de la garantie du châssis

Une tâche de garantie est une tâche planifiée qui consiste à obtenir des informations de garantie depuis le site `support.dell.com` sur tous les systèmes. Vous pouvez trier les colonnes de la vue d'inventaire dans l'ordre croissant et/ou décroissant.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, puis cliquez sur **Historique de garantie**.
3. Développez l'**historique de la garantie** pour afficher la **Garantie des hôtes** et la **Garantie du châssis**.
4. Cliquez sur **Garantie du châssis**.
5. Affichez les détails de la garantie du châssis.


Tableau 12. informations sur le châssis

Historique du châssis	
IP du châssis	Affiche l'adresse IP du châssis
Service Tag	Affiche le numéro de service du châssis. Ce numéro de service est un identificateur unique fourni par le fabricant pour permettre au client d'obtenir des services d'assistance et de maintenance.
État	Affiche l'état du châssis
Durée (MM:SS)	Affiche la durée de la tâche de garantie, au format MM:SS
Date et heure de début	Indique la date et l'heure de démarrage de la tâche de garantie
Date et heure de fin	Indique l'heure de fin de la tâche de garantie

Modification des planifications de tâche de garantie


Les tâches de garantie sont configurées à l'origine dans l'**Assistant de configuration initiale**. Vous pouvez modifier la programmation des tâches de garantie à partir de l'onglet **Paramètres**.


1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, puis cliquez sur **Historique de garantie**.
3. Développez l'**historique de la garantie** pour afficher la **Garantie des hôtes** et la **Garantie du châssis**.
4. Pour afficher les informations correspondant à votre historique des tâches de garantie, sélectionnez **Garantie des hôtes** ou **Garantie du châssis**.

5. Cliquez sur .
6. Dans la boîte de dialogue **Récupération des données de garantie**, procédez comme suit :
 - a) Sous **Données de garantie**, cochez la case **Activer la récupération des données de garantie**.
 - b) Sous **Planification de récupération des données de garantie**, sélectionnez les jours de la semaine pendant lesquels vous souhaitez que la tâche de garantie soit exécutée.
 - c) Dans la zone de texte **Heure de récupération des données de garantie**, saisissez l'heure locale à laquelle vous souhaitez que cette tâche soit exécutée.
Vous pouvez être obligé de calculer le décalage horaire requis pour exécuter la tâche au moment approprié.
7. Cliquez sur **Appliquer**.

Exécution immédiate d'une tâche de garantie des hôtes


Exécutez une tâche de garantie au moins une fois par semaine.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Surveiller**.
2. Cliquez sur **File d'attente des tâches**, puis cliquez sur **Historique de garantie**.
3. Développez l'**historique de la garantie** pour afficher la **Garantie des hôtes** et la **Garantie du châssis**.
4. Pour afficher les informations correspondant à votre historique des tâches de garantie, sélectionnez **Garantie des hôtes** ou **Garantie du châssis**.
5. Sélectionnez la tâche de garantie que vous souhaitez exécuter, puis cliquez sur .
6. Dans la boîte de dialogue **Réussite**, cliquez sur **Fermer**.
La tâche de garantie figure à présent dans la file d'attente.

 **REMARQUE :** La garantie du châssis est exécutée automatiquement pour tous les châssis une fois la garantie de l'hôte exécutée. Dans un environnement SSO 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 manuellement.

Exécution immédiate d'une tâche de garantie du châssis

Exécutez une tâche de garantie au moins une fois par semaine.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Surveiller** > **File d'attente des tâches**.
2. Pour sélectionner la tâche de garantie que vous souhaitez exécuter, cliquez sur **Historique de garantie**, puis sur **Garantie du châssis**.
3. Cliquez sur .
4. Dans la boîte de dialogue **Réussite**, cliquez sur **Fermer**.
La tâche de garantie figure à présent dans la file d'attente.

Surveillance d'un seul hôte

OpenManage Integration for VMware vCenter vous permet d'afficher des informations détaillées sur un hôte particulier. Vous pouvez accéder aux hôtes dans VMware vCenter à partir du volet Navigateur, qui affiche les hôtes de tous les fournisseurs. Pour afficher plus d'informations détaillées, cliquez sur un hôte Dell EMC spécifique. Pour afficher la liste des hôtes Dell EMC, dans OpenManage Integration for VMware vCenter, cliquez sur **Hôtes Dell EMC** dans le volet Navigateur.

Affichage des détails récapitulatifs de l'hôte

Vous pouvez afficher les détails de récapitulatif d'un hôte individuel sur la page **Récapitulatif de l'hôte**, où divers portlets sont affichés. Deux de ces portlets sont applicables à OpenManage Integration for VMware vCenter. Les deux portlets sont les suivants :

- Intégrité de l'hôte Dell EMC
- Informations sur l'hôte Dell EMC

Vous pouvez faire glisser et déposer les deux portlets à l'emplacement de votre choix et vous pouvez formater et personnaliser les deux portlets comme les autres portlets, selon vos besoins. Pour afficher les détails de récapitulatif de l'hôte :

1. Dans Dell OpenManage Integration for VMware vCenter, dans le volet Navigateur, cliquez sur **Hôtes**.
2. Dans l'onglet **Objets**, sélectionnez l'hôte spécifique à passer en revue.

3. Cliquez sur l'onglet **Récapitulatif**.
4. Affichez les détails de récapitulatif de l'hôte :

Tableau 13. Informations de récapitulatif de l'hôte

Informations	Description
Système alternatif	Affiche les alertes pour OpenManage Integration for VMware vCenter dans une zone jaune sous la zone d'état et avant les portlets.
Zone de notification	Affiche les informations d'intégration de produits Dell dans la zone du panneau de droite, où vous pouvez trouver des informations sur les éléments suivants : <ul style="list-style-type: none"> · Tâches récentes · Travail en cours · Alarmes Les informations d'alarmes Dell s'affichent dans le portlet de la zone de notification.

5. Faites défiler l'affichage pour voir le portlet Dell EMC Server Management.

Tableau 14. Portlet Dell EMC Server Management

Informations	Description
Numéro de service	Affiche le numéro de service du serveur PowerEdge. Utilisez ce numéro lorsque vous faites appel au support.
Nom du modèle	Affiche le nom de modèle du serveur.
Mémoire résistante aux pannes	Affiche l'état de l'attribut BIOS. L'attribut BIOS est activé dans le BIOS au cours de la configuration initiale du serveur et affiche le mode opérationnel de la mémoire du serveur. Redémarrez le système si vous changez la valeur du mode opérationnel de la mémoire. Ceci s'applique aux serveurs PowerEdge de 12e génération et de générations ultérieures prenant en charge l'option Mémoire résistante aux pannes (FRM) et exécutant ESXi version 5.5 ou ultérieure. Les quatre différentes valeurs d'attribut du BIOS sont les suivantes : <ul style="list-style-type: none"> · Activé et protégé : cette valeur indique que le système est pris en charge, que le système d'exploitation est de version ESXi 5.5 ou ultérieure et que le mode opérationnel de la mémoire dans le BIOS est défini sur FRM. · NUMA activé et protégé : cette valeur indique que le système est pris en charge, que le système d'exploitation est de version ESXi 5.5 ou ultérieure et que le mode opérationnel de la mémoire dans le BIOS est défini sur NUMA. · Activé et non protégé : cette valeur indique que les systèmes dotés de système d'exploitation de version inférieure à ESXi 5.5 sont pris en charge. · Désactivé : cette valeur indique que les systèmes valides dotés d'un système d'exploitation de n'importe quelle version sont pris en charge et que le mode opérationnel de la mémoire dans le BIOS n'est pas défini sur FRM. · Vide : si le mode opérationnel de la mémoire dans le BIOS n'est pas pris en charge, l'attribut FRM ne s'affiche pas.
Mode de verrouillage du système	Affiche l'état du mode de verrouillage de l'iDRAC pour les serveurs PowerEdge de 14e génération. Le mode de verrouillage de l'iDRAC activé est représenté par un verrou fermé et le mode de verrouillage désactivé est représenté par un verrou ouvert.
Identification	Affiche les éléments suivants :

Informations	Description
	<ul style="list-style-type: none"> Nom d'hôte : affiche le nom de l'hôte Dell EMC État d'alimentation : indique si l'alimentation est sous tension (ON) ou hors tension (OFF) IP de l'iDRAC : affiche l'adresse IP de l'iDRAC IP de gestion : affiche l'adresse IP de gestion Profil de connexion : affiche le nom du profil de connexion de cet hôte Modèle : indique le modèle du serveur Dell EMC Numéro de service : affiche le numéro de service du serveur Numéro d'inventaire : affiche le numéro d'inventaire Jours de garantie restants : affiche le nombre de jours de garantie restant Analyse du dernier inventaire : affiche le jour, la date et l'heure du dernier balayage de l'inventaire
Hyperviseur et micrologiciel	<p>Affiche les éléments suivants :</p> <ul style="list-style-type: none"> Hyperviseur : affiche la version de l'hyperviseur Version du BIOS : affiche la version du BIOS Version de la carte d'accès à distance : affiche la version de la carte d'accès à distance
Consoles de gestion	<p>Les consoles de gestion sont utilisées pour lancer des consoles de gestion de systèmes externes, telles que :</p> <ul style="list-style-type: none"> Lancement de la console Remote Access Console (iDRAC) : lance l'interface utilisateur Web d'iDRAC (Integrated Dell Remote Access Controller). Lancement de la console OMSA : lance la console OMSA pour accéder à l'interface utilisateur d'OpenManage Server Administrator.
Actions de l'hôte	<p>Configurez le serveur physique pour qu'il clignote à différents intervalles de temps. Voir Indicateur de clignotement.</p>

6. Afficher le portlet Intégrité de l'hôte Dell EMC :

Tableau 15. Intégrité de l'hôte Dell EMC

Informations	Description
Intégrité de l'hôte Dell EMC	<p>L'intégrité des composants est une représentation graphique de l'état des composants principaux du serveur hôte : état global du serveur, serveur, bloc d'alimentation, température, tensions, processeurs, batteries, intrusion, journaux de matériel, gestion de l'alimentation, alimentation et mémoire. Les paramètres d'intégrité du châssis s'appliquent aux modèles VRTX version 1.0 et versions ultérieures, M1000e version 4.4 et versions ultérieures. Pour les versions inférieures à 4.3, seuls deux voyants d'intégrité sont affichés, à savoir Intègre et Avertissement ou Critique (triangle inversé avec point d'exclamation orange). L'intégrité globale indique l'intégrité basée sur le châssis doté du nombre de paramètre d'intégrité le plus bas. Les options possibles incluent :</p> <ul style="list-style-type: none"> Intègre (coche verte) : le composant fonctionne normalement Avertissement (triangle jaune avec point d'exclamation) : le composant est affecté d'une erreur non critique. Critique (X rouge) : le composant est affecté d'une panne critique. Inconnu (point d'interrogation) : l'état du composant est inconnu.

Par exemple, s'il existe cinq signes d'intégrité et un signe d'avertissement, le symbole d'intégrité globale correspond à Avertissement.

REMARQUE : Pour les blocs d'alimentation câblés, la surveillance de l'alimentation n'est pas disponible dans OMIVV.

Affichage des détails matériels d'un seul hôte

Vous pouvez afficher les détails matériels d'un hôte dans l'onglet **Informations sur les hôtes Dell EMC**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les vues Matériel signalent directement les données de l'agent OMSA et du contrôleur iDRAC. Voir la section [Exécution des tâches d'inventaire](#).

1. Dans OpenManage Integration for VMware vCenter, dans le Navigateur, cliquez sur **Hôtes**.
2. Dans l'onglet **Hôte**, sélectionnez l'hôte spécifique dont vous voulez afficher le matériel : détails de <Component Name>.
3. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur l'hôte Dell EMC**.

REMARQUE : Si l'option **Mode de verrouillage du système est activée pour l'hôte de 14e génération, une bande jaune s'affiche dans la partie supérieure avec une icône représentant un cadenas fermé.**

Dans le sous-onglet Matériel : <Component Name>, affichez les informations suivantes pour chaque composant.

Tableau 16. Informations sur le matériel d'un seul hôte

Matériel : <i>Composant</i>	Informations
Matériel : unité remplaçable	<ul style="list-style-type: none"> • Nom de pièce : affiche le nom de pièce de l'unité remplaçable • Numéro de pièce : affiche le numéro de pièce de l'unité remplaçable • Fabricant : affiche le nom du fabricant • Numéro de série : affiche le numéro de série du fabricant • Date de fabrication : affiche la date de fabrication
Matériel : processeur	<ul style="list-style-type: none"> • Socket : affiche le numéro de logement • Vitesse : affiche la vitesse actuelle • Marque : affiche la marque du processeur • Versión : affiche la version du processeur • Cœurs : affiche le nombre de cœurs du processeur
Matériel : bloc d'alimentation	<ul style="list-style-type: none"> • Type : affiche le type du bloc d'alimentation. Les types de blocs d'alimentation sont les suivants : <ul style="list-style-type: none"> • INCONNU • LINÉAIRE • COMMUTATION • BATTERIE • ONDULEUR • CONVERTISSEUR • RÉGULATEUR • CA • CC • VRM • Emplacement : affiche l'emplacement du bloc d'alimentation, par exemple logement 1 • Sortie (Watts) : affiche la puissance en watts
Matériel : mémoire	<ul style="list-style-type: none"> • Bancs de mémoire : affiche la quantité de mémoire utilisée, totale et disponible • Capacité de mémoire : affiche la mémoire installée, la capacité de mémoire totale et la mémoire disponible • Logement : affiche l'emplacement DIMM • Taille : affiche la taille de la mémoire • Type : affiche le type de la mémoire

Matériel : <i>Composant</i>	Informations
Matériel : cartes réseau	<ul style="list-style-type: none"> • Total : affiche le nombre total de cartes d'interface réseau disponibles • Nom : affiche le nom de la carte réseau • Fabricant : affiche uniquement le nom du fabricant • Adresse MAC : affiche l'adresse MAC de la carte réseau
Matériel : emplacements PCI	<ul style="list-style-type: none"> • Logements PCI : affiche les logements utilisés, totaux et disponibles • Logement : affiche le logement • Fabricant : affiche le nom du fabricant du logement PCI • Description : affiche la description du périphérique PCI • Type : affiche le type de logement PCI • Largeur : affiche la largeur du bus de données, si disponible
Matériel : carte d'accès à distance	<ul style="list-style-type: none"> • Adresse IP : affiche l'adresse IP de la carte d'accès à distance • Adresse MAC : affiche l'adresse MAC de la carte d'accès à distance • Type de RAC : affiche le type de la carte d'accès à distance • URL : affiche l'URL active de l'iDRAC associé à cet hôte

Affichage des détails de stockage d'un seul hôte

Vous pouvez afficher les détails de stockage d'un seul hôte dans l'onglet **Informations d'hôte Dell EMC**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Le matériel signale directement les données d'OMSA et d'iDRAC. Voir la section [Exécution des tâches d'inventaire](#). La page affiche différentes options, en fonction de ce qui est sélectionné dans la liste déroulante **Afficher**. Si vous sélectionnez **Disques physiques**, une autre liste déroulante s'affiche. La liste déroulante suivante s'appelle **Filtre** et vous permet de filtrer les options des disques physiques. Pour afficher les détails du stockage, procédez comme suit :

1. Dans OpenManage Integration for VMware vCenter, dans le Navigateur, cliquez sur **Hôtes**.
2. Dans l'onglet **Objets**, sélectionnez l'hôte dont vous souhaitez afficher les détails du stockage : **Détails des disques physiques**.
3. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur l'hôte Dell EMC**.

Dans le sous-onglet **Stockage**, consultez les informations suivantes :

Tableau 17. Détails de stockage d'un seul hôte

Composant	Informations
Stockage	Affiche le nombre de disques virtuels, contrôleurs, boîtiers et disques physiques associés ainsi que la quantité de disques de secours globaux et dédiés. L'option que vous sélectionnez dans la liste déroulante Afficher apparaît en surbrillance.
Afficher	Affiche les options que vous souhaitez afficher pour cet hôte : <ul style="list-style-type: none"> • Disques virtuels. • Disques physiques • Contrôleurs • Enceintes

Affichage des détails de stockage pour l'option Afficher

Les options de stockage qui figurent sur la page **Stockage d'hôte** dépendent de ce que vous avez sélectionné dans la liste déroulante **Afficher**.

Sélectionnez l'une des options mentionnées dans la liste déroulante **Afficher** et affichez les éléments suivants :

Tableau 18. Détails de stockage d'un seul hôte

Informations	Description
<p>Disques virtuels.</p>	<ul style="list-style-type: none"> • Nom : affiche le nom du disque virtuel • FGDD de périphérique : affiche le descripteur de périphérique complet • Disque physique : indique le disque physique où se trouve le disque virtuel • Capacité : affiche la capacité du disque virtuel • Disposition : affiche le type de disposition du stockage virtuel, c'est-à-dire le type de RAID configuré pour ce disque virtuel • Type de support : indique s'il s'agit d'un support SSD ou HDD • ID de contrôleur : affiche l'ID du contrôleur • ID de périphérique : affiche l'ID du périphérique • Taille de bande : affiche la taille de bande, c'est-à-dire la quantité d'espace utilisé par chaque bande sur un seul disque • Protocole de bus : affiche la technologie utilisée par les disques physiques inclus dans le disque virtuel. Les valeurs possibles sont : <ul style="list-style-type: none"> • SCSI • SAS • SATA • Stratégie de lecture par défaut : affiche la stratégie de lecture par défaut prise en charge par le contrôleur. Les options possibles incluent : <ul style="list-style-type: none"> • Lecture anticipée • Sans lecture anticipée • Lecture anticipée adaptative • Cache de lecture activé • Lecture du cache désactivée • Stratégie d'écriture par défaut : affiche la stratégie d'écriture par défaut prise en charge par le contrôleur. Les options possibles incluent : <ul style="list-style-type: none"> • Écriture différée • Forcer l'écriture différée • Écriture différée activée • Écriture immédiate • Écriture sur le cache activée et protégée • Écriture sur le cache désactivée • Stratégie relative au cache : indique si la stratégie relative au cache est activée
<p>Disques physiques : lorsque vous sélectionnez cette option, la liste déroulante Filtrer s'affiche.</p> <p>Vous pouvez filtrer les disques physiques en fonction des options suivantes :</p> <ul style="list-style-type: none"> • Tous les disques physiques • Disques de secours globaux • Disques de secours dédiés • La dernière option affiche les disques virtuels nommés personnalisés. 	<ul style="list-style-type: none"> • Nom : affiche le nom du disque physique • FGDD de périphérique : affiche le descripteur de périphérique complet • Capacité : affiche la capacité du disque physique • État du disque : affiche l'état du disque physique. Les options possibles incluent : <ul style="list-style-type: none"> • EN LIGNE • PRÊT • DÉGRADÉ • EN ÉCHEC • HORS LIGNE • RECONSTRUCTION • INCOMPATIBLE • SUPPRIMÉ • EFFACÉ • ALERTE SMART DÉTECTÉE • INCONNU • ÉTRANGER • NON PRIS EN CHARGE • Configuré : indique si le disque est configuré

Informations	Description
	<ul style="list-style-type: none"> • Type de disque de secours : affiche le type du disque de secours. Les options possibles incluent : <ul style="list-style-type: none"> • « Non » signifie qu'il n'existe aucun disque de secours • « Global » signifie qu'un disque de sauvegarde non utilisé fait partie du groupe de disques • Dédié : un disque de sauvegarde inutilisé attribué à un disque virtuel. Lorsqu'un disque physique du disque virtuel échoue, le disque de secours est activé pour remplacer le disque physique problématique sans que le système ne soit interrompu ou que votre intervention ne soit requise. • Disque virtuel : affiche le nom du disque virtuel • Protocole de bus : affiche le protocole de bus • ID de contrôleur : affiche l'ID du contrôleur • ID de connecteur : affiche l'ID du connecteur • ID de boîtier : affiche l'ID du boîtier • ID de périphérique : affiche l'ID du périphérique • Modèle : affiche le numéro de modèle du disque de stockage physique • Numéro de référence : affiche le numéro de référence pour le stockage • Numéro de série : affiche le numéro de série pour le stockage • Fournisseur : affiche le nom du fournisseur pour le stockage
Contrôleurs	<ul style="list-style-type: none"> • ID de contrôleur : affiche l'ID du contrôleur • Nom : affiche le nom du contrôleur • FGDD de périphérique : affiche le descripteur de périphérique complet • Version de micrologiciel : affiche la version du micrologiciel • Micrologiciel minimum requis : affiche la version minimale requise du micrologiciel. Cette colonne est renseignée si le micrologiciel n'est pas à jour et qu'une version plus récente est disponible • Version du pilote : affiche la version du pilote • État de lecture de surveillance : affiche l'état de la lecture de surveillance • Taille du cache : affiche la taille du cache
Enceintes	<ul style="list-style-type: none"> • ID de contrôleur : affiche l'ID du contrôleur • ID de connecteur : affiche l'ID du connecteur • ID de boîtier : affiche l'ID du boîtier • Nom : affiche le nom du boîtier • FGDD de périphérique : affiche le descripteur de périphérique complet • Numéro de service : affiche le numéro de service

À propos des journaux des événements système dans le client Web

Le journal des événements système (JES) fournit des informations sur l'état du matériel détecté par OMIVV et affiche des informations basées sur les critères suivants :

Condition	Différents types d'icônes d'état sont disponibles : Information (point d'exclamation bleu), Avertissement (triangle jaune avec point d'exclamation), Erreur (X rouge) et Inconnu (boîte contenant un point d'interrogation).
Heure (Heure du serveur)	Indique l'heure et la date de l'événement.
Rechercher dans cette page	Affiche le message, les noms de serveur, les paramètres de configuration, etc. spécifiques.

Les niveaux de gravité sont définis de la manière suivante :

Informatif	L'opération OMIVV a été exécutée avec succès.
Avertissement	L'opération OMIVV a partiellement échoué et partiellement réussi.

Erreur L'opération OMIVV a échoué.


Vous pouvez enregistrer le journal dans un fichier CSV externe. Voir [Affichage des journaux des événements système d'un hôte individuel](#).

Affichage des journaux des événements d'un hôte individuel

Pour afficher les événements, procédez comme suit :

1. Accédez à l'onglet **Surveiller**, ouvrez le sous-onglet **Journal des événements système** et effectuez l'une des opérations suivantes :

Option	Description
À partir d'OMIVV	Effectuez les opérations suivantes : a. Dans OpenManage Integration for VMware vCenter, dans le Navigateur, cliquez sur Hôtes . b. Dans l'onglet Objets , double-cliquez sur l'hôte dont vous souhaitez afficher le journal des événements système (SEL).
À partir de la page d'accueil	Sur la page d'accueil , cliquez sur Hôtes et clusters .

2. Dans l'onglet **Surveiller**, sélectionnez **Informations sur l'hôte Dell EMC > Journal des événements système**. Les 10 entrées les plus récentes du journal des événements système apparaissent.
3. Pour mettre à jour le **Journal des événements système**, effectuez une actualisation globale.
4. Pour limiter (filtrer) le nombre d'entrées du journal des événements, choisissez l'une des options suivantes :
 - Dans la zone de texte de recherche/filtrage, entrez une chaîne de texte pour filtrer dynamiquement les entrées du journal.
 - Pour effacer la zone de texte de filtrage, cliquez sur **X** ; toutes les entrées du journal des événements s'affichent.
5. Pour effacer toutes les entrées du journal des événements, cliquez sur **Effacer le journal**.
Un message s'affiche pour vous indiquer qu'après avoir été effacées, toutes les entrées du journal seront supprimées. Vous pouvez sélectionner l'une des options suivantes :
 - Pour accepter d'effacer les entrées du journal, cliquez sur **Effacer le journal**.
 - Pour annuler, cliquez sur **Annuler**.
6. Pour exporter le journal des événements vers un fichier CSV, cliquez sur .
7. Pour accéder à l'emplacement du journal des événements système et l'enregistrer, cliquez sur **Enregistrer**.

Affichage des détails matériels complémentaires pour un seul hôte

Vous pouvez afficher les détails relatifs au micrologiciel, à la surveillance de l'alimentation et à l'état de la garantie d'un seul hôte dans l'onglet **Informations sur les hôtes Dell EMC**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les vues Matériel signalent directement les données de l'agent OMSA et du contrôleur iDRAC. Voir la section [Exécution immédiate d'une tâche d'inventaire du châssis](#).

1. Dans OpenManage Integration for VMware vCenter, dans le volet Navigateur, cliquez sur **Hôtes**.
2. Dans l'onglet **Objets**, sélectionnez l'hôte dont vous voulez afficher les détails relatifs au <Component Name>.
3. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur l'hôte Dell EMC**.
Dans le sous-onglet Matériel : <Component Name>, affichez les informations suivantes pour chaque composant :

Tableau 19. Informations sur un seul hôte

Composant	Informations
Micrologiciel La page de l'hôte permet d'effectuer des recherches, d'assurer le filtrage et d'exporter un fichier CSV contenant des informations sur le micrologiciel.	<ul style="list-style-type: none">• Nom : affiche le nom de tous les micrologiciels sur cet hôte.• Type : affiche le type de micrologiciel.• Versión : affiche la version de tous les micrologiciels sur cet hôte.• Date d'installation : affiche la date d'installation.
Surveillance de l'alimentation	<ul style="list-style-type: none">• Informations générales : affiche le bilan énergétique et le nom du profil actuel.

Composant	Informations
<p>REMARQUE : L'heure de l'hôte, telle qu'utilisée ici, désigne l'heure locale de l'endroit où l'hôte se trouve.</p>	<ul style="list-style-type: none"> • Seuil : affiche, en watts, les seuils d'avertissement et d'échec. • Capacité d'alimentation de réserve : affiche, en watts, la capacité d'alimentation de réserve instantanée et en cas de pic. <p>Statistiques d'énergie</p> <ul style="list-style-type: none"> • Type : affiche le type de statistique énergétique. • Heure de début des mesures (Heure de l'hôte) : affiche la date et l'heure auxquelles l'hôte a commencé à consommer de l'énergie. • Heure de fin des mesures (Heure de l'hôte) : affiche la date et l'heure auxquelles l'hôte a cessé de consommer de l'énergie. • Relevés : affiche la valeur moyenne des relevés effectués sur une période d'une minute. • Heure de pic (Heure de l'hôte) : affiche, en ampères, la date et l'heure du pic de consommation de l'hôte. • Relevé maximal : affiche, en watts, les statistiques d'alimentation en cas de pic du système, c'est-à-dire la consommation maximale du système.
<p>La garantie</p> <p>REMARQUE : Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Exécution d'une tâche de récupération de la garantie. La page État de la garantie vous permet de surveiller la date d'expiration de la garantie. Les paramètres de garantie déterminent la date de récupération des informations de garantie à partir de Dell Online en activant ou désactivant la planification de garantie, puis en configurant l'alerte Seuil d'alerte minimum en jours.</p>	<ul style="list-style-type: none"> • Fournisseur : affiche le nom du fournisseur de la garantie • Description : affiche une description • Date de début : affiche la date de début de la garantie • Date de fin : affiche la date de fin de la garantie • Jours restants : affiche le nombre de jours qui restent avant l'expiration de la garantie • Dernière mise à jour : affiche l'heure de la dernière mise à jour de la garantie

Surveillance des hôtes sur des clusters et centres de données

OpenManage Integration for VMware vCenter vous permet d'afficher des informations détaillées sur tous les hôtes inclus dans un centre de données ou un cluster. Vous pouvez trier les données en cliquant sur l'en-tête de la ligne de la grille de données. Les pages du centre de données et du cluster vous permettent d'exporter des informations vers un fichier CSV, et la grille de données propose une fonctionnalité de filtrage ou de recherche.

Affichage de la présentation des datacenters et clusters

Affichez des informations détaillées sur les datacenters ou clusters de l'hôte dans l'onglet Informations sur les datacenters/clusters. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les données affichées peuvent varier selon la vue à partir de laquelle vous accédez aux données. Les vues Matériel signalent directement les données de l'OMSA et du contrôleur iDRAC. Voir la section [Exécution des tâches d'inventaire](#).

REMARQUE : Les pages du datacenter et du cluster vous permettent d'exporter des informations vers un fichier CSV, et une fonctionnalité de filtrage/recherche est disponible sur la grille de données.

1. Dans OpenManage Integration for VMware vCenter, dans le Navigateur, cliquez sur **vCenter**.
2. Cliquez sur **Datacenters** ou **Clusters**.
3. Dans l'onglet **Objets**, sélectionnez le datacenter ou le cluster dont vous voulez afficher les détails d'hôte.
4. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur le datacenter/cluster Dell EMC > Aperçu** pour afficher les détails.

REMARQUE : Pour afficher la liste exhaustive des informations détaillées, sélectionnez un hôte particulier dans la grille de données.

Tableau 20. Aperçu des datacenters et clusters

Informations	Description
Informations Datacenter/Cluster	Affiche les éléments suivants : <ul style="list-style-type: none"> · Nom de datacenter/cluster · Nombre d'hôtes gérés Dell · Consommation totale d'énergie
Mode de verrouillage du système	Affiche l'état du mode de verrouillage de l'iDRAC. L'état du mode de verrouillage de l'iDRAC du nombre total des hôtes est affiché comme suit : <ul style="list-style-type: none"> · Activé · Désactivé · Non applicable (uniquement pour les serveurs de 14e génération)
Ressources matérielles	Affiche les éléments suivants : <ul style="list-style-type: none"> · Nombre total de processeurs · Mémoire totale · Capacité
Récapitulatif de garantie	Affiche l'état de garantie de l'hôte sélectionné. Les options État disponibles sont les suivantes : <ul style="list-style-type: none"> · Garantie expirée · Garantie active · Garantie inconnue
Hôte	Affiche le nom de l'hôte
Numéro de service	Affiche le numéro de service de l'hôte
Modèle	Affiche le modèle du PowerEdge
Marquage de l'actif	Affiche le numéro d'inventaire, s'il a été défini
Numéro de service du châssis	Affiche le numéro de service du châssis, s'il existe
Version du système d'exploitation	Affiche la version du SE d'ESXi
Emplacement	Lames uniquement : affiche l'emplacement du logement. Pour les autres, affiche « Non applicable »
Mode de verrouillage du système	Uniquement pour les serveurs PowerEdge de 14e génération : affiche le mode de verrouillage de l'hôte iDRAC, qui est activé, désactivé ou inconnu. Pour tous les serveurs PowerEdge antérieurs à la 14e génération, le mode de verrouillage du système affiché est Non applicable.
IP iDRAC	Affiche l'adresse IP de l'iDRAC
Adresse IP de la console de service	Affiche l'adresse IP de la console de service
URL CMC	Affiche l'URL du CMC, qui correspond à l'URL du châssis pour les serveurs lames, ou affiche « Non applicable »
UC	Affiche le nombre d'UC disponibles
Mémoire	Affiche la quantité de mémoire de l'hôte
État de l'alimentation	Indique si l'hôte est alimenté
Dernier inventaire	Affiche le jour, la date et l'heure de la dernière tâche d'inventaire

Informations	Description
Profil de connexion	Affiche le nom du profil de connexion
Version de la carte d'accès à distance	Affichage la version de la carte d'accès à distance
Version du micrologiciel du BIOS	Affiche la version du micrologiciel du BIOS

Affichage des détails matériels des datacenters et clusters

Vous pouvez afficher les détails matériels d'un hôte dans l'onglet **Informations sur les datacenters/clusters Dell EMC**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les pages relatives aux datacenters et aux clusters vous permettent d'exporter ces informations au format CSV, et la grille de données propose une fonctionnalité de filtrage ou de recherche. Les données affichées peuvent varier selon la vue à partir de laquelle vous accédez aux données. Les vues Matériel signalent directement les données de l'agent OMSA et du contrôleur iDRAC. Voir la section [Exécution des tâches d'inventaire](#).

1. Dans OpenManage Integration for VMware vCenter, accédez au volet Navigateur, puis cliquez sur **Listes d'inventaire vCenter**.
2. Cliquez sur **Datacenters** ou **Clusters**.
3. Dans l'onglet **Objets**, sélectionnez le datacenter ou le cluster spécifique dont vous souhaitez afficher les détails des composants.
4. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur les datacenters/clusters Dell EMC**.

Dans le sous-onglet Matériel : <Component Name>, affichez les informations suivantes pour chaque composant.

Tableau 21. Informations sur le matériel des datacenters et des clusters

Matériel : <i>Composant</i>	Informations
Matériel : unité remplaçable	<ul style="list-style-type: none"> • Hôte : affiche le nom d'hôte • Numéro de service : affiche le numéro de service de l'hôte • Nom de pièce : affiche le nom de pièce de l'unité remplaçable • Numéro de pièce : affiche le numéro de pièce de l'unité remplaçable • Fabricant : affiche le nom du fabricant • Numéro de série : affiche le numéro de série du fabricant • Date de fabrication : affiche la date de fabrication
Matériel : processeur	<ul style="list-style-type: none"> • Hôte : affiche le nom d'hôte • Numéro de service : affiche le numéro de service de l'hôte • Socket : affiche le numéro de logement • Vitesse : affiche la vitesse actuelle • Marque : affiche la marque du processeur • Versión : affiche la version du processeur • Cœurs : affiche le nombre de cœurs du processeur
Matériel : bloc d'alimentation	<ul style="list-style-type: none"> • Hôte : affiche le nom d'hôte • Numéro de service : affiche le numéro de service de l'hôte • Type : affiche le type du bloc d'alimentation. Les types de blocs d'alimentation sont les suivants : <ul style="list-style-type: none"> • INCONNU • LINÉAIRE • COMMUTATION • BATTERIE • ONDULEUR • CONVERTISSEUR • RÉGULATEUR • CA • CC • VRM

Matériel : <i>Composant</i>	Informations
	<ul style="list-style-type: none"> · Emplacement : affiche l'emplacement du bloc d'alimentation, par exemple logement 1 · Sortie (Watts) : affiche la puissance en watts · État : affiche l'état du bloc d'alimentation. Les options État disponibles sont les suivantes : <ul style="list-style-type: none"> · AUTRE · INCONNU · OK · CRITIQUE · NON CRITIQUE · RÉCUPÉRABLE · IRRÉCUPÉRABLE · ÉLEVÉ · FAIBLE
Matériel : mémoire	<ul style="list-style-type: none"> · Hôte : affiche le nom d'hôte · Numéro de service : affiche le numéro de service de l'hôte · Logement : affiche l'emplacement DIMM · Taille : affiche la taille de la mémoire · Type : affiche le type de la mémoire
Matériel : cartes réseau	<ul style="list-style-type: none"> · Hôte : affiche le nom d'hôte · Numéro de service : affiche le numéro de service de l'hôte · Nom : affiche le nom de la carte réseau · Fabricant : affiche uniquement le nom du fabricant · Adresse MAC : affiche l'adresse MAC de la carte réseau
Matériel : emplacements PCI	<ul style="list-style-type: none"> · Hôte : affiche le nom d'hôte · Numéro de service : affiche le numéro de service de l'hôte · Logement : affiche le logement · Fabricant : affiche le nom du fabricant du logement PCI · Description : affiche la description du périphérique PCI · Type : affiche le type de logement PCI · Largeur : affiche la largeur du bus de données, si disponible
Matériel : carte d'accès à distance	<ul style="list-style-type: none"> · Hôte : affiche le nom d'hôte · Numéro de service : affiche le numéro de service de l'hôte · Adresse IP : affiche l'adresse IP de la carte d'accès à distance · Adresse MAC : affiche l'adresse MAC de la carte d'accès à distance · Type de RAC : affiche le type de la carte d'accès à distance · URL : affiche l'URL active de l'iDRAC associé à cet hôte

Affichage des détails de stockage des datacenters et clusters

Vous pouvez consulter les détails relatifs au stockage physique d'un datacenter ou d'un cluster dans l'onglet **Informations sur le datacenter/cluster**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les pages de datacenter et de cluster vous permettent d'exporter des informations dans un fichier CSV, et une fonctionnalité de filtrage/recherche est disponible sur la grille de données. Les vues Matériel signalent directement les données de l'agent OMSA et du contrôleur iDRAC. Voir la section [Exécution des tâches d'inventaire](#).

1. Dans OpenManage Integration for VMware vCenter, accédez au volet Navigateur, puis cliquez sur **Listes d'inventaire vCenter**.
2. Cliquez sur **Datacenters** ou **Clusters**.

3. Dans l'onglet **Objets**, sélectionnez le datacenter ou le cluster spécifique.
4. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur le datacenter/cluster Dell EMC** et accédez à **Stockage > Disque physique/disque virtuel**.

Pour afficher la liste exhaustive des informations détaillées, sélectionnez un hôte particulier dans la grille de données.

Tableau 22. Détails du stockage pour un datacenter et un cluster

Stockage : disques	Description
Disque physique	<ul style="list-style-type: none"> • Hôte : affiche le nom d'hôte • Numéro de service : affiche le numéro de service de l'hôte • Capacité : affiche la capacité du disque physique • État du disque : affiche l'état du disque physique. Les options possibles incluent : <ul style="list-style-type: none"> • EN LIGNE • PRÊT • DÉGRADÉ • EN ÉCHEC • HORS LIGNE • RECONSTRUCTION • INCOMPATIBLE • SUPPRIMÉ • EFFACÉ • DÉTECTION D'ALERTE INTELLIGENTE • INCONNU • ÉTRANGER • NON PRIS EN CHARGE <p>REMARQUE : Pour en savoir plus sur la signification de ces alertes, voir le Guide d'utilisation de Dell EMC OpenManage Server Administrator Storage Management à l'adresse dell.com/support</p> <ul style="list-style-type: none"> • Numéro de modèle : affiche le numéro de modèle du disque physique de stockage • Dernier inventaire : affiche le jour, le mois et l'heure de la dernière exécution de l'inventaire • État : affiche l'état de l'hôte • ID de contrôleur : affiche l'ID du contrôleur • ID de connecteur : affiche l'ID du connecteur • ID de boîtier : affiche l'ID du boîtier • ID de périphérique : affiche l'ID du périphérique • Protocole de bus : affiche le protocole de bus • Type de disque de secours : affiche le type du disque de secours. Les options possibles incluent : <ul style="list-style-type: none"> • Non : signifie qu'il n'existe aucun disque de secours • Global : disque de sauvegarde non utilisé qui fait partie du groupe de disques • Dédié : un disque de sauvegarde inutilisé attribué à un disque virtuel. Lorsqu'un disque physique du disque virtuel échoue, le disque de secours est activé pour remplacer le disque physique problématique sans que le système ne soit interrompu ou que votre intervention ne soit requise • Numéro de référence : affiche le numéro de référence pour le stockage • Numéro de série : affiche le numéro de série pour le stockage • Nom du fournisseur : affiche le nom du fournisseur de stockage
Disque virtuel	<ul style="list-style-type: none"> • Hôte : affiche le nom de l'hôte • Numéro de service : affiche le numéro de service de l'hôte • Nom : affiche le nom du disque virtuel • Disque physique : indique le disque physique où se trouve le disque virtuel • Capacité : affiche la capacité du disque virtuel • Disposition : affiche le type de disposition du stockage virtuel. C'est-à-dire le type de RAID configuré pour ce disque virtuel

Stockage : disques	Description
	<ul style="list-style-type: none"> • Dernier inventaire : affiche le jour, la date et l'heure de la dernière exécution de l'inventaire • ID de contrôleur : affiche l'ID du contrôleur • ID de périphérique : affiche l'ID du périphérique • Type de support : indique s'il s'agit d'un support SSD ou HDD • Protocole de bus : affiche la technologie utilisée par les disques physiques inclus dans le disque virtuel. Les valeurs possibles sont les suivantes : <ul style="list-style-type: none"> • SCSI • SAS • SATA • Taille de bande : affiche la taille de bande du disque virtuel. La taille de bande fait référence à la quantité d'espace utilisée par chaque bande sur un seul disque • Stratégie de lecture par défaut : affiche la stratégie de lecture par défaut prise en charge par le contrôleur. Les options possibles incluent : <ul style="list-style-type: none"> • Lecture anticipée • Sans lecture anticipée • Lecture anticipée adaptative • Cache de lecture activé • Lecture du cache désactivée • Stratégie d'écriture par défaut : affiche la stratégie d'écriture par défaut prise en charge par le contrôleur. Les options possibles incluent : <ul style="list-style-type: none"> • Écriture différée • Forcer l'écriture différée • Écriture différée activée • Écriture immédiate • Écriture sur le cache activée et protégée • Écriture sur le cache désactivée • Stratégie de cache de disque : affiche la stratégie de mise en cache par défaut prise en charge par le contrôleur. Les options possibles incluent : <ul style="list-style-type: none"> • Activé : E/S de cache • Désactivé : E/S directe

Affichage des détails matériels complémentaires pour les datacenters et clusters

Vous pouvez afficher les détails relatifs au micrologiciel, à la surveillance de l'alimentation et à l'état de la garantie d'un cluster dans l'onglet **Informations sur les datacenters/clusters Dell EMC**. Pour que ces informations s'affichent sur cette page, exécutez une tâche d'inventaire. Les pages de datacenter et de cluster vous permettent d'exporter des informations dans un fichier CSV, et une fonctionnalité de filtrage/recherche est disponible sur la grille de données. Les vues Matériel signalent directement les données de l'agent OMSA et du contrôleur iDRAC. Voir la section [Exécution immédiate d'une tâche d'inventaire](#).

1. Dans OpenManage Integration for VMware vCenter, dans le volet Navigateur, cliquez sur **vCenter**.
2. Cliquez sur **Datacenters** ou **Clusters**.
3. Dans l'onglet **Objets**, sélectionnez le datacenter ou le cluster spécifique dont vous souhaitez afficher les détails de composants d'hôte.
4. Dans l'onglet **Surveiller**, sélectionnez l'onglet **Informations sur les datacenters/clusters Dell EMC**.

Le sous-onglet <Component Name> affiche les informations suivantes pour chacun des composants :

Tableau 23. Informations sur un seul hôte

Composant	Informations
Micrologiciel	<ul style="list-style-type: none"> • Hôte : affiche le nom de l'hôte • Numéro de service : affiche le numéro de service de l'hôte • Nom : affiche le nom de tous les micrologiciels sur cet hôte.

Composant	Informations
	<ul style="list-style-type: none"> • Version : affiche la version de tous les micrologiciels sur cet hôte.
<p>Surveillance de l'alimentation</p> <p>i REMARQUE : Pour afficher la liste exhaustive des informations détaillées, sélectionnez un hôte particulier dans la grille de données.</p>	<ul style="list-style-type: none"> • Hôte : affiche le nom de l'hôte • Numéro de service : affiche le numéro de service de l'hôte • Profil actuel : affiche le profil d'alimentation en vue d'optimiser les performances de votre système et d'économiser de l'énergie • Consommation énergétique : affiche la consommation électrique de l'hôte • Capacité de réserve maximale : affiche la capacité de réserve d'alimentation en cas de pic • Bilan énergétique : affiche le seuil énergétique de cet hôte • Seuil d'avertissement : affiche la valeur maximale configurée sur votre système pour le seuil d'avertissement du capteur de température. • Seuil d'échec : affiche la valeur maximale configurée sur votre système pour le seuil d'échec du capteur de température • Capacité de réserve instantanée : affiche la capacité de marge instantanée de l'hôte • Date de début de la consommation électrique : affiche la date et l'heure auxquelles l'hôte a commencé à consommer de l'énergie • Date de fin de la consommation électrique : affiche la date et l'heure auxquelles l'hôte a cessé de consommer de l'énergie • Puissance système maximale : affiche l'alimentation de l'hôte en cas de pic • Date de début de la puissance système maximale : affiche la date et l'heure auxquelles le pic d'alimentation de l'hôte a commencé • Date de fin de la puissance système maximale : affiche la date et l'heure auxquelles le pic d'alimentation de l'hôte s'est arrêté • Pic de consommation du système (en ampères) : affiche la consommation maximale de l'hôte en ampères • Date de début du pic de consommation du système (en ampères) : affiche, en ampères, la date et l'heure auxquelles le pic de consommation du système a commencé • Date de fin du pic de consommation du système (en ampères) : affiche, en ampères, la date et l'heure auxquelles le pic de consommation du système s'est arrêté
<p>Récapitulatif de garantie</p> <p>i REMARQUE : Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Exécution d'une tâche de récupération de la garantie. La page Récapitulatif de la garantie vous permet de surveiller la date d'expiration de la garantie. Les paramètres de garantie déterminent la date de récupération des informations de garantie à partir de Dell Online en activant ou désactivant la planification de garantie, puis en configurant l'alerte Seuil d'alerte minimum en jours.</p>	<ul style="list-style-type: none"> • Récapitulatif de la garantie : le récapitulatif de la garantie de l'hôte s'affiche sous forme d'icônes, pour montrer visuellement le nombre d'hôtes dans chaque catégorie d'état • Hôte : affiche le nom d'hôte • Numéro de service : affiche le numéro de service de l'hôte. • Description : affiche une description. • État de la garantie : affiche l'état de la garantie de l'hôte. Les options d'état possibles incluent : <ul style="list-style-type: none"> • Actif : l'hôte est sous garantie et aucun seuil n'a été franchi • Avertissement : l'hôte est sous garantie, mais le seuil d'avertissement a été franchi

Composant	Informations
	<ul style="list-style-type: none"> · Critique : l'hôte est sous garantie, mais un seuil critique a été franchi · Expiré : la garantie de cet hôte est arrivée à expiration · Inconnu : OpenManage Integration for VMware vCenter ne parvient pas à obtenir l'état de la garantie, car la tâche de garantie n'est pas exécutée, une erreur s'est produite lors de l'obtention des données ou le système n'a pas de garantie · Jours restants : affiche le nombre de jours qui restent avant l'expiration de la garantie

Configuration du clignotement du voyant d'un serveur physique

Pour mieux localiser un serveur physique dans un grand environnement de datacenter, vous pouvez configurer le voyant avant de sorte qu'il clignote pendant la période spécifiée.

1. Dans OpenManage Integration for VMware vCenter, dans la zone Navigateur, sous Listes d'inventaire, cliquez sur **Hôtes**.
2. Dans l'onglet **Objet**, double-cliquez sur l'hôte de votre choix.
3. Dans l'onglet **Récapitulatif**, faites défiler l'affichage jusqu'au portlet Dell EMC Server Management.
4. Sous **Actions de l'hôte**, sélectionnez **Faire clignoter le voyant**
5. Choisissez l'une des options suivantes :
 - Pour activer le clignotement et spécifier la période, accédez à la boîte de dialogue **Voyant**, cliquez sur **Clignotement activé** et utilisez la liste déroulante Délai d'expiration pour sélectionner l'incrément du délai d'expiration, puis cliquez sur **OK**.
 - Pour désactiver le clignotement, accédez à la boîte de dialogue **Voyant**, cliquez sur **Clignotement désactivé**, puis cliquez sur **OK**.

Configuration du mode de verrouillage du système

Le paramètre du mode de verrouillage du système est disponible dans l'iDRAC pour la 14e génération de serveurs PowerEdge. Lorsque ce paramètre est activé, la configuration du système, notamment les mises à jour du micrologiciel, sont verrouillées. Ce paramètre est destiné à protéger le système des modifications non-intentionnelles. Vous pouvez activer ou désactiver le mode de verrouillage du système pour les hôtes gérés par l'utilisation de l'appliance OMIVV ou à partir de la console iDRAC.

À partir de l'OMIVV version 4.1 et ultérieures, vous pouvez configurer et contrôler le mode de verrouillage de l'iDRAC dans les serveurs. Vous pouvez configurer le mode de verrouillage du système en verrouillant ou déverrouillant l'hôte ou le cluster au niveau de l'hôte ou du cluster. Lorsque le mode de verrouillage du système est activé, les fonctionnalités suivantes sont limitées :

- Toutes les tâches de configuration, telles que la mise à jour du micrologiciel, le déploiement du système d'exploitation, la suppression des journaux d'événements du système, la réinitialisation de l'iDRAC et la configuration de la destination d'interruption d'iDRAC.

Pour configurer le mode de verrouillage du système d'un hôte ou d'un cluster au niveau de l'hôte ou du cluster, effectuez les étapes suivantes :

1. Pour lancer l'Assistant Configuration du mode de verrouillage du système, effectuez l'une des opérations suivantes :
 - a) Dans le volet **Navigateur**, cliquez sur **Hôtes et clusters**, sélectionnez et cliquez avec le bouton droit sur un hôte ou un cluster ou sélectionnez un hôte ou un cluster et cliquez sur la liste déroulante **Actions**, puis sélectionnez **Toutes les actions d'OpenManage Integration > Configuration du mode de verrouillage du système**.
 - b) Dans OpenManage Integration, cliquez sur la page **Hôtes** ou **Clusters**, sélectionnez et cliquez avec le bouton droit sur un hôte ou un cluster ou sélectionnez un hôte ou un cluster et cliquez sur la liste déroulante **Actions**, puis sélectionnez **Toutes les actions d'OpenManage Integration > Configuration du mode de verrouillage du système**.
 - c) Dans le volet **Navigateur**, sélectionnez un hôte ou un cluster, puis cliquez sur **Résumé > Informations sur l'hôte Dell EMC > Configuration du mode de verrouillage du système**.
 - d) Dans le volet **Navigateur**, sélectionnez un hôte ou un cluster, puis cliquez sur **Moniteur > Informations sur l'hôte Dell EMC > Micrologiciel > Configuration du mode de verrouillage du système**.
2. Pour activer le mode de verrouillage du système, sélectionnez l'option **Activer**. Pour désactiver le mode de verrouillage, sélectionnez **Désactiver**.
3. Cliquez sur **Appliquer**.

Si vous essayez de configurer le mode de verrouillage du système pour les serveurs PowerEdge de la 11e à la 13e génération, un message indiquant que cette fonctionnalité n'est pas prise en charge s'affiche sur cette plate-forme.

Une fois la configuration du verrouillage du système terminée, vous pouvez afficher l'état mis à jour du mode de verrouillage sur la page **File d'attente des tâches**. Les informations de la file d'attente des tâches du mode de verrouillage sont valides uniquement au niveau du cluster. Pour accéder à la page File d'attente des tâches, dans OpenManage Integration, sélectionnez **Surveiller > File d'attente des tâches > Tâches du mode de verrouillage du système**. Voir la documentation de l'iDRAC pour plus d'informations sur le mode de verrouillage du système.

Surveillance d'événements, d'alarmes et de l'intégrité

L'objectif de la gestion matérielle est de fournir l'état d'intégrité du système et des informations actualisées sur l'infrastructure dont l'administrateur a besoin pour répondre à des événements matériels critiques sans quitter le plug-in OMIVV ou vCenter.

La surveillance du datacenter et du système hôte permet à un administrateur de surveiller l'intégrité de l'infrastructure en affichant les événements matériels (serveur et stockage) et relatifs à la virtualisation dans les onglets **Tâches** et **Événements** de vCenter. En outre, les alertes matérielles critiques peuvent déclencher les alarmes d'OpenManage Integration for VMware vCenter et quelques alarmes définies pour les événements connexes à la virtualisation Dell peuvent faire basculer le système d'ordinateur hôte géré en mode maintenance.

Pour recevoir des événements de la part des serveurs, OMIVV est configuré comme destination d'interruption sur tous les appareils surveillés et les diverses destinations sont définies comme suit :

- La destination d'interruption SNMP est définie dans le contrôleur iDRAC pour les hôtes de 12e génération et de générations ultérieures.
- La destination d'interruption est définie dans OMSA pour les hôtes antérieurs à la 12e génération.
- La destination d'interruption est définie dans CMC pour le châssis.

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

Pour assurer la surveillance, procédez comme suit :

- Configurez les paramètres **Événements et alarme**.
- Configurez les destinations d'interruptions SNMP OMSA, le cas échéant.
- Utilisez l'onglet **Tâches** et **événements** de vCenter pour examiner les informations sur les événements.

Sujets :

- [À propos des événements et alarmes pour les hôtes](#)
- [À propos des événements et alarmes pour le châssis](#)
- [Événements relatifs à la virtualisation](#)
- [Événements Proactive HA](#)
- [Affichage des paramètres d'alarme et événement](#)
- [Affichage des événements](#)
- [Intégrité de la redondance des composants matériels - Proactive HA](#)
- [Lancement des consoles de gestion](#)

À propos des événements et alarmes pour les hôtes

Vous pouvez modifier des événements et alarmes d'OpenManage Integration for VMware vCenter depuis l'onglet **Gérer > Paramètres**. À partir de cet onglet, vous pouvez sélectionner le niveau de publication des événements, activer les alarmes des hôtes Dell EMC ou restaurer les alarmes par défaut. Vous pouvez configurer des événements et alarmes séparément (pour chaque vCenter) ou simultanément (pour tous les vCenters enregistrés).

Voici les quatre niveaux de publication d'événement :

Tableau 24. Niveau de publication d'événement

Événement	Description
Ne pas publier d'événement	Ne pas autoriser l'OpenManage Integration for VMware vCenter à transférer les événements ou alertes dans les vCenters associés.

Événement	Description
Publier tous les événements	Publier tous les événements, notamment les événements non formels, que l'OpenManage Integration for VMware vCenter reçoit des hôtes Dell EMC gérés dans les vCenters associés.
Publier uniquement les événements Critique et Avertissement	Publier uniquement les événements de type Critique ou Avertissement dans les vCenter associés.
Publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation	Publier uniquement les événements relatifs à la virtualisation reçus des hôtes dans les vCenter associés. Les événements relatifs à la virtualisation sont ceux que Dell a sélectionnés comme étant les plus critiques pour les hôtes exécutant des machines virtuelles.


Lorsque vous configurez vos événements et alarmes, vous pouvez les activer. Lorsqu'elles sont activées, les alarmes matérielles critiques peuvent amener l'appliance OMIVV à mettre le système hôte en mode de maintenance, et dans certains cas, migrer les machines virtuelles vers un autre système hôte. OpenManage Integration for VMware vCenter transmet les événements reçus des hôtes Dell EMC gérés, et crée des alarmes pour ces événements. Utilisez ces alarmes pour déclencher des actions depuis vCenter, comme un redémarrage, un mode de maintenance ou une migration.

Par exemple, lorsqu'un bloc d'alimentation double tombe en panne et qu'une alarme est créée, la machine passe en mode maintenance, ce qui entraîne la migration des charges de travail vers un autre hôte dans le cluster.

Les hôtes situés en dehors de clusters, ou dans des clusters où VMware Distributed Resource Scheduling (DRS) n'est pas activé, pourraient voir les machines virtuelles arrêtées en raison d'un événement critique. DRS surveille en permanence l'utilisation dans un pool de ressources et répartit intelligemment les ressources disponibles entre les machines virtuelles en fonction des besoins commerciaux. Pour veiller à ce que les machines virtuelles soient automatiquement migrées en cas d'événements matériels critiques, utilisez des clusters avec alarmes Dell configurées par DRS. Les informations contenues dans les messages qui s'affichent à l'écran répertorient les clusters de l'instance de vCenter qui pourraient être affectés. Vérifiez que les clusters sont bien affectés avant d'activer des événements et alarmes.

Si vous avez besoin de restaurer les paramètres d'alarme par défaut, vous pouvez le faire avec le bouton **Réinitialiser l'alarme par défaut**. Cet astucieux bouton permet de restaurer la configuration d'alarme par défaut sans désinstaller et réinstaller le produit. Si des configurations d'alarme Dell ont été modifiées depuis l'installation, ces changements sont annulés lorsque vous utilisez ce bouton.

 **REMARQUE :** Pour recevoir ces événements Dell, veillez à activer les événements.

 **REMARQUE :** OpenManage Integration for VMware vCenter présélectionne les événements relatifs à la virtualisation permettant aux hôtes d'exécuter avec succès les machines virtuelles. Par défaut, les alarmes des hôtes Dell sont désactivées. Si les alarmes Dell sont activées, les clusters doivent utiliser DRS pour veiller à ce que les machines virtuelles qui envoient les événements critiques soient automatiquement migrées.

À propos des événements et alarmes pour le châssis

Les événements et alarmes correspondant à un châssis sont uniquement affichés au niveau du serveur vCenter. Les paramètres des événements et alarmes des hôtes de chaque serveur vCenter s'appliquent également au niveau du châssis. Vous pouvez modifier les paramètres des événements et alarmes à partir de l'onglet **Gérer > Paramètres** d'OpenManage Integration for VMware vCenter. Cet onglet vous permet également de sélectionner le niveau de publication des événements, d'activer les alarmes du châssis et des hôtes Dell EMC, ou de restaurer les alarmes par défaut. Vous pouvez configurer des événements et alarmes individuellement (pour chaque vCenter) ou simultanément (pour tous les serveurs vCenter enregistrés).

Affichage des événements de châssis

1. Dans le volet gauche, sélectionnez vCenter, puis cliquez sur les serveurs vCenter.
2. Cliquez sur un vCenter particulier.
3. Cliquez sur l'onglet **Surveiller > Événements**.
4. Pour afficher davantage de détails d'événement, sélectionnez un événement spécifique.

Affichage des alarmes de châssis

1. Dans le volet gauche, sélectionnez vCenter, puis cliquez sur les serveurs vCenter.

2. Cliquez sur un vCenter particulier.
Les alarmes s'affichent. Seules les quatre premières alarmes apparaissent.
3. Pour afficher la liste complète des alarmes, cliquez sur **Afficher tout** pour afficher la liste détaillée dans l'onglet **Surveiller** pour **Tous les problèmes**.
4. Dans **Alarmes déclenchées**, cliquez sur **Alarme** pour afficher la définition d'alarme.

Événements relatifs à la virtualisation

Le tableau suivant contient les événements critiques et d'avertissement relatifs à la virtualisation. Il inclut le nom de l'événement, sa description, son niveau de gravité et l'action recommandée.

Les événements relatifs à la virtualisation s'affichent au format suivant :

Dell-Message ID:<numéro d'ID>, Message:<Description du message>.

Les événements relatifs au châssis s'affichent au format suivant :

Dell-Message:<description du message>, Chassis name:<nom du châssis>, Chassis Service Tag:<numéro de série du châssis>, Chassis Location:<emplacement du châssis>

Tableau 25. Événements de virtualisation

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Un capteur de courant a détecté une valeur d'avertissement	Un capteur de courant présent dans le système spécifié a dépassé son seuil d'avertissement	Avertissement	Pas d'action
Dell - Un capteur de courant a détecté une valeur de défaillance	Un capteur de courant présent dans le système spécifié a dépassé son seuil de défaillance	Erreur	Mettez le système en mode de maintenance
Dell - Un capteur de courant a détecté une valeur irrécupérable	Un capteur de courant dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action
Dell - Redondance regagnée	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Redondance dégradée	Un capteur de redondance présent dans le système spécifié a détecté que l'un des composants de l'unité de redondance a échoué, mais l'unité est encore redondante	Avertissement	Pas d'action
Dell - Perte de la redondance	Un capteur de redondance présent dans le système spécifié a détecté que l'un des composants de l'unité redondante a été déconnecté, est en panne ou n'est pas présent	Erreur	Mettez le système en mode de maintenance
Dell - Retour à la normale de l'alimentation	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Avertissement détecté par l'alimentation	La lecture d'un capteur de bloc d'alimentation présent dans le système spécifié a dépassé un seuil d'avertissement configurable par l'utilisateur	Avertissement	Pas d'action
Dell - L'alimentation a détecté une panne	Un bloc d'alimentation a été déconnecté ou a échoué	Erreur	Mettez le système en mode de maintenance

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Le capteur d'alimentation a détecté une valeur non récupérable	Un capteur de bloc d'alimentation présent dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action
Dell - Avertissement de l'état du périphérique mémoire	Le taux de correction d'un périphérique de mémoire a dépassé une valeur acceptable	Avertissement	Pas d'action
Dell - Erreur de périphérique mémoire	Le taux de correction d'un périphérique de mémoire a dépassé une valeur acceptable, un banc de mémoire de secours a été activé ou une erreur ECC multibits s'est produite	Erreur	Mettez le système en mode de maintenance
Dell - Boîtier de ventilateur inséré dans le système	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Boîtier de ventilateur retiré du système	Un boîtier de ventilateur a été retiré du système spécifié	Avertissement	Pas d'action
Dell - Boîtier de ventilateur retiré du système pendant une période étendue	Un boîtier de ventilateur a été retiré du système spécifié pendant une période configurable par l'utilisateur	Erreur	Pas d'action
Dell - Le capteur de boîtier de ventilateur a détecté une valeur non récupérable	Un capteur de boîtier de ventilateur présent dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action
Dell - L'alimentation CA a été restaurée	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Avertissement de perte d'alimentation CA	Un cordon d'alimentation secteur a perdu son alimentation, mais une redondance suffisante existe pour classer cela comme un avertissement	Avertissement	Pas d'action
Dell - Un cordon d'alimentation secteur a perdu son alimentation	Un cordon d'alimentation secteur a perdu son alimentation, et le manque de redondance exige de classer cela comme une erreur	Erreur	Pas d'action
Dell - Le capteur de processeur est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Le capteur de processeur a détecté une valeur d'avertissement	Un capteur de processeur présent dans le système spécifié est dans un état ralenti	Avertissement	Pas d'action
Dell - Le capteur de processeur a détecté une valeur de défaillance	Un capteur de processeur présent dans le système spécifié est désactivé, présente une erreur de configuration, ou enregistre un déclenchement thermique	Erreur	Pas d'action
Dell - Le capteur de processeur a détecté une valeur non récupérable	Un capteur de processeur dans le système spécifié a échoué.	Erreur	Pas d'action

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Erreur de configuration du périphérique	Une erreur de configuration a été détectée pour un dispositif enfichable dans le système spécifié	Erreur	Pas d'action
Dell - Le capteur de batterie est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Le capteur de batterie a détecté une valeur d'avertissement	Un capteur de batterie présent dans le système spécifié a détecté qu'une batterie se trouve dans un état de défaillance prédictive	Avertissement	Pas d'action
Dell - Le capteur de batterie a détecté une valeur de défaillance	Un capteur de batterie présent dans le système spécifié a détecté que la batterie est défaillante	Erreur	Pas d'action
Dell - Le capteur de batterie a détecté une valeur non récupérable	Un capteur de batterie présent dans le système spécifié a détecté que la batterie est défaillante	Erreur	Aucune action
Dell - La protection contre l'arrêt thermique a été initiée	Ce message est généré lorsqu'un système est configuré pour effectuer un arrêt thermique en cas d'événement d'erreur. Si une lecture du capteur de température dépasse le seuil d'erreur pour lequel le système est configuré, le système d'exploitation s'arrête et le système se met hors tension. Cet événement peut également être exécuté sur des systèmes où un boîtier de ventilateur est retiré du système pendant une période prolongée	Erreur	Pas d'action
Dell - Le capteur de température est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Le capteur de température a détecté une valeur d'avertissement	Un capteur de température présent sur la carte de fond de panier, la carte système, l'UC ou le logement du lecteur au sein du système spécifié a dépassé son seuil d'avertissement	Avertissement	Pas d'action
Dell - Le capteur de température a détecté une valeur de défaillance	Un capteur de température présent sur la carte de fond de panier, la carte système ou le logement du lecteur au sein du système spécifié a dépassé son seuil de défaillance	Erreur	Mettez le système en mode de maintenance
Dell - Le capteur de température a détecté une valeur non récupérable	Un capteur de température présent sur la carte de fond de panier, la carte système ou le logement du lecteur au sein du système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Le capteur de ventilateur est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Le capteur de ventilateur a détecté une valeur d'avertissement	La lecture d'un capteur de ventilateur présent dans l'hôte <x> a dépassé une valeur de seuil d'avertissement	Avertissement	Aucune action
Dell - Le capteur de ventilateur a détecté une valeur de défaillance	Un capteur de ventilateur présent dans le système spécifié a détecté la défaillance d'un ou de plusieurs ventilateurs	Erreur	Mettez le système en mode de maintenance
Dell - Le capteur de ventilateur a détecté une valeur non récupérable	Un capteur de ventilateur a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action
Dell - Le capteur de tension est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Le capteur de tension a détecté une valeur d'avertissement	Un capteur de tension présent dans le système spécifié a dépassé son seuil d'avertissement.	Avertissement	Pas d'action
Dell - Le capteur de tension a détecté une valeur de défaillance	Un capteur de tension présent dans le système spécifié a dépassé son seuil de défaillance	Erreur	Mettez le système en mode de maintenance
Dell - Le capteur de tension a détecté une valeur non récupérable	Un capteur de tension présent dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer	Erreur	Pas d'action
Dell - Le capteur d'intensité est revenu à une valeur normale	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Stockage : erreur de gestion de stockage	La gestion du stockage a détecté un état d'erreur indépendant du périphérique	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : avertissement de contrôleur	Une partie du disque physique est endommagée.	Avertissement	Pas d'action
Dell - Stockage : défaillance de contrôleur	Une partie du disque physique est endommagée.	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : défaillance de canal	Défaillance de canal	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : informations du matériel de l'enceinte	Informations du matériel de l'enceinte	Informatif	Pas d'action
Dell - Stockage : avertissement du matériel de l'enceinte	Avertissement du matériel de l'enceinte	Avertissement	Pas d'action
Dell - Stockage : défaillance du matériel de l'enceinte	Erreur du matériel de l'enceinte	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : défaillance d'un disque de matrice	Défaillance d'un disque de matrice	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : défaillance d'EMM	Défaillance du EMM	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : défaillance de bloc d'alimentation	Défaillance de bloc d'alimentation	Erreur	Mettez le système en mode de maintenance

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Stockage : avertissement de sonde de température	Avertissement de capteur de température de disque physique (trop froid ou trop chaud).	Avertissement	Pas d'action
Dell - Stockage : défaillance de sonde de température	Erreur de capteur de température de disque physique (trop froid ou trop chaud).	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : défaillance de ventilateur	Défaillance du ventilateur	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : avertissement concernant la batterie	Avertissement de la batterie	Avertissement	Pas d'action
Dell - Stockage : avertissement de disque virtuel dégradé	Avertissement de disque virtuel dégradé	Avertissement	Pas d'action
Dell - Stockage : défaillance de disque virtuel dégradé	Défaillance de disque virtuel dégradé	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : informations de sonde de température	Informations de capteur de température	Informatif	Pas d'action
Dell - Stockage : avertissement de disque de matrice	Avertissement d'un disque de matrice	Avertissement	Pas d'action
Dell - Stockage : informations de disque de matrice	Informations d'un disque de matrice	Informatif	Pas d'action
Dell - Stockage : avertissement de bloc de bloc d'alimentation	Avertissement de bloc d'alimentation	Avertissement	Pas d'action
Dell - Défaillance de disque Fluid Cache	Défaillance de disque Fluid Cache	Erreur	Mettez le système en mode de maintenance
Dell - Défaillance de câble ou événement critique	Défaillance du câble ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Chassis Management Controller a détecté un avertissement	Le Chassis Management Controller a détecté un avertissement	Avertissement	Pas d'action
Dell - Chassis Management Controller a détecté une erreur	Le Chassis Management Controller a détecté une erreur	Erreur	Mettez le système en mode de maintenance
Dell - Échec de la virtualisation d'E/S ou événement critique	Échec de la virtualisation d'E/S ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement d'état du lien	Avertissement d'état du lien	Avertissement	Pas d'action
Dell - Échec de l'état du lien ou événement critique	Échec de l'état du lien ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement de sécurité	Avertissement de sécurité	Avertissement	Pas d'action
Dell - Système : avertissement de configuration du logiciel	Système : avertissement de configuration du logiciel	Avertissement	Pas d'action
Dell - Système : échec de configuration du logiciel	Système : échec de configuration du logiciel	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement de sécurité du stockage	Avertissement de sécurité du stockage	Avertissement	Pas d'action
Dell - Échec de sécurité du stockage ou événement critique	Échec de sécurité du stockage ou événement critique	Erreur	Mettez le système en mode de maintenance

Nom de l'événement	Description	Gravité	Action recommandée
Dell - Avertissement de mise à jour concernant le changement de logiciel	Avertissement de mise à jour concernant le changement de logiciel	Avertissement	Pas d'action
Dell - Avertissement concernant l'audit de Chassis Management Controller.	Avertissement concernant l'audit du Chassis Management Controller	Avertissement	Pas d'action
Dell - Échec d'audit de Chassis Management Controller ou événement critique	Échec d'audit de Chassis Management Controller ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement d'audit du périphérique PCI	Avertissement concernant l'audit du périphérique PCI	Avertissement	Pas d'action
Dell - Avertissement d'audit du bloc d'alimentation	Avertissement concernant l'audit du bloc d'alimentation	Avertissement	Pas d'action
Dell - Échec de l'audit du bloc d'alimentation ou événement critique	Échec de l'audit du bloc d'alimentation ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement d'audit de l'utilisation d'énergie	Avertissement d'audit de l'utilisation d'énergie	Avertissement	Pas d'action
Dell - Échec de l'audit de l'utilisation d'énergie ou événement critique	Échec de l'audit de l'utilisation d'énergie ou événement critique	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement de configuration de la sécurité	Avertissement de configuration de la sécurité	Avertissement	Pas d'action
Dell - Configuration : avertissement de configuration du logiciel	Configuration : avertissement de configuration du logiciel	Avertissement	Pas d'action
Dell - Configuration : échec de la configuration du logiciel	Configuration : échec de la configuration logicielle	Erreur	Mettez le système en mode de maintenance
Dell - Défaillance de partition de disque virtuel	Défaillance de partition de disque virtuel	Erreur	Mettez le système en mode de maintenance
Dell - Avertissement de partition de disque virtuel	Avertissement de partition de disque virtuel	Avertissement	Pas d'action

Événements iDRAC

REMARQUE : Pour tous les hôtes activés Proactive HA faisant partie d'un cluster, les événements de virtualisation suivants sont mappés aux événements Proactive HA ; à l'exception des événements « Les ventilateurs ne sont pas redondants » et « Les blocs d'alimentation ne sont pas redondants » ne sont pas mappés.

Les ventilateurs sont redondants	Aucun	Informatif	Pas d'action
La redondance du ventilateur est perdue	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Critique	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.
La redondance des ventilateurs est dégradée	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Avertissement	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.
Les ventilateurs ne sont pas redondants	Un ou plusieurs ventilateurs sont en panne ou ont été retirés	Informatif	Enlevez et réinstallez les ventilateurs qui sont en panne

Nom de l'événement	Description	Gravité	Action recommandée
	ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.		ou installez des ventilateurs supplémentaires.
Les ventilateurs ne sont pas redondants. Les ressources sont insuffisantes pour maintenir un fonctionnement normal	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Critique	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.
Les blocs d'alimentation sont redondants	Aucun	Informatif	Pas d'action
Perte de la redondance du bloc d'alimentation	Le mode opérationnel de l'alimentation actuel est non redondant en raison d'une exception de bloc d'alimentation, un changement d'inventaire de bloc d'alimentation ou un changement d'inventaire d'alimentation du système. Le système fonctionnait précédemment dans un mode de redondance de l'alimentation.	Critique	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation d'énergie
Dégradation de la redondance du bloc d'alimentation	Le mode opérationnel de l'alimentation actuel est non redondant en raison d'une exception de bloc d'alimentation, un changement d'inventaire de bloc d'alimentation ou un changement d'inventaire d'alimentation du système. Le système fonctionnait précédemment dans un mode de redondance de l'alimentation.	Avertissement	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation d'énergie
Les blocs d'alimentation ne sont pas redondants	La configuration actuelle de bloc d'alimentation ne correspond pas aux spécifications de la plateforme permettant la redondance. Si un bloc d'alimentation tombe en panne, le système peut s'arrêter.	Informatif	Lorsque cela n'est pas délibéré, vérifiez la configuration du système ainsi que la consommation électrique puis installez les blocs d'alimentation en conséquence. Vérifiez l'état des blocs d'alimentation afin de vérifier les pannes.
Les blocs d'alimentation ne sont pas redondants. Les ressources sont insuffisantes pour maintenir un fonctionnement normal	Le système peut s'éteindre ou fonctionner dans un état dégradé.	Critique	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation électrique puis mettez à niveau ou installez les blocs d'alimentation en conséquence.
Le double module SD interne est redondant	Aucun	Informatif	Pas d'action
Perte de la redondance du double module SD interne	L'une des cartes SD, ou les deux, ne fonctionnent pas correctement.	Critique	Remplacez la carte SD défectueuse.

Nom de l'événement	Description	Gravité	Action recommandée
Dégradation de la redondance du double module SD interne	L'une des cartes SD, ou les deux, ne fonctionne(nt) pas correctement.	Avertissement	Remplacez la carte SD défectueuse.
Le double module SD interne n'est pas redondant	Aucun	Informatif	Installez une carte SD supplémentaire et configurez-la de manière à bénéficier de la redondance si besoin.
Événements relatifs au châssis			
Perte de la redondance du bloc d'alimentation	Le mode opérationnel de l'alimentation actuel est non redondant en raison d'une exception de bloc d'alimentation, un changement d'inventaire de bloc d'alimentation ou un changement d'inventaire d'alimentation du système. Le système fonctionnait précédemment dans un mode de redondance de l'alimentation.	Critique	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation d'énergie
Dégradation de la redondance du bloc d'alimentation	Le mode opérationnel de l'alimentation actuel est non redondant en raison d'une exception de bloc d'alimentation, un changement d'inventaire de bloc d'alimentation ou un changement d'inventaire d'alimentation du système. Le système fonctionnait précédemment dans un mode de redondance de l'alimentation.	Avertissement	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation d'énergie
Les blocs d'alimentation sont redondants	Aucun	Informatif	Pas d'action
Les blocs d'alimentation ne sont pas redondants	La configuration actuelle de bloc d'alimentation ne correspond pas aux spécifications de la plateforme permettant la redondance. Si un bloc d'alimentation tombe en panne, le système peut s'arrêter.	Informatif	Lorsque cela n'est pas délibéré, vérifiez la configuration du système ainsi que la consommation électrique puis installez les blocs d'alimentation en conséquence. Vérifiez l'état des blocs d'alimentation afin de vérifier les pannes.
Les blocs d'alimentation ne sont pas redondants. Les ressources sont insuffisantes pour maintenir un fonctionnement normal	Le système peut s'éteindre ou fonctionner dans un état dégradé.	Critique	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation électrique puis mettez à niveau ou installez les blocs d'alimentation en conséquence.
La redondance du ventilateur est perdue	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Critique	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.

Nom de l'événement	Description	Gravité	Action recommandée
La redondance des ventilateurs est dégradée	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Avertissement	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.
Les ventilateurs sont redondants	Aucun	Informatif	Pas d'action
Les ventilateurs ne sont pas redondants	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Informatif	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.
Les ventilateurs ne sont pas redondants. Les ressources sont insuffisantes pour maintenir un fonctionnement normal	Un ou plusieurs ventilateurs sont en panne ou ont été retirés ou il y a eu une modification de la configuration, ce qui nécessite des ventilateurs supplémentaires.	Critique	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.

Événements Proactive HA

Selon les composants pris en charge par VMware pour Proactive HA, les événements suivants sont enregistrés par le fournisseur Dell Inc au cours de son enregistrement avec vCenter :

REMARQUE : L'état d'intégrité Proactive HA des composants pris en charge peut être normal (vert), avertissement (jaune), critique (rouge) ou inconnu (gris).

Tableau 26. Événements Dell Proactive HA

Événement du fournisseur Dell Inc	Type de composant	Description
DellFanRedundancy	Ventilateur	Événements de redondance des ventilateurs
DellPowerRedundancy	Bloc d'alimentation (PSU)	Événements de redondance de l'alimentation
DellDSDMRedundancy	Stockage	Événements de redondance de l'DSDM

Pour un hôte activé Proactive HA, les interruptions suivantes sont utilisées par OMIVV comme déclencheur pour déterminer l'intégrité redondante des composants : en fonction de l'information sur l'intégrité redondante, une mise à jour d'intégrité Proactive HA peut être envoyée au vCenter pour cet hôte. Ces interruptions ne sont pas transférées directement à un vCenter pour un hôte Proactive HA.

Tableau 27. Événements Proactive HA

Nom de l'événement	Description	Gravité
Informations du ventilateur	Informations du ventilateur	Informatif
Avertissement de ventilateur	Avertissement de ventilateur	Avertissement
Défaillance du ventilateur	Défaillance du ventilateur	Critique
Bloc d'alimentation normal	Le bloc d'alimentation revient à l'état normal	Informatif
Avertissement de bloc d'alimentation	Le bloc d'alimentation détecte un avertissement	Avertissement
Défaillance de bloc d'alimentation	Le bloc d'alimentation détecte une défaillance	Critique
Bloc d'alimentation absent	Le bloc d'alimentation est absent.	Critique
Informations de redondance	Informations de redondance	Informatif
Redondance dégradée	La redondance est dégradée	Avertissement

Nom de l'événement	Description	Gravité
Redondance perdue	La redondance est perdue	Critique
Informations relatives au double module SD intégré	Informations relatives au double module SD intégré (IDSDM)	Informatif
Avertissement du double module SD intégré	Avertissement du double module SD intégré	Avertissement
Échec du double module SD intégré	Échec du double module SD intégré	Critique
Absence du double module SD intégré	Le double module SD intégré est absent	Critique
Informations relatives à la redondance du double module SD intégré	Informations relatives à la redondance du double module SD intégré	Informatif
Dégradation de la redondance du double module SD intégré	Dégradation de la redondance du double module SD intégré	Avertissement
Perte de la redondance du double module SD intégré	Perte de la redondance du double module SD interne	Critique
Événements relatifs au châssis		
Informations du ventilateur	Informations du ventilateur	Informatif
Avertissement de ventilateur	Avertissement de ventilateur	Avertissement
Défaillance du ventilateur	Défaillance du ventilateur	Critique
Bloc d'alimentation normal	Le bloc d'alimentation revient à l'état normal	Informatif
Avertissement de bloc d'alimentation	Le bloc d'alimentation détecte un avertissement	Avertissement
Défaillance de bloc d'alimentation	Le bloc d'alimentation détecte une défaillance	Critique
Informations de redondance	Informations de redondance	Informatif
Redondance dégradée	La redondance est dégradée	Avertissement
Redondance perdue	La redondance est perdue	Critique

Affichage des paramètres d'alarme et événement

Après avoir configuré des alarmes et des événements, vous pouvez savoir si les alarmes vCenter des hôtes sont activées et connaître le niveau de publication d'événement sélectionné dans l'onglet Paramètres.

1. Dans l'onglet **Gérer > Paramètres** d'OpenManage Integration for VMware vCenter, sous **Paramètres vCenter**, développez **Événements et alarmes**.

Les options suivantes s'affichent :

- Alarmes vCenter des hôtes Dell EMC : la valeur affichée est **Activé** ou **Désactivé**.
- Niveau de publication d'événement

2. Configurer des événements et alarmes. Voir [Configuration des événements et alarmes](#).

Pour afficher les niveaux de publication d'événement, voir [À propos des événements et des alarmes](#).

Affichage des événements

Pensez à configurer les événements que vous souhaitez afficher dans l'onglet **Événements**. Voir [Configuration des événements et alarmes](#).

Affichez les événements d'un hôte, d'un cluster ou d'un centre de données spécifique dans l'onglet Événements.

1. Dans le navigateur Dell OpenManage Integration for VMware vCenter, cliquez sur **Hôtes**, **Centre de données** ou **Clusters**.
2. Dans l'onglet **Objets**, sélectionnez l'hôte, le centre de données ou le cluster spécifique dont vous voulez afficher les événements.
3. Dans l'onglet **Surveiller**, cliquez sur **Événements**.
4. Pour afficher les détails de l'événement, sélectionnez un événement spécifique.

Intégrité de la redondance des composants matériels - Proactive HA

- REMARQUE :** Seuls les serveurs qui prennent en charge l'état d'intégrité de la redondance pour les composants pris en charge (bloc d'alimentation, ventilateurs et IDSDM) sont pris en charge pour Proactive HA.
- REMARQUE :** Les stratégies configurées pour Proactive HA sur le cluster Proactive HA pourraient être affectées lorsque les alertes globales sont configurées via OMIVV.
- REMARQUE :** Proactive HA est disponible uniquement sur les plateformes prenant en charge la redondance sur l'alimentation, le ventilateur et le module IDSDM.
- REMARQUE :** La fonction Proactive HA n'est pas prise en charge pour les blocs d'alimentation pour lequel la redondance ne peut pas être configurée (par exemple, les blocs d'alimentation câblés).

Proactive HA est une fonctionnalité vCenter (vCenter 6.5 et versions ultérieures) active avec OMIVV. Lorsque vous activez Proactive HA, la fonctionnalité protège vos charges de travail de manière proactive en prenant des mesures basées sur la dégradation d'intégrité de la redondance des composants pris en charge dans un hôte.

- REMARQUE :** Tous les hôtes de PowerEdge de 12e génération et versions ultérieures et ESXi v6.0 et versions ultérieures qui font partie d'un profil de connexion et sont correctement répertoriés sont pris en charge pour Proactive HA.

Après avoir évalué l'état d'intégrité de la redondance des composants hôtes pris en charge, l'appliance OMIVV met à jour le changement d'état d'intégrité par rapport au serveur vCenter. Les états d'intégrité de la redondance disponibles pour les composants pris en charge (bloc d'alimentation, ventilateurs et IDSDM) sont :

- Intègre (informations) : le composant fonctionne normalement.
- Avertissement (modérément dégradé) : le composant est affecté d'une erreur non critique.
- Critique (gravement dégradé) : le composant est affecté d'une panne critique.

- REMARQUE :** Les états « modérément dégradé » et « gravement dégradé » sont représentés comme *Avertissement* dans la colonne Type sur la page Événements.

- REMARQUE :** Un état d'intégrité *Inconnu* signale l'indisponibilité d'une mise à jour d'intégrité Proactive HA depuis le fournisseur Dell Inc. L'état d'intégrité inconnu peut se produire lorsque :

- Tous les hôtes ajoutés à un cluster Proactive HA restent à l'état inconnu pendant quelques minutes jusqu'à ce qu'OMIVV les initialise avec leurs états appropriés.
- Un redémarrage du serveur vCenter rassemble les hôtes dans un cluster Proactive HA à l'état inconnu jusqu'à ce qu'OMIVV les réinitialise avec leurs états appropriés.

Lorsqu'OMIVV détecte un changement d'état d'intégrité de la redondance des composants pris en charge (en raison d'interruptions ou d'interrogations), la notification de mise à jour de l'intégrité pour ces composants est envoyée au serveur vCenter. L'interrogation s'exécute toutes les heures et est disponible sous forme d'un mécanisme sans échec pour couvrir la possibilité de perte d'interruption.

Configuration de Proactive HA pour les serveurs rack et tour

Pour configurer les serveurs rack et tour, procédez comme suit :

Assurez-vous que tous les hôtes sont correctement configurés pour la redondance des trois composants redondants pris en charge (bloc d'alimentation, ventilateurs et IDSDM).

1. Créez un profil de connexion et associez les hôtes à ce profil de connexion. Voir [Création d'un profil de connexion](#).
2. Vérifiez que l'inventaire des hôtes s'est terminé avec succès. Voir [Affichage de l'inventaire des hôtes](#).
3. Dans le contrôleur iDRAC, vérifiez que la destination d'interruption SNMP est définie sur l'adresse IP de l'appliance OMIVV.
 - REMARQUE :** Assurez-vous que depuis l'onglet **OpenManage Integration > Surveiller > Journal le journal des actions de l'utilisateur** confirme la disponibilité d'un hôte pour un cluster Proactive HA.
4. Activez Proactive HA sur un cluster. Voir [Activation de Proactive HA sur un cluster](#).

Configuration de Proactive HA pour les serveurs modulaires

Pour configurer les serveurs modulaires, procédez comme suit :

Avant de configurer Proactive HA pour les serveurs modulaires, assurez-vous que les conditions suivantes sont remplies :

- Tous les hôtes sont correctement configurés pour la redondance des trois composants redondants pris en charge (bloc d'alimentation, ventilateurs et IDSDM).
- L'inventaire des hôtes et du châssis s'est terminé avec succès.

REMARQUE : Il est recommandé que tous les hôtes modulaires dans un cluster Proactive HA ne se situent pas dans le même châssis, car un échec du châssis a une incidence sur tous ses ensembles.

1. Créez un profil de connexion et associez les hôtes à ce profil de connexion. Voir [Création d'un profil de connexion](#).
2. Vérifiez que l'inventaire des hôtes s'est terminé avec succès. Voir [Affichage de l'inventaire des hôtes](#).

REMARQUE : Assurez-vous que depuis l'onglet **OpenManage Integration > Surveiller > Journal le journal des actions de l'utilisateur confirme la disponibilité d'un hôte pour un cluster Proactive HA**.

3. Créez un profil de châssis pour le châssis associé. Voir [Création d'un profil de châssis](#).
4. Vérifiez que l'inventaire du châssis s'est terminé avec succès. Voir [Affichage de l'inventaire du châssis](#).
5. Lancez le contrôleur CMC et vérifiez que la destination d'interruption du châssis est définie sur l'adresse IP de l'appliance OMIVV.
6. Dans **Chassis Management Controller**, accédez à **Configuration > Général**.
7. Sur la page **Paramètres généraux du châssis**, sélectionnez **Activer la journalisation et les événements avancés pour le châssis**.
8. Activez Proactive HA sur un cluster. Voir [Activation de Proactive HA sur un cluster](#).

Activation de Proactive HA sur des clusters

Avant d'activer Proactive HA sur des clusters, assurez-vous que les conditions suivantes sont remplies :

- Un cluster dont les fonctions DRS sont activées est créé et configuré dans la console vCenter. Pour activer DRS dans un cluster, voir la documentation VMware.
- Tous les hôtes composant le cluster doivent faire partie d'un profil de connexion et être correctement répertoriés, et le châssis doit être muni d'un profil de châssis le cas échéant.

1. Dans OpenManage Integration, cliquez sur **Clusters**.
2. Sous **Clusters**, cliquez sur un cluster, sélectionnez **Configurer > Disponibilité vSphere**, puis cliquez sur **Modifier**. L'Assistant **Modifier les paramètres de cluster** s'affiche.
3. Cliquez sur **vSphere DRS** et sélectionnez l'option **Activer vSphere DRS**, si elle n'est pas activée.
4. Cliquez sur **Disponibilité vSphere** et sélectionnez l'option **Activer Proactive HA**, si elle n'est pas activée.
5. Dans le volet gauche, sous **Disponibilité vSphere**, cliquez sur **Échecs et réponses de Proactive HA**. L'écran **Échecs et réponses Proactive HA** s'affiche.
6. Sur l'écran **Échecs et réponses de Proactive HA**, développez le volet **Niveau d'automatisation**.
7. Pour le **Niveau d'automatisation**, sélectionnez **Manuel** ou **Automatique**.
8. Pour la **Correction**, sélectionnez le mode de quarantaine, le mode de maintenance ou une combinaison des deux modes en fonction de l'état de gravité (mode Mixte). Voir la documentation VMware pour plus d'informations.
9. Sous **Fournisseurs Proactive HA**, cochez la case afin de sélectionner le fournisseur Dell pour le cluster.
10. Cliquez sur **Modifier** en regard du fournisseur Dell sélectionné. La boîte de dialogue **Modifier les conditions d'échec bloqué** pour le fournisseur Proactive HA s'affiche.
11. Pour empêcher une condition d'échec de poster des événements, utilisez les cases à cocher pour sélectionner les événements (générés par des interruptions ou interrogations) dans le tableau **Conditions d'échec**.
Vous pouvez filtrer le contenu de la grille de données des conditions d'échec en utilisant le champ **Filtre**. Vous pouvez également glisser et déplacer des colonnes dans la grille de données des conditions d'échec. Les conditions d'échec peuvent être appliquées à un niveau cluster ou un niveau hôte.
12. Pour appliquer cette option à tous les hôtes actuels et futurs du cluster, sélectionnez la case à cocher **Niveau du cluster**.
13. Pour appliquer les modifications, dans **Modifier les conditions d'échec bloqué**, cliquez sur **OK** ou sur **Annuler** pour annuler.
14. Pour appliquer les modifications, dans l'Assistant **Modifier les paramètres de cluster**, cliquez sur **OK** ou sur **Annuler** pour annuler.

Une fois Proactive HA activé sur un cluster, OMIVV vérifie tous les hôtes du cluster et initialise l'état d'intégrité Proactive HA de tous les composants du serveur hôte pris en charge. OMIVV peut maintenant envoyer les notifications de mise à jour de l'intégrité pour les composants pris en charge au serveur vCenter. En fonction des notifications de mise à jour de l'intégrité envoyées par OMIVV, le serveur vCenter effectue l'action manuelle ou automatique que vous avez sélectionnée pour la **Correction**.

Pour remplacer la gravité existant, voir [Remplacement de la gravité des notifications de mise à jour de l'intégrité](#).

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, accédez à l'onglet **Gérer**, puis cliquez sur **Configuration de Proactive HA > Événements Proactive HA**.
2. Cliquez pour afficher des informations sur la liste des événements pris en charge.
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.
3. Pour modifier la gravité d'un hôte ou d'un de ses composants, dans la colonne **Remplacer la gravité**, sélectionnez l'état souhaité dans la liste déroulante.
Cette stratégie s'applique à tous les hôtes Proactive HA sur tous les serveurs vCenter qui sont enregistrés avec OMIVV.
4. Répétez l'étape 3 pour tous les événements devant être personnalisés.
5. Effectuez l'une des actions suivantes :
 - a) Pour enregistrer la personnalisation, cliquez sur **Appliquer les modifications**
 - b) Pour rétablir la gravité effacée après la sélection d'un niveau de gravité, cliquez sur **Annuler**.
 - c) Pour appliquer la gravité par défaut à la gravité remplacée, cliquez sur **Rétablir les valeurs par défaut**.

Lancement des consoles de gestion

Il existe trois consoles de gestion que vous pouvez lancer depuis le portlet Dell EMC Server Management. Elles incluent :

- Pour accéder à l'interface utilisateur de l'iDRAC, démarrez la console d'accès à distance. Voir [Lancement de la console d'accès à distance \(iDRAC\)](#).
- Pour accéder à l'interface utilisateur d'OpenManage Server Administrator, démarrez la console OMSA. Avant de démarrer console OMSA, l'URL d'OMSA doit être configuré dans OpenManage Integration for VMware vCenter. Voir [Lancement de la console OMSA](#).
- Pour accéder à l'interface utilisateur du châssis, cliquez sur la console de châssis lame. Voir [Lancement de la console du contrôleur de gestion du châssis \(CMC\)](#).

REMARQUE : Si vous êtes sur un système lame, lancez la console CMC pour lancer l'interface utilisateur du contrôleur de gestion du châssis. Si vous n'êtes pas sur un système lame, l'interface utilisateur du contrôleur de gestion du châssis ne s'affiche pas.

Lancement de la console Remote Access

Vous pouvez démarrer l'interface utilisateur de l'iDRAC depuis le portlet Dell EMC Server Management.

1. Dans OpenManage Integration for VMware vCenter, dans la zone Navigateur, sous Listes d'inventaire, cliquez sur **Hôtes**.
2. Dans l'onglet **Objet**, double-cliquez sur l'hôte de votre choix.
3. Dans l'onglet **Résumé**, faites défiler l'affichage jusqu'au portlet Dell EMC Server Management.
4. Cliquez sur **Consoles de gestion > Remote Access Console (iDRAC)**.

Lancement de la console OMSA

Avant de démarrer la console OMSA, vérifiez que vous avez défini l'URL d'OMSA et installé et configuré le serveur Web d'OMSA. Vous pouvez définir l'URL d'OMSA à partir de l'onglet **Paramètres**.

 **REMARQUE** : Installez OMSA pour surveiller et gérer les serveurs Dell PowerEdge de 11e génération à l'aide d'OpenManage Integration for VMware vCenter.

1. Dans OpenManage Integration for VMware vCenter, dans la zone Navigateur, sous Listes d'inventaire, cliquez sur **Hôtes**.
2. Dans l'onglet **Objet**, double-cliquez sur l'hôte de votre choix.
3. Dans l'onglet **Résumé**, faites défiler l'affichage jusqu'à **Informations sur l'hôte Dell EMC**.
4. Dans la section **Informations sur l'hôte Dell EMC**, cliquez sur **Console OMSA**.

Lancement de la console Chassis Management Controller

Vous pouvez démarrer l'interface utilisateur de l'iDRAC à partir du portlet Dell EMC Server Management.

1. Dans OpenManage Integration for VMware vCenter, dans la zone Navigateur, sous Listes d'inventaire, cliquez sur **Hôtes**.
2. Dans l'onglet **Objet**, double-cliquez sur le serveur lame de votre choix.
3. Dans l'onglet **Récapitulatif**, faites défiler l'affichage jusqu'au portlet Dell EMC Server Management.
4. Cliquez sur **Consoles de gestion** > **Console du contrôleur de gestion de châssis (CMC)**.

À propos des mises à jour de micrologiciel

L'appliance OMIVV vous permet d'effectuer des tâches de mise à jour du BIOS et du micrologiciel sur les hôtes gérés. Vous pouvez effectuer des tâches de mise à jour de micrologiciel simultanées sur plusieurs clusters ou hôtes non mis en cluster. L'exécution simultanée d'une mise à jour de micrologiciel sur deux hôtes du même cluster n'est pas autorisée.

Le tableau suivant répertorie le nombre de tâches de mise à jour de micrologiciel que vous pouvez exécuter simultanément dans divers modes de déploiement, bien que vous puissiez planifier autant de tâches de mise à jour de micrologiciel que vous le souhaitez :

Tableau 28. Tâches de mise à jour de micrologiciel dans divers modes de déploiement

Mode de déploiement Petit	Mode de déploiement Moyen	Mode de déploiement Grand
5	10	15

Voici les deux méthodes permettant d'effectuer une mise à jour de micrologiciel :

- DUP unique : effectue une mise à jour de micrologiciel pour l'iDRAC, le BIOS ou le LC en pointant directement vers l'emplacement du DUP (partage CIFS ou NFS). La méthode DUP unique peut être utilisée uniquement au niveau de l'hôte.

Référentiel : exécute le BIOS et toutes les mises à jour de micrologiciel prises en charge. Cette méthode peut être utilisée à la fois au niveau hôte et au niveau cluster. Voici les deux emplacements de référentiel :

- Dell Online : l'emplacement utilise la logithèque Dell de mise à jour du micrologiciel (ftp.dell.com). OpenManage Integration for VMware vCenter télécharge les mises à jour de micrologiciel sélectionnées dans le référentiel Dell et met à jour les hôtes gérés.
 - ❗ **REMARQUE : En fonction des paramètres réseau, activez les paramètres de proxy, si le réseau a besoin d'un proxy.**
- Dossier de réseau partagé : vous pouvez conserver un référentiel local du micrologiciel dans un partage réseau CIFS ou NFS. Ce référentiel peut soit servir de dépôt pour Server Update Utility (SUU) que Dell utilise pour proposer des mises à jour périodiques ou de référentiel personnalisé créé à l'aide de DRM. Ce partage réseau doit être accessible par OMIVV.
 - ❗ **REMARQUE : Si vous utilisez le partage CIFS, les mots de passe de référentiel ne peuvent pas dépasser 31 caractères. N'utilisez pas les caractères suivants dans un mot de passe : @, &, %, ', ", , (virgule), <>.**
 - ❗ **REMARQUE : Assurez-vous d'utiliser la dernière version DRM (3.x) ou une version ultérieure.**

Pour en savoir plus sur la configuration des référentiels de mise à jour du micrologiciel, voir [Configuration du référentiel de mise à jour du micrologiciel](#).

L'**Assistant Mise à jour du micrologiciel** vérifie toujours les niveaux minimum du micrologiciel d'iDRAC, BIOS et Lifecycle Controller, et tente de les mettre à jour aux versions minimales requises. Voir la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter* pour plus d'informations sur les niveaux minimums de micrologiciel pour l'iDRAC, le BIOS et Lifecycle Controller. Lorsque les versions du micrologiciel d'iDRAC, BIOS et Lifecycle Controller satisfont les conditions minimales, le processus de mise à jour du micrologiciel permet d'effectuer les mises à jour de toutes les versions du micrologiciel, y compris : iDRAC, Lifecycle Controller, RAID, carte réseau / LOM, bloc d'alimentation, BIOS, etc.

Sujets :

- [Exécution de la mise à jour du micrologiciel pour un hôte non vSAN](#)
- [Exécution de l'Assistant Mise à jour du micrologiciel pour un hôte vSAN](#)
- [Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters non vSAN](#)
- [Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters vSAN](#)

Exécution de la mise à jour du micrologiciel pour un hôte non vSAN

❗ **REMARQUE : Pendant le processus de mise à jour du micrologiciel, veillez à ne pas supprimer les éléments suivants :**

- Hôte de vCenter visé par la tâche de mise à jour de micrologiciel en cours.

• Profil de connexion de l'hôte visé par la tâche de mise à jour de micrologiciel en cours.

Pour effectuer la mise à jour de micrologiciel pour un hôte non vSAN, effectuez les étapes suivantes :

1. Pour accéder à l'Assistant Mise à jour de micrologiciel, accédez à OpenManage Integration, puis cliquez sur **Hôtes** et effectuez l'une des opérations suivantes :

- Cliquez avec le bouton droit de la souris sur **Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Sur la page **Hôtes**, cliquez sur un hôte, puis sélectionnez **Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Dans le volet **Navigateur**, sélectionnez un hôte, puis cliquez sur **Récapitulatif > Informations d'hôte Dell EMC > Exécuter l'Assistant Micrologiciel**.
- Dans le volet **Navigateur**, sélectionnez un hôte, puis cliquez sur **Surveiller > Informations d'hôte Dell EMC > Micrologiciel > Exécuter l'Assistant Micrologiciel**.

OMIVV vérifie la conformité de l'hôte et si toute autre tâche de mise à jour de micrologiciel est en cours dans n'importe quel hôte au sein du même cluster. Une fois la vérification effectuée, l'Assistant **Mise à jour du micrologiciel** s'affiche.

REMARQUE : Si vous effectuez la mise à niveau d'une version antérieure d'OMIVV à la version disponible alors qu'une tâche de mise à jour de micrologiciel est déjà planifiée, vous pouvez lancer l'Assistant Mise à jour de micrologiciel sur le même hôte après avoir sauvegardé la base de données d'OMIVV et l'avoir restaurée avec la version disponible.

2. Lisez les instructions indiquées sur la page **Bienvenue**, puis cliquez sur **Suivant**.

La page **Sélectionner une source de mise à jour** s'affiche.

3. Sur la page **Sélectionner une source de mise à jour**, sélectionnez l'une des actions suivantes :

- a) L'**Emplacement de la logithèque actuel** s'affiche et sélectionne le lot de mises à jour de micrologiciel dans la liste déroulante **Sélectionner un lot de mises à jour**.

REMARQUE : Les lots 64 bits ne sont pas pris en charge sur les hôtes de 12e génération avec la version 1.51 ou une version antérieure d'iDRAC.

REMARQUE : Les lots 64 bits ne sont pas pris en charge sur les hôtes de 11e génération sur toutes les versions d'iDRAC.

REMARQUE : OMIVV prend en charge les lots 32 et 64 bits pour la mise à jour de micrologiciel. En plus des lots mentionnés, OMIVV crée également un lot hybride lorsque plusieurs lots 32 et 64 bits sont disponibles dans le catalogue pour un modèle particulier, avec le même ID de version.

- b) Pour charger une seule mise à jour de micrologiciel depuis un fichier, sélectionnez **DUP unique**. Si vous sélectionnez **DUP unique**, passez à l'étape 6.

Un DUP unique peut résider sur un partage CIFS ou NFS qui est accessible par l'appliance virtuelle. Saisissez l'**Emplacement du fichier** dans l'un des formats suivants :

- Partage NFS : <hôte> :/<chemin_partage/NomFichier.exe
- Partage CIFS : \\<chemin de partage accessible d'hôte>\<NomFichier>.exe

Pour le partage CIFS, OMIVV vous invite à entrer le nom d'utilisateur et le mot de passe dans un format de domaine capable d'accéder au lecteur de partage.

REMARQUE : Les caractères @, % et , ne sont pas pris en charge dans les noms d'utilisateur et les mots de passe du dossier de réseau partagé.

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

4. Cliquez sur **Suivant**.

La page **Sélectionner les composants** s'affiche.


5. À l'aide des cases à cocher, sélectionnez au moins un composant de micrologiciel dans la liste, puis cliquez sur **Suivant**.

Il est impossible de sélectionner les composants qui sont dans une rétrogradation ou dont la mise à jour est déjà planifiée. Vous pouvez sélectionner les composants qui sont répertoriés pour une rétrogradation en sélectionnant l'option **Autoriser la rétrogradation**.

La page **Planifier une mise à jour de micrologiciel** s'affiche.

REMARQUE : Lorsque vous effectuez la mise à niveau d'une version antérieure d'OMIVV à la version disponible, le champ **Redémarrage nécessaire** est défini sur « Non » pour tous les composants, sauf si vous actualisez le référentiel de mise à jour de micrologiciel.

Pour filtrer des valeurs séparées par des virgules provenant du contenu des divers composants de la grille de données, utilisez le champ **Filtre**.

Vous pouvez également faire glisser les colonnes dans la grille des données des composants. Si vous souhaitez exporter à partir de l'Assistant, cliquez sur .

REMARQUE : Si vous sélectionnez des composants qui nécessitent un redémarrage, assurez-vous que l'environnement vCenter est configuré de sorte que les charges de travail puissent être migrées.

6. Sur la page **Planifier une mise à jour du micrologiciel**, procédez comme suit :

a) Spécifiez le nom de la tâche dans le champ **Nom de la tâche de mise à jour de micrologiciel** et, si vous le souhaitez, spécifiez également la description de cette tâche dans le champ **Description de la mise à jour de micrologiciel**.

Le nom de la tâche de mise à jour du micrologiciel est obligatoire et empêche l'utilisation d'un nom existant. Si vous supprimez la tâche de mise à jour du micrologiciel, vous pouvez réutiliser son nom.

b) Saisissez la valeur d'expiration du délai en mode maintenance (en minutes). Si le temps d'attente dépasse le temps indiqué, la tâche de mise à jour échoue et la tâche d'entrée en mode maintenance sera annulée ou expirera. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.

REMARQUE : La valeur minimale d'expiration du délai en mode maintenance est de 60 minutes.

REMARQUE : La valeur maximale d'expiration du délai en mode maintenance est d'un jour.

c) Sélectionnez l'une des options suivantes :

- Sélectionnez **Mettre à jour maintenant** pour démarrer immédiatement la tâche de mise à jour du micrologiciel.

Par défaut, l'option *Quitter le mode de maintenance après la mise à jour du micrologiciel* est sélectionnée.

Par défaut, l'option *Déplacer les machines virtuelles hors tensions et suspendues sur d'autres hôtes du cluster* est sélectionnée. La désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.

- Pour exécuter la tâche de mise à jour du micrologiciel ultérieurement, sélectionnez **Planifier la mise à jour**. Vous pouvez planifier la tâche de mise à jour du micrologiciel pour qu'elle intervienne 30 minutes plus tard.
 - Dans la zone Calendrier sélectionnez les mois et jour.
 - Dans la zone de texte Heure, saisissez l'heure au format HH:MM. L'heure est celle de l'appliance OMIVV.
- Pour éviter une interruption de service, sélectionnez **Appliquer les mises à jour lors du prochain redémarrage**.
- Pour appliquer la mise à jour et redémarrer même si l'hôte n'est pas en mode maintenance, sélectionnez **Appliquer les mises à jour et forcer le redémarrage sans passer en mode maintenance**. Cette méthode n'est pas recommandée.

7. Cliquez sur **Suivant**.

La page **Récapitulatif** indique les détails de tous les composants après la mise à jour du micrologiciel.

8. Cliquez sur **Terminer**.

La tâche de mise à jour du micrologiciel prend plusieurs minutes et sa durée varie en fonction du nombre de composants qui y sont inclus. Vous pouvez afficher l'état des tâches de mise à jour du micrologiciel sur la page **File d'attente des tâches**. Pour accéder à la page File d'attente des tâches, dans OpenManage Integration, sélectionnez **Surveiller > File d'attente des tâches > Mises à jour du micrologiciel**. Une fois la tâche de mise à jour du micrologiciel terminée, l'inventaire s'exécute automatiquement sur les hôtes sélectionnés et les hôtes quittent automatiquement le mode de maintenance si l'option correspondante est sélectionnée sur la page **Planifier une mise à jour du micrologiciel**.

Exécution de l'Assistant Mise à jour du micrologiciel pour un hôte vSAN

Assurez-vous que les conditions préalables suivantes sont respectées avant de planifier la mise à jour :

- L'option DRS est activée.
- L'hôte n'est pas en mode de maintenance.
- Les objets de données vSAN sont intègres.

Pour ignorer les vérifications ci-dessus, décochez la case **Vérifier les conditions requises** sur la page **Planifier une mise à jour du micrologiciel**.

- Les versions des pilotes et du micrologiciel sélectionnées sont conformes aux directives VMware vSAN. Les pilotes sélectionnés sont installés avant la mise à jour du micrologiciel.
- Le cluster répond aux exigences vSAN pour l'option de migration de données sélectionnée.
- Exécutez de nouveau l'inventaire après avoir activé vSAN.

REMARQUE : Pendant le processus de mise à jour du micrologiciel, Dell EMC recommande de ne pas supprimer les éléments suivants :

- **Hôte de vCenter visé par la tâche de mise à jour de micrologiciel en cours.**
- **Profil de connexion de l'hôte visé par la tâche de mise à jour de micrologiciel en cours.**

Pour effectuer la mise à jour de micrologiciel pour un seul hôte, effectuez les étapes suivantes :

1. Pour accéder à l'Assistant Mise à jour de micrologiciel, accédez à OpenManage Integration, puis cliquez sur **Hôtes** et effectuez l'une des opérations suivantes :
 - Cliquez avec le bouton droit de la souris sur **Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
 - Sur la page **Hôtes**, cliquez sur un hôte, puis sélectionnez **Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
 - Dans le volet **Navigateur**, sélectionnez un hôte, puis cliquez sur **Récapitulatif > Informations d'hôte Dell EMC > Exécuter l'Assistant Micrologiciel**.
 - Dans le volet **Navigateur**, sélectionnez un hôte, puis cliquez sur **Surveiller > Informations d'hôte Dell EMC > Micrologiciel > Exécuter l'Assistant Micrologiciel**.

OMIVV vérifie la conformité de l'hôte et si toute autre tâche de mise à jour du micrologiciel est en cours dans n'importe quel hôte au sein du même cluster. Une fois la vérification effectuée, l'Assistant **Mise à jour du micrologiciel** s'affiche.

REMARQUE : Si vous effectuez la mise à niveau d'une version antérieure d'OMIVV à la version disponible alors qu'une tâche de mise à jour de micrologiciel est déjà planifiée, vous pouvez lancer l'Assistant Mise à jour de micrologiciel sur le même hôte après avoir sauvegardé la base de données d'OMIVV et l'avoir restaurée avec la version disponible.

2. Lisez les instructions indiquées sur la page **Bienvenue**, puis cliquez sur **Suivant**.

La page **Sélectionner une source de mise à jour** s'affiche.

3. Sur la page **Sélectionner une source de mise à jour**, procédez comme suit :

- a) Sélectionnez le profil de logithèque de pilotes, le profil de logithèque de micrologiciels ou une combinaison des deux depuis la liste déroulante.

Si la logithèque de la ligne de base est associée dans profil de cluster, les logithèques associées de micrologiciels et de pilotes sont sélectionnées automatiquement.
- b) Sélectionnez un lot approprié dans le menu déroulant **Sélectionner un lot de mise à jour**.

Si la logithèque de pilotes est sélectionnée, la page **Sélection de pilotes** s'affiche. La page affiche les détails des composants du pilote, tels que le **Nom d'hôte**, le **Numéro de service**, le **Nom du composant**, le **Fournisseur**, le **Nom du package**, l'**État actuel**, la **Disponibilité**, la **Mise à jour applicable** et le **Redémarrage requis**.
- c) Sur la page **Sélection de pilotes**, sélectionnez le composant de pilote que vous souhaitez mettre à jour, puis cliquez sur **Suivant**.


Lorsque vous sélectionnez un composant de pilote pour le mettre à jour, tous les composants du package sont sélectionnés. Si la logithèque de micrologiciels est sélectionnée, la page **Sélectionner les composants** s'affiche. La page affiche les détails des composants tels que le **Nom d'hôte**, le **Numéro de service**, le **Nom du modèle**, le **Composant**, l'**État actuel**, la **Disponibilité**, l'**Importance** et le **Redémarrage requis**.
- d) À l'aide des cases à cocher, sélectionnez au moins un composant de micrologiciel dans la liste, puis cliquez sur **Suivant**.

Il est impossible de sélectionner les composants qui sont dans une rétrogradation ou dont la mise à jour est déjà planifiée. Vous pouvez sélectionner les composants qui sont répertoriés pour une rétrogradation en sélectionnant l'option **Autoriser la rétrogradation**.

La page **Planifier une mise à jour du micrologiciel** s'affiche.

Pour filtrer des valeurs séparées par des virgules provenant du contenu des divers composants de la grille de données, utilisez le champ **Filtre**.

Vous pouvez également faire glisser les colonnes dans la grille des données des composants. Si vous souhaitez exporter à partir de

l'Assistant, cliquez sur .

REMARQUE : Si vous sélectionnez des composants qui nécessitent un redémarrage, assurez-vous que l'environnement vCenter est configuré de sorte que les charges de travail puissent être migrées.

4. Sur la page **Planifier une mise à jour du micrologiciel**, procédez comme suit :

- a) Spécifiez le nom de la tâche dans le champ **Nom de la tâche de mise à jour de micrologiciel** et, si vous le souhaitez, spécifiez également la description de cette tâche dans le champ **Description de la mise à jour de micrologiciel**.

Le nom de la tâche de mise à jour de micrologiciel est obligatoire et empêche l'utilisation d'un nom existant. Si vous supprimez le nom d'une tâche de mise à jour de micrologiciel, vous pouvez le réutiliser.

REMARQUE : Par défaut, la case **Vérifier les conditions requises** est cochée. La tâche de mise à jour du micrologiciel est interrompue si :

- L'option **DRS n'est pas activée**.

- **Le mode de maintenance est activé pour certains hôtes du cluster.**
- **Les objets vSAN ne sont pas intègres.**

b) Saisissez la valeur d'expiration du délai en mode maintenance (en minutes). Si le temps d'attente dépasse le temps indiqué, la tâche de mise à jour échoue et la tâche d'entrée en mode maintenance sera annulée ou expirera. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.

REMARQUE : La valeur minimale d'expiration du délai en mode maintenance est de 60 minutes.

REMARQUE : La valeur maximale d'expiration du délai en mode maintenance est d'un jour.

c) Sélectionnez l'une des options suivantes :

- Sélectionnez **Mettre à jour maintenant** pour démarrer immédiatement la tâche de mise à jour du micrologiciel.
Par défaut, l'option *Quitter le mode de maintenance après la mise à jour du micrologiciel* est sélectionnée.
Par défaut, l'option *Déplacer les machines virtuelles hors tensions et suspendues sur d'autres hôtes du cluster* est sélectionnée. La désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.
- Pour exécuter la tâche de mise à jour du micrologiciel ultérieurement, sélectionnez **Planifier la mise à jour**. Vous pouvez planifier la tâche de mise à jour du micrologiciel pour qu'elle intervienne 30 minutes plus tard.
 - Dans la zone Calendrier sélectionnez les mois et jour.
 - Dans la zone de texte Heure, saisissez l'heure au format HH:MM. L'heure est celle de l'appliance OMIVV.
- Pour éviter une interruption de service, sélectionnez **Appliquer les mises à jour lors du prochain redémarrage**.
- Pour appliquer la mise à jour et redémarrer même si l'hôte n'est pas en mode maintenance, sélectionnez **Appliquer les mises à jour et forcer le redémarrage sans passer en mode maintenance**. Cette méthode n'est pas recommandée.

5. Cliquez sur **Suivant**.

La page **Récapitulatif** indique les détails de tous les composants après la mise à jour du micrologiciel.

6. Cliquez sur **Terminer**.

La tâche de mise à jour du micrologiciel prend plusieurs minutes et sa durée varie en fonction du nombre de composants qui y sont inclus. Vous pouvez afficher l'état des tâches de mise à jour du micrologiciel sur la page **File d'attente des tâches**. Pour accéder à la page File d'attente des tâches, dans OpenManage Integration, sélectionnez **Surveiller > File d'attente des tâches > Mises à jour du micrologiciel**. Une fois la tâche de mise à jour du micrologiciel terminée, l'inventaire s'exécute automatiquement sur les hôtes sélectionnés et les hôtes quittent automatiquement le mode de maintenance si l'option correspondante est sélectionnée sur la page **Planifier une mise à jour du micrologiciel**.

Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters non vSAN

OMIVV vous permet d'effectuer des mises à jour du BIOS et du micrologiciel sur tous les hôtes d'un cluster. L'Assistant met uniquement à jour les hôtes qui font partie d'un profil de connexion et qui sont conformes en termes de micrologiciel, d'état CSIOR, d'hyperviseur et d'état OMSA (serveurs de 11e génération uniquement). OMIVV effectue une mise à jour du micrologiciel adaptée au cluster si l'option Distribute Resource Scheduling (DRS) est active sur le cluster, en migrant la charge de travail lorsqu'un hôte passe en mode de maintenance ou le quitte.

Assurez-vous que les conditions suivantes sont remplies avant d'exécuter l'Assistant Mise à jour du micrologiciel :

- La logithèque de mise à jour du micrologiciel est déjà définie. Pour obtenir des informations sur la configuration du référentiel de mise à jour de micrologiciel, voir la section [Configuration du référentiel de mise à jour de micrologiciel](#).
- Il n'y a pas de tâches de mise à jour de micrologiciel actives pour tous les hôtes du cluster que vous mettez à jour.
- Les hôtes du cluster sont ajoutés à un profil de connexion et l'inventaire est exécuté avec succès.
- L'option DRS est activée.

REMARQUE : VMware recommande de créer les clusters avec du matériel de serveur identique.

REMARQUE : Pendant le processus de mise à jour du micrologiciel, Dell EMC recommande de ne pas supprimer les éléments suivants :

- **le ou les hôtes d'un cluster de vCenter pour lesquels la tâche de mise à jour du micrologiciel est en cours ;**
- **le profil de connexion du ou des hôtes d'un cluster pour lesquels la tâche de mise à jour du micrologiciel est en cours.**

1. Pour lancer l'Assistant Mise à jour du micrologiciel, dans OpenManage Integration, cliquez sur **Clusters** et effectuez l'une des sous-opérations suivantes :

- Cliquez sur un cluster, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Dans l'onglet **Objets**, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Cliquez sur un cluster, sélectionnez **Surveiller > Informations du cluster Dell EMC > Micrologiciel**. Dans l'écran **Micrologiciel**, cliquez sur le lien **Assistant Exécution du micrologiciel**.
- Cliquez avec le bouton droit de la souris sur un cluster, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.

OMIVV vérifie la conformité de l'hôte et si toute autre tâche de mise à jour du micrologiciel est en cours dans n'importe quel hôte au sein du même cluster. Une fois la vérification effectuée, la page **Mise à jour du micrologiciel** s'affiche.

2. Lisez les instructions indiquées dans la page **Bienvenue**, puis cliquez sur **Suivant**.
La page **Sélectionner les serveurs** s'affiche.
3. Sur la page **Sélectionner les serveurs**, dans l'arborescence **Nom**, utilisez les cases à cocher pour sélectionner les hôtes.
4. Cliquez sur **Suivant**.

La page **Sélectionner une source de mise à jour** s'affiche et vous pouvez sélectionner les lots. L'emplacement de la logithèque s'affiche également.

5. Sur la page **Sélectionner une source de mise à jour**, chaque modèle de l'hôte sélectionné dispose d'une liste déroulante en regard du nom de modèle, dans laquelle vous pouvez sélectionner le lot requis. Sélectionnez le lot requis pour la mise à jour du micrologiciel.

REMARQUE : OMIVV prend en charge les lots 32 et 64 bits pour la mise à jour de micrologiciel. En plus de ces lots, OMIVV crée également un lot hybride lorsque plusieurs lots 32 et 64 bits disponibles dans le catalogue pour un modèle particulier possèdent le même ID de version.

REMARQUE : Les lots 64 bits ne sont pas pris en charge sur les hôtes de 12e génération avec la version 1.51 ou une version antérieure d'iDRAC.

REMARQUE : Les lots 64 bits ne sont pas pris en charge sur les hôtes de 11e génération sur toutes les versions d'iDRAC.


6. Cliquez sur **Suivant**.
La page **Sélectionner les composants** s'affiche. La page affiche les détails des composants tels que le **Nom d'hôte**, le **Numéro de service**, le **Nom du modèle**, le **Composant**, l'**État actuel**, la **Disponibilité**, l'**Importance** et le **Redémarrage requis**.

7. Dans la page **Sélectionner les composants**, utilisez les cases à cocher pour sélectionner au moins un composant dans la liste, puis cliquez sur **Suivant** pour continuer.

Il est impossible de sélectionner les composants qui sont dans une rétrogradation ou dont la mise à jour est déjà planifiée. Vous pouvez sélectionner les composants qui sont répertoriés pour une rétrogradation en sélectionnant l'option **Autoriser la rétrogradation**.

Pour filtrer des valeurs séparées par des virgules provenant du contenu des divers composants de la grille de données, utilisez le champ **Filtre**.

Vous pouvez également faire glisser les colonnes dans la grille des données des composants. Si vous souhaitez exporter à partir de

l'Assistant, cliquez sur .

8. Sur la page **Informations de mise à jour du micrologiciel**, vous pouvez afficher tous les détails de mise à jour du micrologiciel.
9. Cliquez sur **Suivant**.

La page **Planifier une mise à jour du micrologiciel** s'affiche.

- a) Saisissez le nom de la tâche de mise à jour de micrologiciel dans le champ **Nom de la tâche de mise à jour de micrologiciel**.
Le nom de la tâche de mise à jour du micrologiciel est obligatoire et empêche l'utilisation d'un nom existant. Si vous supprimez le nom d'une tâche de mise à jour du micrologiciel, vous pouvez le réutiliser.
- b) Saisissez la description de la mise à jour du micrologiciel dans le champ **Description de la mise à jour du micrologiciel**. Cette valeur est facultative.
- c) Saisissez la valeur d'expiration du délai en mode maintenance (en minutes). Si le temps d'attente dépasse le temps indiqué, la tâche de mise à jour échoue et la tâche d'entrée en mode maintenance sera annulée ou expirera. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.

REMARQUE : La valeur minimale d'expiration du délai en mode maintenance est de 60 minutes.

REMARQUE : La valeur maximale d'expiration du délai en mode maintenance est d'un jour.

- d) Sous **Planifier des mises à jour de micrologiciel**, sélectionnez une option parmi les suivantes :

- Pour exécuter la tâche de mise à jour maintenant, cliquez sur **Mettre à jour maintenant**.
- Pour exécuter la tâche de mise à jour ultérieurement, cliquez sur **Planifier une mise à jour**, puis effectuez les sous-opérations suivantes :

1. Dans la zone **Calendrier** sélectionnez les mois et jour.

2. Dans la zone de texte **Heure**, saisissez l'heure au format HH:MM.

10. Cliquez sur **Suivant**.

La page **Résumé** s'affiche.

11. Dans la page **Résumé**, cliquez sur **Terminer**. Le message **La tâche de mise à jour de micrologiciel a été créée avec succès** s'affiche.

La tâche de mise à jour du micrologiciel prend plusieurs minutes et sa durée varie en fonction du nombre d'hôtes sélectionnés et du nombre de composants présents dans chaque hôte. Vous pouvez afficher l'état des tâches de mise à jour du micrologiciel sur la page **File d'attente des tâches**. Pour accéder à la page File d'attente des tâches, dans OpenManage Integration, sélectionnez **Surveiller > File d'attente des tâches > Mises à jour du micrologiciel**. Une fois que la tâche de mise à jour du micrologiciel est terminée, l'inventaire s'exécute automatiquement sur les hôtes sélectionnés et les hôtes quittent automatiquement le mode maintenance.

Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters vSAN

Assurez-vous que les conditions suivantes sont remplies avant d'exécuter l'Assistant Mise à jour du micrologiciel :

- L'option DRS est activée.
- Les hôtes ne sont pas en mode de maintenance.
- Les objets de données vSAN sont intègres. Si les objets vSAN ne sont pas intègres pour le premier hôte, la tâche de mise à jour du micrologiciel échoue. Pour d'autres hôtes, il attend 60 minutes afin que l'intégrité des objets vSAN soit rétablie.
- Les pilotes et le micrologiciel sélectionnés sont conformes aux directives VMware vSAN. Les pilotes sélectionnés sont installés avant la mise à jour du micrologiciel.
- Le cluster répond aux exigences vSAN pour l'option de migration de données sélectionnée. Il est fortement recommandé de sélectionner la logithèque de pilotes ou de micrologiciels référencée (Profil de cluster).
- Vous devez créer un profil de logithèque de pilotes et un profil de logithèque de micrologiciels avant de commencer la mise à jour du micrologiciel. Pour plus d'informations sur la création de logithèques de pilotes et de micrologiciels, voir [Création d'un profil de logithèque](#).
- Il n'y a pas de tâches de mise à jour de micrologiciel actives pour tous les hôtes du cluster que vous mettez à jour.
- Les hôtes du cluster sont ajoutés à un profil de connexion et l'inventaire est exécuté avec succès.
- Exécutez de nouveau l'inventaire après avoir activé le vSAN.

REMARQUE : VMware recommande de créer les clusters avec du matériel de serveur identique.

REMARQUE : Pendant le processus de mise à jour du micrologiciel, Dell EMC recommande de ne pas supprimer les éléments suivants :

- **le ou les hôtes d'un cluster de vCenter pour lesquels la tâche de mise à jour du micrologiciel est en cours ;**
- **le profil de connexion du ou des hôtes d'un cluster pour lesquels la tâche de mise à jour du micrologiciel est en cours.**
- **Les logithèques situées dans CIFS ou NFS.**

1. Pour lancer l'Assistant Mise à jour du micrologiciel, dans **OpenManage Integration**, cliquez sur **Clusters** et effectuez l'une des sous-opérations suivantes :

- Cliquez sur un cluster, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Dans l'onglet **Objets**, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.
- Cliquez sur un cluster, sélectionnez **Surveiller > Informations du cluster Dell EMC > Micrologiciel**. Dans l'écran **Micrologiciel**, cliquez sur le lien **Assistant Exécution du micrologiciel**.
- Cliquez avec le bouton droit de la souris sur un cluster, sélectionnez **Actions > Toutes les actions OpenManage Integration > Mise à jour du micrologiciel**.

OMIVV vérifie la conformité de l'hôte et si toute autre tâche de mise à jour du micrologiciel est en cours dans n'importe quel hôte au sein du même cluster. Une fois la vérification effectuée, la page **Mise à jour du micrologiciel** s'affiche.

2. Lisez les instructions indiquées dans la page **Bienvenue**, puis cliquez sur **Suivant**.

La page **Sélectionner les serveurs** s'affiche.

3. Sur la page **Sélectionner les serveurs**, dans l'arborescence **Nom**, utilisez les cases à cocher pour sélectionner les hôtes.

4. Cliquez sur **Suivant**.

La page **Sélectionner une source de mise à jour** s'affiche.

5. Sur la page **Sélectionner une source de mise à jour**, procédez comme suit :

- a) Sélectionnez le profil de logithèque de pilotes, le profil de logithèque de micrologiciels ou une combinaison des deux depuis la liste déroulante.

Si la logithèque de la ligne de base est associée dans profil de cluster, les logithèques associées de micrologiciels et de pilotes sont sélectionnées automatiquement.

Par défaut, le nom du modèle de l'hôte est sélectionné dans la zone **Sélectionner les lots**.

- b) Si la logithèque de micrologiciels est sélectionnée, chaque modèle de l'hôte sélectionné dispose d'une liste déroulante en regard du nom de modèle, dans laquelle vous pouvez sélectionner le lot requis pour la mise à jour du micrologiciel. Sélectionnez le lot souhaité dans la liste déroulante, puis cliquez sur **Suivant**.

Si la logithèque de pilotes est sélectionnée, la page **Sélection de pilotes** s'affiche. La page affiche les détails des composants du pilote, tels que le **Nom d'hôte**, le **Numéro de service**, le **Nom du composant**, le **Fournisseur**, le **Nom du package**, l'**État actuel**, la **Disponibilité**, la **Mise à jour applicable** et le **Redémarrage requis**.

REMARQUE : OMIVV prend en charge les lots 32 et 64 bits pour la mise à jour de micrologiciel. En plus de ces lots, OMIVV crée également un lot hybride lorsque plusieurs lots disponibles du catalogue possèdent le même ID de version.

REMARQUE : Les lots 64 bits ne sont pas pris en charge sur les hôtes de 12e génération avec la version 1.51 ou une version antérieure d'iDRAC.

6. Sur la page **Sélection de pilotes**, sélectionnez le composant de pilote que vous souhaitez mettre à jour, puis cliquez sur **Suivant**. Si la logithèque de micrologiciels est sélectionnée, la page **Sélectionner les composants** s'affiche. La page affiche les détails des composants tels que le **Nom d'hôte**, le **Numéro de service**, le **Nom du modèle**, le **Composant**, l'**État actuel**, la **Disponibilité**, l'**Importance** et le **Redémarrage requis**.
7. Sur la page **Sélectionner les composants**, sélectionnez le composant de micrologiciel que vous souhaitez mettre à jour, puis cliquez sur **Suivant**.

Il est impossible de sélectionner les composants qui sont dans une rétrogradation ou dont la mise à jour est déjà planifiée. Vous pouvez sélectionner les composants qui sont répertoriés pour une rétrogradation en sélectionnant l'option **Autoriser la rétrogradation**.

Pour filtrer des valeurs séparées par des virgules provenant du contenu des divers composants de la grille de données, utilisez le champ **Filtre**.

Vous pouvez également faire glisser les colonnes dans la grille des données des composants. Si vous souhaitez exporter à partir de

l'Assistant, cliquez sur .

8. Dans la page **Informations de mise à jour du micrologiciel**, consultez tous les détails de mise à jour du micrologiciel, puis cliquez sur **Suivant**.

La page **Planifier une mise à jour du micrologiciel** s'affiche.

9. Sur la page **Planifier une mise à jour du micrologiciel**, procédez comme suit :

- a) Saisissez le nom de la tâche de mise à jour de micrologiciel dans le champ **Nom de la tâche de mise à jour de micrologiciel**.

REMARQUE : Le nom de la tâche de mise à jour de micrologiciel est obligatoire et empêche l'utilisation d'un nom existant. Si vous supprimez le nom d'une tâche de mise à jour de micrologiciel, vous pouvez le réutiliser.

- b) Saisissez la description de la mise à jour du micrologiciel dans le champ **Description de la mise à jour de micrologiciel**. Cette valeur est facultative.

- c) Saisissez la valeur d'expiration du délai en mode maintenance (en minutes). Si le temps d'attente dépasse le temps indiqué, la tâche de mise à jour échoue et la tâche d'entrée en mode maintenance sera annulée ou expirera. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.

REMARQUE : La valeur minimale d'expiration du délai en mode maintenance est de 60 minutes.

REMARQUE : La valeur maximale d'expiration du délai en mode maintenance est d'un jour.

- d) Pour exécuter la tâche de mise à jour maintenant, cliquez sur **Mettre à jour maintenant**.

- e) Sélectionnez les options adéquates dans la liste déroulante **Migration de données vSAN**. Par défaut, l'option **Assurer l'accessibilité** est sélectionnée.

REMARQUE : Par défaut, l'option **Déplacer les machines virtuelles hors tensions et suspendues sur d'autres hôtes du cluster** est sélectionnée. La désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.

- f) Pour exécuter la tâche de mise à jour ultérieurement, cliquez sur **Planifier une mise à jour**, puis effectuez les tâches suivantes :

1. Dans la zone **Calendrier** sélectionnez les mois et jour.

2. Dans la zone de texte **Heure**, saisissez l'heure au format HH:MM.

3. Sélectionnez les options adéquates dans la liste déroulante **Migration de données vSAN**. Par défaut, l'option **Assurer l'accessibilité** est sélectionnée.



REMARQUE : Par défaut, l'option *Déplacer les machines virtuelles hors tensions et suspendues sur d'autres hôtes du cluster* est sélectionnée. La désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.

10. Cliquez sur **Suivant**.

La page **Résumé** s'affiche.

11. Dans la page **Résumé**, cliquez sur **Terminer**. Le message **La tâche de mise à jour de micrologiciel a été créée avec succès** s'affiche.

La tâche de mise à jour du micrologiciel prend plusieurs minutes et sa durée varie en fonction du nombre d'hôtes sélectionnés et du nombre de composants présents dans chaque hôte. Vous pouvez afficher l'état des tâches de mise à jour du micrologiciel sur la page **File d'attente des tâches**. Pour accéder à la page File d'attente des tâches, dans OpenManage Integration, sélectionnez **Surveiller > File d'attente des tâches > Mises à jour du micrologiciel**. Une fois la tâche de mise à jour du micrologiciel terminée, l'inventaire s'exécute automatiquement sur les hôtes sélectionnés et les hôtes quittent automatiquement le mode maintenance.

Gestion de châssis

OMIVV vous permet d'afficher des informations supplémentaires sur les châssis associés aux serveurs modulaires. Dans l'onglet Informations sur le châssis, vous pouvez afficher un aperçu des informations relatives à un châssis individuel ainsi que des informations sur l'inventaire du matériel, sur les micrologiciels et le contrôleur de gestion, sur l'intégrité des composants du châssis et sur la garantie de celui-ci. Les trois onglets suivants s'affichent pour chaque châssis et varient en fonction du modèle du châssis.

- Onglet Récapitulatif
- Onglet Surveiller
- Onglet Manage (Gérer)

REMARQUE : Pour afficher toutes les informations, assurez-vous que les châssis sont associés à un profil de châssis et que l'inventaire du châssis s'est terminé avec succès. Pour plus d'informations, voir [À propos du profil de châssis](#).

Sujets :

- [Affichage des détails récapitulatifs du châssis](#)
- [Affichage des informations d'inventaire matériel du châssis](#)
- [Affichage de la configuration du matériel supplémentaire du châssis](#)
- [Affichage de l'hôte associé à un châssis](#)

Affichage des détails récapitulatifs du châssis

Vous pouvez afficher le récapitulatif détaillé d'un châssis à la page **Récapitulatif** du châssis.

1. Dans la page d'**accueil**, cliquez sur **vCenter**.
2. Dans le volet gauche, sous **OpenManage Integration**, cliquez sur **Châssis Dell EMC**.
3. Dans le volet gauche, sélectionnez l'IP du châssis correspondant.
4. Cliquez sur l'onglet **Récapitulatif**.

Les informations suivantes sur le châssis sélectionné s'affichent :

- Nom
- Modèle
- Version du micrologiciel
- Numéro de service
- CMC

REMARQUE : Si vous cliquez sur le lien CMC, la page Contrôleur de gestion de châssis s'affiche.

REMARQUE : Si vous n'exécutez pas la tâche d'inventaire pour le châssis, vous pouvez voir uniquement le numéro de service et l'adresse IP du CMC.

5. Affichez la condition d'intégrité des périphériques associés au châssis sélectionné. Le volet principal affiche l'intégrité générale d'un châssis. Les voyants d'intégrité valides sont **Intègre**, **Avertissement**, **Critique**, **Non Présent**. Dans la vue de grille **Intégrité du châssis**, l'intégrité de chaque grille composant s'affiche. Les paramètres d'intégrité du châssis s'appliquent aux modèles VRTX version 1.0 et versions ultérieures, M1000e version 4.4 et versions ultérieures. Pour les versions inférieures à 4.3, seuls deux voyants d'intégrité sont affichés, à savoir Intègre et Avertissement ou Critique (triangle inversé avec point d'exclamation orange).

REMARQUE : L'intégrité globale indique l'intégrité basée sur le châssis doté du nombre de paramètre d'intégrité le plus bas. Par exemple, s'il existe 5 signes d'intégrité et 1 signe d'avertissement, le symbole d'intégrité globale correspond à Avertissement

6. Affichez **Entreprise CMC** ou **Express** avec le type de licence et la date d'expiration d'un châssis. Les détails mentionnés ne sont pas applicables au châssis M1000e.
7. Cliquez sur l'icône **Garantie** pour afficher le nombre de jours restants et les jours utilisés pour un hôte. Si vous avez plusieurs garanties, le dernier jour de la dernière garantie est pris en compte pour calculer le nombre de jours restants pour la garantie.

8. Affichez les erreurs répertoriées dans le tableau **Erreurs actives**, pour un châssis. Elles s'affichent sur la page **Intégrité du châssis**.

REMARQUE : Pour les châssis M1000e version 4.3 et antérieures, les erreurs actives ne sont pas affichées.

Affichage des informations d'inventaire matériel du châssis

Vous pouvez afficher les informations sur l'inventaire matériel dans le châssis sélectionné. Pour afficher les informations de cette page, veuillez à exécuter une tâche d'inventaire et à exporter un fichier CSV contenant les informations des composants.


1. Dans la page d'**accueil**, cliquez sur **vCenter**.
2. Dans le volet gauche, sous **OpenManage Integration**, cliquez sur **Châssis Dell EMC**.
3. Dans le volet gauche, sélectionnez l'IP du châssis correspondant.
4. Cliquez sur l'onglet **Surveiller**.

Pour afficher les informations relatives au composant pertinent, naviguez dans OMIVV :

Tableau 29. Les informations sur l'inventaire matériel

Inventaire matériel : composant	Navigaison dans OMIVV	Informations
Ventilateurs	Utilisez l'une des méthodes suivantes : <ul style="list-style-type: none"> • Dans l'onglet Présentation, cliquez sur Ventilateurs. • Dans l'onglet Surveiller, développez le volet gauche, cliquez sur Inventaire du matériel, puis sur Ventilateurs. 	Informations relatives aux ventilateurs : <ul style="list-style-type: none"> • Nom • Présent • État de l'alimentation • Valeur • Seuil d'avertissement • Seuil critique <ul style="list-style-type: none"> • Minimum • Maximum
Blocs d'alimentation	Utilisez l'une des méthodes suivantes : <ul style="list-style-type: none"> • Dans l'onglet Présentation, cliquez sur Blocs d'alimentation. • Dans l'onglet Surveiller, développez le volet gauche, cliquez sur Inventaire du matériel, puis cliquez sur Blocs d'alimentation. 	Informations relatives aux blocs d'alimentation : <ul style="list-style-type: none"> • Nom • Capacité • Présent • État de l'alimentation
Capteurs de température	Utilisez l'une des méthodes suivantes : <ul style="list-style-type: none"> • Dans l'onglet, Présentation, cliquez sur Capteurs de température. • Dans l'onglet Surveiller, développez le volet gauche, cliquez sur Inventaire du matériel, puis cliquez sur Capteurs de température. 	Informations relatives aux capteurs de température : <ul style="list-style-type: none"> • Emplacement • Valeur • Seuil d'avertissement <ul style="list-style-type: none"> • Maximum • Minimum • Seuil critique <ul style="list-style-type: none"> • Maximum • Minimum <p>REMARQUE : Pour le châssis PowerEdge M1000e, les informations sur les capteurs de température s'affichent uniquement pour le châssis. Pour les autres châssis, des</p>

Inventaire matériel : composant	Navigation dans OMIVV	Informations
		<p>informations sur les capteurs de température s'affichent pour le châssis et les serveurs modulaires associés.</p>
Modules d'E/S	<p>Utilisez l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Dans l'onglet Présentation, cliquez sur Modules d'E/S. • Dans l'onglet Gérer, développez le volet gauche, cliquez sur Inventaire du matériel, puis sur Modules d'E/S. 	<p>Informations relatives aux modules d'E/S :</p> <ul style="list-style-type: none"> • Logement/Emplacement • Présent • Nom • Structure • Numéro de service • État de l'alimentation <p>Pour afficher des informations supplémentaires, sélectionnez le module d'E/S correspondant et les informations suivantes s'affichent :</p> <ul style="list-style-type: none"> • Rôle • Version du micrologiciel • Version du matériel • Adresse IP • Masque de sous-réseau • Passerelle • Adresse MAC • DHCP activé
PCIe	<p>Utilisez l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Dans l'onglet Présentation, cliquez sur PCIe. • Dans l'onglet Surveiller, développez le volet gauche, cliquez sur Inventaire du matériel, puis cliquez sur PCIe. 	<p>Informations relatives à PCIe :</p> <ul style="list-style-type: none"> • Logement PCIe <ul style="list-style-type: none"> • Emplacement • Nom • État d'alimentation • Structure • Logement du serveur <ul style="list-style-type: none"> • Nom • Numéro <p>Pour afficher des informations supplémentaires, sélectionnez le PCIe correspondant et les informations suivantes s'affichent :</p> <ul style="list-style-type: none"> • Type de logement • Mappage des serveurs • État d'affectation • Alimentation de logement allouée • ID de PCI • Numéro/ID fournisseur <p>REMARQUE : Les informations sur le PCIe ne s'appliquent pas au châssis M1000e.</p>
iKVM	<p>Utilisez l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Dans l'onglet Présentation, cliquez sur iKVM. • Dans l'onglet Surveiller, développez le volet gauche, cliquez sur Inventaire du matériel, puis cliquez sur iKVM. 	<p>Informations relatives au module iKVM :</p> <ul style="list-style-type: none"> • Nom du module iKVM • Présent • Version du micrologiciel • USB/Vidéo du panneau avant activés • Autoriser l'accès à l'interface de ligne de commande CMC <p>REMARQUE : Vous pouvez afficher les informations concernant iKVM uniquement pour le châssis PowerEdge M1000e.</p>

Inventaire matériel : composant	Navigation dans OMIVV	Informations
		 REMARQUE : L'onglet iKVM s'affiche uniquement si le châssis contient un module iKVM.

Affichage de la configuration du matériel supplémentaire du châssis

Vous pouvez afficher les informations sur les détails concernant la garantie, le stockage, le micrologiciel et le contrôleur de gestion du châssis sélectionné. Pour afficher les informations de cette page, veuillez à exécuter une tâche d'inventaire et à exporter un fichier CSV contenant les informations de composant.

Pour afficher des informations détaillées sur la garantie, le stockage, le micrologiciel ou le contrôleur de gestion du châssis, procédez comme suit :

1. Dans la page d'**accueil**, cliquez sur **vCenter**.
2. Dans le volet gauche, sous **OpenManage Integration**, cliquez sur **Châssis Dell EMC**.
3. Dans le volet gauche, sélectionnez l'IP du châssis correspondant.
4. Cliquez sur l'onglet **Surveiller**.

Pour consulter les informations concernant la garantie, le stockage, le micrologiciel et le contrôleur de gestion, naviguez dans OMIVV.

Tableau 30. Détails du micrologiciel

Configuration matérielle	Navigation dans OMIVV	Informations
Micrologiciel	<ol style="list-style-type: none"> a. Dans l'onglet Surveiller, cliquez sur la marque flèche double et développez le volet gauche, puis cliquez sur Micrologiciel. b. Dans l'onglet Surveiller, si vous cliquez sur Lancer le CMC, la page Contrôleur de gestion de châssis s'affiche. 	Informations relatives au micrologiciel : <ul style="list-style-type: none"> • Composant • Version actuelle

Tableau 31. Détails sur le contrôleur de gestion

Configuration matérielle	Navigation dans OMIVV	Informations
Contrôleur de gestion	<ol style="list-style-type: none"> a. Dans l'onglet Surveiller, cliquez sur la marque flèche double et développez le volet gauche, puis cliquez sur Contrôleur de gestion. b. Dans la page Contrôleur de gestion, pour afficher des informations supplémentaires, cliquez sur la flèche et développez la colonne de gauche. 	Informations relatives au contrôleur de gestion : <ul style="list-style-type: none"> • Général <ul style="list-style-type: none"> • Nom • Version du micrologiciel • Heure de la dernière mise à jour • Emplacement du contrôleur CMC • Version du matériel • Réseau commun <ul style="list-style-type: none"> • Nom de domaine DNS • Utiliser DHCP pour DNS • Adresse MAC • Mode de redondance • Informations sur l'IPv4 de CMC <ul style="list-style-type: none"> • IPv4 activé • DHCP activé • Adresse IP

Configuration matérielle	Navigation dans OMIVV	Informations
		<ul style="list-style-type: none"> • Masque de sous-réseau • Passerelle • Serveur DNS préféré • Serveur DNS auxiliaire

Tableau 32. Informations sur le stockage

Configuration matérielle	Navigation dans OMIVV	Informations
Stockage	Dans l'onglet Surveiller , cliquez sur Stockage .	<p>Informations relatives au stockage :</p> <ul style="list-style-type: none"> • Disques virtuels. • Contrôleurs • Encéintes • Disques physiques • Disques de secours <p>REMARQUE : Lorsque vous cliquez sur un lien en surbrillance situé sous Stockage, le tableau Afficher affiche les détails de chaque élément en surbrillance. Dans le tableau Afficher, si vous cliquez sur chaque élément de ligne, des informations supplémentaires s'affichent pour chaque élément.</p> <p>Pour les châssis M1000e, si vous disposez d'un module de stockage, les détails de stockage suivants s'affichent dans une grille sans informations supplémentaires :</p> <ul style="list-style-type: none"> • Nom • Modèle • Numéro de service • Adresse IP (lien au stockage) • Structure • Nom de groupe • Adresse IP du groupe (lien au groupe de stockage)

Tableau 33. Informations sur la garantie

Configuration matérielle	Navigation dans OMIVV	Informations
Garantie	Dans l'onglet Surveiller , cliquez sur Garantie .	<p>Informations relatives à la garantie :</p> <ul style="list-style-type: none"> • Fournisseur • Description • État • Date de début • Date de fin • Jours restants • Dernière mise à jour <p>REMARQUE : Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Exécution d'une tâche de récupération de la garantie.</p>

Affichage de l'hôte associé à un châssis

Vous pouvez afficher les informations sur l'hôte associé au châssis sélectionné dans l'onglet **Gérer**.

1. Dans la page d'**accueil**, cliquez sur **vCenter**.

2. Dans le volet gauche, sous **OpenManage Integration**, cliquez sur **Châssis Dell EMC**.
3. Dans le volet gauche, sélectionnez l'IP du châssis correspondant.
4. Cliquez sur l'onglet **Gérer**.

Les informations suivantes sur l'hôte associé s'affichent :

- Nom de l'hôte (si vous cliquez sur l'IP de l'hôte sélectionné, les détails concernant l'hôte s'affichent).
- Numéro de service
- Modèle
- IP iDRAC
- Emplacement de logement
- Dernier inventaire

Déploiement d'hyperviseur

OMIVV vous permet de configurer les composants suivants sur les serveurs sans système d'exploitation pris en charge, ainsi que le déploiement de l'hyperviseur et son ajout au datacenter et au cluster spécifiés dans un vCenter :

- Paramètre d'ordre de démarrage
- Configuration RAID
- Configuration BIOS
- Configuration iDRAC

Vous pouvez créer des profils matériels, des profils système et des profils d'hyperviseur sur les serveurs PowerEdge sans système d'exploitation à l'aide de VMware vCenter sans utiliser PXE.

REMARQUE : Il est recommandé d'utiliser le profil système pour les serveurs de 14e génération et plus lors du déploiement de l'hyperviseur.

Pour configurer le matériel et procéder au déploiement, vérifiez que les serveurs physiques s'affichent dans l'Assistant Déploiement. Assurez-vous que tous les serveurs physiques respectent les conditions suivantes :

- Respectez les informations spécifiques à la prise en charge du matériel disponibles dans la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter*.
- Respectez les versions minimales prises en charge pour le micrologiciel iDRAC, le Lifecycle Controller et le BIOS. Pour obtenir des informations spécifiques sur le micrologiciel pris en charge, voir la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter*.
- À l'issue du déploiement, configurez manuellement les cartes réseau aux emplacements PCI. Si vous utilisez des cartes réseau d'extension, les LOM (LAN On Motherboard) ou NDC (Network Daughter Card - Carte fille de réseau) de l'hôte doivent être activés sur le système et ceux-ci doivent être connectés au réseau. OMIVV ne prend en charge le déploiement qu'à l'aide des LOM embarqués ou intégrés.
- Respectez les spécifications de stockage du module iDSDM. Pour en savoir plus sur les spécifications de stockage du module iDSDM, consultez la documentation VMware. Veillez à activer le module iDSDM à partir du BIOS avant de déployer l'hyperviseur avec OMIVV. OMIVV permet un déploiement sur le module iDSDM ou sur les disques durs locaux.
- Assurez-vous qu'il existe un itinéraire entre les réseaux vCenter et iDRAC si le serveur vCenter et le contrôleur iDRAC sont connectés à différents réseaux.
- Assurez-vous que la fonction Collect System Inventory on Restart (CSIOR) est activée. Avant de lancer la détection automatique/manuelle, vérifiez que les données récupérées sont à jour en effectuant une mise hors tension complète du système, avant de le remettre sous tension (redémarrage matériel).
- Cliquez pour commander les serveurs Dell avec les options de détection automatique et d'établissement de liaison (« handshake ») préconfigurées en usine. Si un serveur n'est pas préconfiguré avec ces options, entrez manuellement l'adresse IP d'OMIVV ou configurez votre réseau local pour fournir cette information.
- Assurez-vous que les conditions suivantes sont remplies avant de lancer le déploiement de l'hyperviseur si OMIVV n'est pas utilisé pour la configuration matérielle :
 - Activez l'indicateur de technologie de virtualisation (VT) dans le BIOS.
 - Configurez la séquence de démarrage du système sur un disque virtuel amorçable ou sur un module iDSDM pour l'installation du système d'exploitation.
- Si OMIVV est utilisé pour la configuration matérielle, vérifiez que le paramètre du BIOS est automatiquement activé pour VT, même si la configuration du BIOS ne fait pas partie du profil matériel. La configuration RAID Express/Clone est requise si aucun disque virtuel n'est présent sur le système cible.
- Assurez-vous que les images ESXi personnalisées qui contiennent tous les lecteurs Dell sont disponibles pour le déploiement. Vous trouverez les images adéquates sur le site support.dell.com en vous rendant sur la page **Pilotes et téléchargements Dell** et en enregistrant les images personnalisées à un emplacement de partage CIFS ou NFS auquel OMIVV aura accès lors du processus de déploiement. Pour consulter la liste actualisée des versions ESXi prises en charge par cette version, voir la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter*. Pour utiliser les images adéquates, voir [Téléchargement d'images ISO Dell personnalisées](#).
- Assurez-vous que le mode BIOS est sélectionné dans le profil matériel de référence avant d'appliquer le profil d'hyperviseur car seul le mode BIOS est pris en charge par OMIVV pour le déploiement automatique de l'hyperviseur sur le serveur cible. Si aucun profil matériel n'est sélectionné, configurez manuellement le mode d'amorçage sur le BIOS et redémarrez le serveur avant d'appliquer le profil d'hyperviseur.

Si les versions des serveurs sont antérieures aux serveurs PowerEdge de 12e génération, le processus de déploiement effectue les tâches suivantes :

- Installe le progiciel OMSA sur le système cible.
- Configure automatiquement le pointage de la destination d'interruption SNMP vers OMIVV dans OMSA.

Sujets :

- Détection de périphériques
- Provisioning
- Profils système
- Gestion des profils système
- Configuration d'un profil matériel
- Création d'un profil d'hyperviseur
- Création de modèles de déploiement
- À propos de l'Assistant Déploiement
- Synchronisation de la tâche de déploiement
- Téléchargement d'images ISO EMC Dell personnalisées

Détection de périphériques

La détection est le processus d'ajout d'un serveur sans système d'exploitation PowerEdge pris en charge. Une fois le serveur détecté, vous pouvez l'utiliser à des fins de déploiement d'hyperviseur ou de matériel. Voir la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter* pour obtenir la liste des serveurs PowerEdge requis pour le déploiement. Cette opération nécessite également une connectivité réseau de l'iDRAC de serveur Dell EMC sans système d'exploitation à la machine virtuelle OMIVV.

- REMARQUE :** Les hôtes dotés d'hyperviseurs existants ne doivent pas être détectés dans OMIVV, mais ajoutés au vCenter. Ajoutez-les au profil de connexion, puis réconciliez-les avec OpenManage Integration for VMware vCenter à l'aide de l'Assistant Conformité d'hôte.
- REMARQUE :** Si des serveurs sans système d'exploitation antérieurs à OMIVV 4.0 sont détectés, supprimez les machines de la liste des serveurs sans système d'exploitation et recherchez-les à nouveau.
- REMARQUE :** Pour effectuer un déploiement de système d'exploitation sur carte SD pour les serveurs PowerEdge 12e génération sans système d'exploitation, assurez-vous que l'iDRAC 2.30.30.30 et version ultérieure est installé.

Détection manuelle

Vous pouvez ajouter manuellement un serveur sans système d'exploitation qui n'est pas ajouté par le processus de détection. Une fois ajouté, le serveur s'affiche dans la liste des serveurs dans l'Assistant de déploiement.

1. Dans OpenManage Integration for VMware vCenter, sur l'onglet **Gérer > Déploiement**, cliquez sur l'icône . La boîte de dialogue **Ajouter un serveur** s'affiche.
2. Dans la boîte de dialogue **Ajouter un serveur**, procédez comme suit :
 - a) Dans la boîte de dialogue **Adresse IP iDRAC**, entrez l'adresse IP iDRAC.
 - b) Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
 - c) Dans la zone de texte **Mot de passe**, entrez le mot de passe.
3. Cliquez sur **Ajouter le serveur**.

La tâche d'ajout du serveur peut prendre quelques minutes.

Détection automatique dans OpenManage Integration for VMware vCenter

La détection automatique est le processus d'ajout d'un serveur PowerEdge sans système d'exploitation. Une fois le serveur détecté, utilisez-le pour le déploiement d'hyperviseur ou de matériel. La détection automatique est une fonctionnalité de l'iDRAC qui supprime la tâche de détection manuelle d'un serveur sans système d'exploitation à partir de l'OMIVV.

Conditions préalables à la détection automatique

Avant toute tentative de détection de serveurs PowerEdge sans système d'exploitation, assurez-vous qu'OMIVV a déjà été installé. Les serveurs PowerEdge dotés d'iDRAC Express ou d'iDRAC Enterprise peuvent être détectés dans un pool de serveurs sans système d'exploitation. Assurez-vous qu'il existe une connexion réseau entre le contrôleur iDRAC du serveur Dell sans système d'exploitation et l'appliance OMIVV.

REMARQUE : Les hôtes dotés d'hyperviseurs existants ne doivent pas être détectés dans OMIVV. Ajoutez plutôt l'hyperviseur au profil de connexion, puis réconciliez avec OMIVV à l'aide de l'Assistant Conformité d'hôte.

Pour que la détection automatique se produise, les conditions suivantes doivent être réunies :

- Alimentation : branchez le serveur à la prise secteur. Le serveur ne doit pas être mis sous tension.
- Connectivité réseau : vérifiez que l'iDRAC du serveur dispose d'une connectivité réseau et communique avec le serveur de configuration sur le port 4433. Vous pouvez obtenir l'adresse IP à l'aide du serveur DHCP ou la spécifier manuellement dans l'utilitaire de configuration de l'iDRAC.
- Paramètres réseau supplémentaires : en cas d'utilisation de DHCP, activez le paramètre Obtenir l'adresse serveur DNS depuis DHCP afin de permettre la résolution de noms DNS.
- Emplacement du service d'approvisionnement : assurez-vous que le contrôleur iDRAC connaît l'adresse IP ou le nom d'hôte du serveur du service d'approvisionnement. Voir [Emplacement du service d'approvisionnement](#).
- Accès au compte désactivé : activez l'accès du compte administratif au contrôleur iDRAC. S'il existe des comptes iDRAC dotés de droits d'administrateur, désactivez-les d'abord dans la console Web du contrôleur iDRAC. Une fois la détection automatique terminée, le compte administrateur du contrôleur iDRAC sera réactivé.
- Détection automatique activée : assurez-vous que la détection automatique est activée sur l'iDRAC du serveur afin que le processus de détection automatique puisse commencer.

Emplacement du service d'approvisionnement

Utilisez les options suivantes pour obtenir l'emplacement du service d'approvisionnement par iDRAC pendant la découverte automatique :

- Spécifié manuellement dans l'iDRAC : spécifiez manuellement l'emplacement dans l'utilitaire de configuration de l'iDRAC sous Configuration utilisateur du réseau local, Serveur de configuration.
- Option d'étendue DHCP : spécifiez l'emplacement en utilisant une option d'étendue DHCP.
- Enregistrement de service DNS : spécifiez l'emplacement via un enregistrement de service DNS.
- Nom connu DNS : le serveur DNS spécifie l'adresse IP d'un serveur dont le nom connu est DCIMCredentialServer.

Si la valeur du service de configuration n'est pas spécifiée manuellement dans la console iDRAC, iDRAC tente d'utiliser la valeur de l'option d'étendue DHCP. Si l'option d'étendue DHCP n'est pas présente, iDRAC tente d'utiliser la valeur de l'enregistrement de service de DNS.

Pour obtenir des informations détaillées sur la configuration de l'option d'étendue DHCP et de l'enregistrement de service DNS, reportez-vous aux Spécifications de configuration réseau de la détection automatique Dell à l'adresse suivante : http://en.community.dell.com/techcenter/extras/m/white_papers/20178466

Activation ou désactivation de comptes administratifs sur les serveurs iDRAC

Avant de configurer la détection automatique, désactivez tous les comptes administratifs autres que le compte racine. Le compte racine doit être désactivé au cours de la procédure de détection automatique. Une fois la détection automatique configurée avec succès, revenez à l'interface graphique utilisateur du contrôleur iDRAC et réactivez les comptes administratifs, autres que le compte racine, qui ont été désactivés.

REMARQUE : Pour éviter un échec de la détection automatique, vous pouvez activer un compte non administratif sur le contrôleur iDRAC. Le compte non administratif permet un accès à distance lorsque la détection automatique échoue.

1. Dans un navigateur, saisissez l'**adresse IP d'iDRAC**.
2. Connectez-vous à l'**interface GUI d'iDRAC**.
3. Effectuez l'une des opérations suivantes :
 - Pour iDRAC6 : dans le volet gauche, sélectionnez l'onglet **Paramètres d'iDRAC > Réseau/Sécurité > Utilisateurs**.
 - Pour iDRAC7 : dans le volet gauche, sélectionnez l'onglet **Paramètres d'iDRAC > Authentification de l'utilisateur > Utilisateurs**.
 - Pour iDRAC8 : dans le volet gauche, sélectionnez l'onglet **Paramètres d'iDRAC > Authentification de l'utilisateur > Utilisateurs**.
4. Dans l'onglet **Utilisateurs**, recherchez tous les comptes administratifs autres que le compte racine.
5. Pour activer le compte, sélectionnez l'**ID** sous ID utilisateur.

6. Cliquez sur **Suivant**.
7. Dans la page **Configuration de l'utilisateur**, sous **Généralités**, décochez la case **Activer l'utilisateur**.
8. Cliquez sur **Appliquer**.
9. Pour réactiver chaque compte administratif, répétez les étapes 1 à 8 après avoir configuré avec succès la détection automatique. Sélectionnez la case à cocher **Activer l'utilisateur**, puis cliquez sur **Appliquer**.

Configuration manuelle des serveurs PowerEdge de 11e génération en vue d'une détection automatique

Vérifiez que vous disposez des adresses IP du contrôleur iDRAC et de l'hôte.

Si la détection automatique n'a pas été paramétrée en usine sur votre appliance sans système d'exploitation, vous pouvez la configurer manuellement.

Lorsque des serveurs sans système d'exploitation sont automatiquement détectés, un nouveau compte administrateur est créé ou un compte existant est activé avec les informations d'identification renvoyées par le service de liaison. Tous les autres comptes administrateur désactivés avant la détection automatique ne sont pas activés. Assurez-vous de réactiver les comptes administrateur après l'exécution de la détection automatique. Voir [Activation ou désactivation de comptes administratifs sur les serveurs iDRAC](#).

REMARQUE : Si, pour une raison quelconque, la détection automatique échoue, il est impossible de se connecter à l'iDRAC à distance. Pour vous connecter à distance, vous devez activer un compte non administrateur sur l'iDRAC. Si aucun compte non administrateur n'est activé sur l'iDRAC, la seule façon d'accéder à l'iDRAC consiste à vous connecter localement et à activer le compte sur l'iDRAC.

1. Entrez l'**adresse IP de l'iDRAC** dans le navigateur.
2. Connectez-vous à l'**interface GUI d'iDRAC Enterprise**.
3. Dans l'onglet **iDRAC 6 - Enterprise (Integrated Dell Remote Access Controller 6 - Enterprise)** > **Résumé système**, cliquez sur **Lancer** dans l'aperçu de la console virtuelle.
4. Dans la boîte de dialogue **Avertissement — Sécurité**, cliquez sur **Oui**.
5. Dans la console de l'utilitaire iDRAC, appuyez une ou deux fois sur la touche **F12**. La boîte de dialogue **Authentification requise** s'affiche.
6. Dans la boîte de dialogue **Authentification requise**, consultez le nom affiché, puis appuyez sur **Entrée**.
7. Saisissez le mot de passe.
8. Appuyez sur **Entrée**.
9. Lorsque la boîte de dialogue **Arrêter/Redémarrer** s'affiche, appuyez sur la touche **F11**.
10. L'hôte redémarre. L'écran affiche des informations relatives au chargement de la mémoire et du RAID, puis le contrôleur iDRAC. Lorsque vous y êtes invité, appuyez immédiatement sur les touches **CTRL + E**. Si vous affichez la boîte de dialogue suivante, l'action est réussie. Sinon, passez au menu Alimentation, mettez l'appareil hors tension, puis de nouveau sous tension et répétez cette étape.

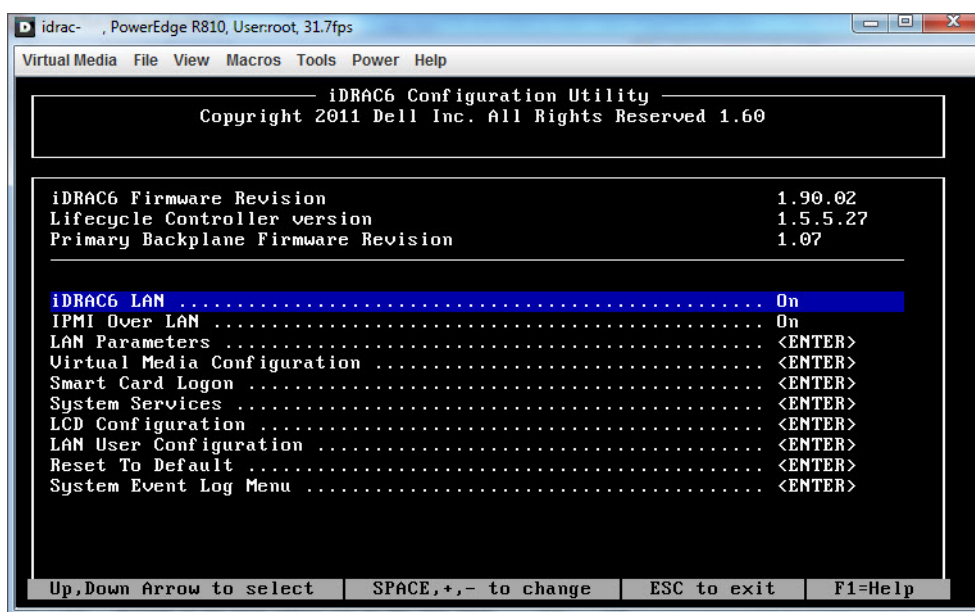


Figure 1. Utilitaire de configuration iDRAC

11. Dans l'utilitaire de configuration du contrôleur iDRAC6, utilisez les touches fléchées pour sélectionner l'option **Paramètres du LAN**.
12. Appuyez sur **Entrée**.
13. Si cet hôte est une lame, vous devez, pour configurer le NIC, utiliser la barre d'espace afin de basculer les options sur **Activé**.
14. Si vous utilisez DHCP, utilisez les touches fléchées pour sélectionner l'option **Nom de domaine via DHCP**.
15. Utilisez la barre d'espace pour basculer l'option sur **Activer**.
16. Si vous utilisez DHCP, utilisez les touches fléchées pour naviguer vers les paramètres IPv4, puis sélectionnez l'option **Serveurs DNS via DHCP**.
17. Utilisez la barre d'espace pour basculer l'option sur **Activer**.
18. Pour quitter, appuyez sur la touche **Échap** de votre clavier.
19. Utilisez les touches fléchées pour sélectionner l'option **Configuration de l'utilisateur LAN**.
20. Utilisez les touches fléchées pour sélectionner l'option **Serveur de provisionnement**.
21. Appuyez sur **Entrée**.
22. Entrez l'adresse IP de l'hôte.
23. Appuyez sur la touche **Échap**.
24. Utilisez les touches fléchées pour sélectionner l'option **Accéder au compte**.
25. Utilisez la barre d'espace pour basculer l'option sur **Désactiver**.
26. Utilisez les touches fléchées pour sélectionner l'option **Détection automatique**.
27. Utilisez la barre d'espace pour basculer l'option sur **Activé**.
28. Appuyez sur la touche **Échap** de votre clavier.
29. Appuyez de nouveau sur **Échap**.

Configuration manuelle des serveurs PowerEdge de 12e génération et de générations ultérieures pour la détection automatique

Assurez-vous que vous disposez d'une adresse iDRAC.

Lorsque vous commandez des serveurs auprès de Dell, vous pouvez demander à ce que la fonction de détection automatique soit activée sur les serveurs après avoir fourni l'adresse IP du serveur de configuration. L'adresse IP du serveur de configuration correspond à l'adresse IP d'OMIVV. Par conséquent, les serveurs Dell reçus sont automatiquement détectés lorsque vous les mettez sous tension après avoir monté et branché le câble iDRAC. Les serveurs sont automatiquement détectés et répertoriés sur la première page de l'Assistant Déploiement.

REMARQUE : Pour les serveurs détectés automatiquement, les informations d'identification fournies dans **Gérer > Paramètres > Références de déploiement** sont définies en tant qu'informations d'identification et sont utilisées pour toute communication ultérieure avec le serveur, jusqu'à ce que le déploiement du système d'exploitation soit terminé.

Après une opération de déploiement de système d'exploitation réussie, les références iDRAC fournies dans le profil de connexion associé sont définies.

Pour activer manuellement la détection automatique sur l'ordinateur cible, procédez comme suit pour les serveurs de 12e génération et de générations ultérieures :

1. Pour accéder à la configuration du système, démarrez/redémarrez le système cible et appuyez sur la touche F2 pendant le démarrage initial.
2. Accédez à **Paramètres iDRAC > Configuration de l'utilisateur** et désactivez l'utilisateur racine. Pour ce faire, assurez-vous qu'il n'existe aucun autre utilisateur doté de droits d'administrateur actifs sur l'adresse iDRAC.
3. Cliquez sur **Retour**, puis sur **Activation à distance**.
4. Définissez l'option **Activer la détection automatique** sur **Activé** et le **Serveur de configuration** sur l'adresse IP de l'OMIVV.
5. Enregistrer les paramètres.
Le serveur est détecté automatiquement lors du prochain démarrage du serveur. Une fois la détection automatique réussie, l'utilisateur racine est activé et l'indicateur **Activer la détection automatique** est désactivé automatiquement.

Suppression d'un serveur sans système d'exploitation

Vous pouvez supprimer manuellement un serveur qui a été découvert automatiquement ou ajouté manuellement.

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Gérer > Déploiement**.
2. Sur la page **Serveurs sans système d'exploitation**, sélectionnez les serveurs et cliquez sur **X**.

Provisioning

Tous les systèmes sans systèmes d'exploitation conformes détectés automatiquement/manuellement sont accessibles à OMIVV pour le déploiement de l'hyperviseur et l'approvisionnement matériel. Pour préparer l'approvisionnement et le déploiement, procédez comme suit :

Tableau 34. Préparation au déploiement

Étapes	Description
Créer un profil système	Contient les paramètres de configuration du système rassemblés à partir d'un serveur de référence de 14e génération utilisé pour configurer les nouveaux serveurs.
Créer un profil matériel	Contient les paramètres matériels rassemblés à partir d'un serveur de référence utilisé pour déployer de nouveaux serveurs. Voir la section Création ou personnalisation d'un profil matériel . REMARQUE : Il est recommandé d'utiliser le profil matériel des serveurs de 13e génération et versions antérieures.
Créer un profil d'hyperviseur	Contient les informations d'installation de l'hyperviseur nécessaires au déploiement ESXi. Voir la section Création d'un profil d'hyperviseur .
Créer un modèle de déploiement	Un modèle de déploiement contient un profil système, un profil matériel, un profil d'hyperviseur, une combinaison de profil système et de profil d'hyperviseur, ou une combinaison de profil matériel et de profil d'hyperviseur. Vous pouvez enregistrer et réutiliser ces profils pour tous les serveurs de datacenter disponibles.

Après avoir créé le modèle de déploiement, utilisez l'Assistant pour rassembler les informations nécessaires pour créer un travail planifié qui alloue le matériel serveur et déploie de nouveaux hôtes dans vCenter. Pour plus d'informations sur l'exécution de l'Assistance de déploiement, voir [Exécution de l'Assistant Déploiement](#). Enfin, affichez l'état de la tâche via la file d'attente des tâches et modifiez les tâches de déploiement en attente.

Profils système

La fonctionnalité des profils système est disponible dans l'iDRAC pour les serveurs PowerEdge qui fournissent une prise en charge de CNA, FCoE en plus de la prise en charge de la configuration pour la séquence d'amorçage, RAID, le BIOS, l'iDRAC. OMIVV prend en charge les profils système de l'iDRAC de 14e génération en tant que « Profil système ». Grâce à la prise en charge du profil de configuration de serveur, OMIVV vous permet d'exporter l'intégralité de la configuration d'un serveur Dell EMC de 14e génération et de l'importer dans des serveurs cibles.

Lors de l'application d'un profil système d'un serveur modulaire installé dans un châssis FX2 à un autre serveur similaire installé dans un autre châssis FX2, les numéros des emplacements des deux serveurs doivent être identiques.

Par exemple, un profil système issu d'un serveur FC640 situé dans l'emplacement 1 d'un châssis FX2s peut uniquement être appliqué sur un autre serveur FC640 se trouvant dans l'emplacement 1 d'un autre châssis FX2s.

REMARQUE : Le profil système ne prend pas en charge les configurations suivantes :

- Activation et désactivation des options d'amorçage
- Configuration BOSS-related

REMARQUE : Au cours de l'utilisation du profil système, l'exportation d'un profil système avec une licence Enterprise, puis l'importation du même profil système sur les serveurs avec une licence Express, et inversement, occasionne un échec.

REMARQUE : Il n'est pas possible d'importer un profil système à l'aide de la licence Express de micrologiciel iDRAC9 3.00.00.00. Vous devez disposer d'une licence Enterprise.

REMARQUE : Les profils système recherchent une instance exacte (FGDD) lors de l'application du profil, ce qui fonctionne avec succès sur les serveurs rack (identiques), mais peut avoir quelques restrictions sur les serveurs modulaires. Par exemple, dans FC640, les profils système créés à partir d'un serveur modulaire ne peuvent pas être appliqués sur d'autres serveurs modulaires dans le même châssis FX en raison de restrictions au niveau de la carte réseau. Dans ce cas, il est recommandé de disposer d'un profil système de référence issu de chaque emplacement du châssis et d'appliquer ces profils système uniquement dans les emplacements correspondants du châssis.

Les tâches typiques de l'utilisation d'un profil système comprennent :


- La création ou la capture des informations du profil système à partir d'un serveur de référence. Voir la section [Création d'un profil système](#).
- Application du profil sur des serveurs sélectionnés en utilisant le modèle de déploiement. Voir la section [Création de modèles de déploiement](#).

REMARQUE : Il est recommandé d'utiliser le profil système pour les serveurs de 14e génération et versions ultérieures.

Pour lancer la page du profil de système, effectuez les étapes suivantes :

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils système**.
 - a. Sur la page **Profils système**, affichez la liste des profils système que vous avez créés.

Le tableau qui s'affiche répertorie les profils système ainsi que le nom du profil, la description, le modèle de serveur et les informations du serveur de référence.
 - b. Pour afficher plus de détails sur un hôte de profil système, sélectionnez un profil système.

Vérifiez les informations du profil système qui affiche des informations, telles que le nom du profil, l'IP de l'iDRAC, le type d'iDRAC, le numéro de service, le nom d'hôte, le modèle de serveur, la date de création, la date de modification et l'auteur de la modification.
 - c. Pour permuter les colonnes dans la grille de données, glissez et déplacez les colonnes dans la grille de données.
 - d. Pour filtrer ou effectuer une recherche dans le contenu de la grille de données, cliquez sur le champ **Filtre**.
 - e. Pour exporter les informations du profil système vers un fichier .CSV, sélectionnez un profil de système, puis cliquez sur l'icône  dans le coin droit de la grille de données.


Création d'un profil système

Assurez-vous que les conditions suivantes sont remplies avant la création d'un profil système :

- Le serveur de référence est configuré en fonction de vos besoins, à l'extérieur d'OMIVV. La modification de toute valeur des attributs n'est pas prise en charge dans la version actuelle, à l'exception des mots de passe utilisateur de l'iDRAC.
- L'option Collecter l'inventaire système au redémarrage est activée sur un serveur de référence et le serveur de référence est redémarré, afin que les données retournées à partir de l'iDRAC soient à jour.
- OpenManage Integration a effectué un inventaire réussi sur chaque hôte géré vCenter.
- Les serveurs sans système d'exploitation disposent des versions minimums du BIOS et du micrologiciel. Voir la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter* pour plus d'informations sur les niveaux minimums de micrologiciel pour l'iDRAC, le BIOS et Lifecycle Controller.

Vous pouvez créer un profil système en utilisant uniquement un serveur de référence de 14e génération.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils système**.

2. Cliquez sur .
3. Lisez les instructions indiquées dans la page **Bienvenue**, puis cliquez sur **Suivant**.
 - Dans la zone de texte **Nom de profil**, entrez le nom du profil.
 - Dans la zone de texte **Description du profil**, saisissez une description. La description est facultative.
4. Cliquez sur **Suivant**.
La boîte de dialogue **Serveur de référence** s'affiche. Vous pouvez sélectionner des serveurs de référence de 14e génération à partir de la boîte de dialogue ou via le bouton Parcourir à la page source du profil.
5. Sélectionnez un serveur de référence de 14e génération en effectuant l'une des sous-opérations suivantes :

REMARQUE : Tous les hôtes de la 11e à la 14e génération s'affichent dans la boîte de dialogue et le lien de sélection est activé uniquement pour les hôtes et serveurs sans système d'exploitation de 14e génération compatibles. Seuls les serveurs sans système d'exploitation de 14e génération sont affichés et le lien de sélection est activé uniquement pour les serveurs sans système d'exploitation compatibles.

- a. Dans la boîte de dialogue **Serveur de référence**, choisissez le serveur de référence de 14e génération adéquat, puis cliquez sur le lien **Sélectionner** en regard du serveur de référence.


REMARQUE : Le lien **Sélectionner** est activé uniquement pour les serveurs conformes.

- b. Sur la page **Serveur de référence**, cliquez sur **Parcourir** pour sélectionner un serveur de référence hôte de 14e génération compatible géré et correctement inventorié par OMIVV ou un serveur sans système d'exploitation de 14e génération conforme.

La boîte de dialogue **Confirmation d'extraction** indiquant que les paramètres sont extraits s'affiche. Pour extraire la configuration matérielle à partir du serveur de référence, cliquez sur **Oui** dans la boîte de dialogue **Confirmation d'extraction**. L'extraction est effectuée en quelques minutes.

Le nom du serveur sélectionné, le type de serveur de référence, l'adresse IP iDRAC, le modèle et le numéro de service s'affichent dans la page **Source de profil**.

REMARQUE : Si le Type de serveur de référence est un serveur sans système d'exploitation, seule l'adresse IP de l'iDRAC s'affiche. Si le Type de serveur de référence est un hôte, les adresses IP de l'iDRAC et IP/FQDN de l'hôte s'affichent.

6. Cliquez sur **Suivant**.
7. Sur la page **Paramètres de profil**, développez iDRAC pour afficher les attributs de profil système. Vous pouvez trier les colonnes de la grille de données par ordre croissant ou décroissant. Cliquez sur l'icône de filtre les données pour filtrer les données.
 - a) Pour consulter rapidement le lien de Définition du mot de passe dans la colonne **Valeur**, cliquez sur l'icône , saisissez « mot de passe » dans la **Valeur contient** et saisissez le mot de passe de l'utilisateur activé.

REMARQUE : Dell EMC recommande de fournir les informations d'identification identiques aux informations d'identification utilisées pendant l'ajout des serveurs sans système d'exploitation. Si vous modifiez le mot de passe dans le modèle de déploiement, les modifications ne sont pas affichées pour l'utilisateur racine. Au cours du déploiement du système d'exploitation, si un profil d'hyperviseur est associé au modèle de déploiement, le déploiement utilise le mot de passe du profil de connexion (iDRAC et ESXi).

REMARQUE : L'option Définir un mot de passe est uniquement disponible pour l'utilisateur iDRAC activé avec un nom d'utilisateur valide.

Par ailleurs, vous pouvez afficher les paramètres de profil pour les composants basés sur la configuration du serveur de référence Dell tels que iDRAC, BIOS, RAID, NIC, CNA, FCoE et EvenFilters.

- b) Développez chacun des composants pour afficher les options de configuration telles que **Instance**, **Nom d'attribut**, **Valeur**, **Destructeur**, **Dépendance** et **Groupe**.

Lorsque vous passez le curseur sur les attributs, des informations supplémentaires sur ces derniers sont affichées.

Par défaut, quelques attributs tels que **Lecture seule**, **Spécifique au système** et **Destructeur** sont désactivés pour la sélection. Si le texte de dépendance n'est pas disponible, la case contenant le texte de dépendance est vide.

REMARQUE : Lors de la mise à niveau RPM ou de la sauvegarde et de la restauration, les règles suivantes s'appliquent à tous les profils migrés :

- Lorsque vous passez le curseur sur les attributs, les noms d'attribut s'affichent.
- Seuls les attributs non spécifiques au système sont sélectionnés.
- Le texte de dépendance ne s'affiche pas.
- Les attributs activés affichent le nombre total d'attributs sélectionnés.

8. Cliquez sur **Suivant**.

La page **Récapitulatif** s'affiche. Elle contient des informations sur les détails du profil et les statistiques des attributs des configurations système.

Le nombre total d'attributs, le nombre total d'attributs activés, le nombre total d'attributs spécifiques à la plate-forme et le nombre total d'attributs destructeurs s'affichent sous les statistiques des attributs.

9. Dans la page **Récapitulatif**, cliquez sur **Terminer**.

Le profil est enregistré automatiquement et s'affiche dans la fenêtre **Profils système**.

Tous les attributs spécifiques du système ne sont pas pris en charge dans la version actuelle. Pour plus d'informations sur les attributs spécifiques du système, voir [Attributs spécifiques au système](#).

Quelques attributs du Profil système sont substitués pour que l'OMIVV puisse fonctionner. Pour plus d'informations sur la personnalisation des attributs, voir [Attributs de personnalisation](#). Pour plus d'informations sur le modèle de configuration du Profil système, des attributs et des flux de travail, voir [Informations supplémentaires](#).

Gestion des profils système

Les profils système définissent la configuration du système d'un serveur en utilisant un serveur de référence. Dans OpenManage Integration for VMware vCenter, il existe plusieurs actions de gestion que vous pouvez effectuer sur les profils système existants, y compris :

- Affichage d'un profil système
- Suppression d'un profil système

REMARQUE : La version actuelle ne prend pas en charge la modification d'un profil système par OMIVV. Vous devez configurer votre machine en dehors d'OMIVV, puis l'utiliser comme serveur de référence d'un profil système.

Configuration d'un profil matériel

Pour configurer les paramètres matériels du serveur, créez un profil matériel. Un profil matériel est un modèle de configuration que vous pouvez appliquer aux composants d'infrastructure nouvellement découverts ; il nécessite les informations suivantes :

Tableau 35. Configuration requise pour la création d'un profil matériel

Configuration requise	Description
Séquence d'amorçage	La séquence de démarrage est composée de la séquence de périphérique de démarrage et de la séquence de disque dur, que vous pouvez modifier uniquement si le mode de démarrage est défini sur BIOS.
Paramètres du BIOS	Les paramètres du BIOS comprennent ce qui suit : mémoire, processeur, SATA, périphériques intégrés, communications série, gestion de serveur intégrée, gestion de l'alimentation, sécurité système, et divers paramètres. REMARQUE : OpenManage Integration for VMware vCenter active certains paramètres du BIOS dans le groupe Processeur dans le BIOS sur tous les serveurs déployés, quels que soient les paramètres sur le serveur de référence. Avant d'utiliser un serveur de référence pour créer un profil matériel, le paramètre CSIOR du serveur de référence doit être activé et redémarré pour fournir des informations d'inventaire et de configuration exactes.
Paramètres iDRAC	Les paramètres iDRAC comprennent ce qui suit : réseau, liste d'utilisateurs et configuration d'utilisateurs.
Configuration RAID	La configuration RAID affiche la topologie RAID actuelle sur le serveur de référence au moment où le profil matériel a été extrait. REMARQUE : Deux options de configuration RAID sont configurées dans le profil matériel : <ol style="list-style-type: none">1. Appliquer le RAID1 et créer un disque de secours dédié, le cas échéant : utilisez cette option si vous souhaitez appliquer les paramètres de configuration RAID par défaut au serveur cible.2. Cloner la configuration RAID depuis le serveur de référence : utilisez cette option si vous souhaitez cloner le paramètre du serveur de référence. Voir Personnalisation du serveur de référence pour la création d'un profil matériel.

Les tâches de création de profils matériels comprennent :

- Activation de CSIOR sur un serveur de référence
- Personnalisation des serveurs de référence pour créer un profil matériel

- Clonage d'un profil matériel

Activation de CSIOR sur un serveur de référence

Avant de créer un profil matériel à l'aide d'un serveur de référence, activez le paramètre Collect System Inventory On Reboot (CSIOR) et redémarrez le serveur pour fournir des informations d'inventaire et de configuration exactes.

Deux méthodes sont disponibles pour activer CSIOR :

Tableau 36. Méthodes d'activation de CSIOR

Méthode	Description
Localement	Cette méthode utilise un hôte individuel via l'interface utilisateur Dell Lifecycle Controller United Server Configurator (USC).
À distance	Cette méthode utilise un script WS-Man. Pour plus d'informations sur les scripts de cette fonctionnalité, voir <i>Dell TechCenter</i> et <i>Profil de gestion DCIM Lifecycle Controller Manager</i> .

Pour activer CSIOR localement sur un serveur de référence :

1. Mettez le système sous tension et, pendant le POST, appuyez sur **F2** pour lancer USC.
2. Sélectionnez **Configuration matérielle > Configuration du remplacement de pièce**.
3. Activez le paramètre **Collecte de l'inventaire du système au redémarrage** et quittez USC.

Création ou personnalisation d'un profil matériel

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils matériels**.
2. Cliquez sur l'icône **+**.
3. Dans l'**Assistant Profil matériel**, cliquez sur **Suivant** dans la page **Bienvenue** et procédez comme suit :
 - Dans la zone de texte **Nom de profil**, entrez le nom du profil.
 - Dans la zone de texte **Description**, saisissez une description. La description est facultative.
4. Cliquez sur **Suivant**.
La boîte de dialogue **Serveur de référence** s'affiche. Vous pouvez sélectionner des serveurs de référence à partir de la boîte de dialogue ou via le bouton **Parcourir** dans la fenêtre du serveur de référence.
5. Sélectionnez un serveur de référence en effectuant l'une des sous-opérations suivantes :
 - Dans la boîte de dialogue **Serveur de référence**, choisissez le serveur de référence adéquat, puis cliquez sur le lien **Sélectionner** en regard du serveur de référence.
La boîte de dialogue **Confirmation d'extraction** indiquant que les paramètres sont extraits s'affiche. Pour extraire la configuration matérielle à partir du serveur de référence, cliquez sur **Oui** dans la boîte de dialogue **Confirmation d'extraction**. L'extraction est effectuée en quelques minutes.
 - Sur la page **Serveur de référence**, cliquez sur **Parcourir** pour sélectionner un serveur de référence compatible géré et correctement inventorié par OMIVV ou un serveur sans système d'exploitation conforme.
Pour extraire la configuration matérielle du serveur de référence, dans la boîte de dialogue **Confirmation d'extraction**, cliquez sur **Oui**.

Le nom du serveur sélectionné, l'adresse IP iDRAC, le modèle et le numéro de service s'affichent dans la page **Serveur de référence**.
6. Dans la page **Serveur de référence**, pour personnaliser les paramètres du serveur de référence, cliquez sur **Personnaliser les paramètres du serveur de référence** et choisissez les paramètres suivants, qui peuvent éventuellement être inclus et personnalisés :
 - **Paramètres RAID**
 - **Paramètres du BIOS**
 - **Séquence de démarrage**
 - **Paramètres iDRAC**
 - **Paramètres réseau**
 - **Liste d'utilisateurs**
7. Dans la fenêtre **Configuration RAID**, sélectionnez l'une des options suivantes, puis cliquez sur **Suivant** :

- **Appliquer le RAID1 et créer un disque de secours dédié, le cas échéant** : utilisez cette option si vous souhaitez appliquer les paramètres de configuration RAID par défaut au serveur cible. La tâche de configuration RAID passe à RAID1 par défaut sur les deux premiers disques du contrôleur intégré qui prennent en charge RAID1. Un disque de secours dédié est également créé pour la baie RAID1, si un disque candidat répondant aux critères RAID existe.
 - **Cloner la configuration RAID depuis le serveur de référence, tel qu'indiqué ci-dessous** : utilisez cette option, si vous souhaitez cloner le paramètre du serveur de référence.
8. Dans la page **Paramètres du BIOS**, pour inclure les informations de paramètres BIOS dans le profil, développez une catégorie pour afficher les options de paramètres, puis cliquez sur **Modifier** pour mettre à jour l'une des options suivantes :

- **Informations sur le système**
- **Paramètres de mémoire**
- **Paramètres du processeur**
- **Paramètres SATA**
- **Paramètres de démarrage**
- **Démarrage unique**
- **Périphériques intégrés**
- **Désactivation des logements**
- **Communications série**
- **Paramètres du profil du système**
- **Sécurité du système**
- **Paramètres divers**

Après avoir effectué toutes les mises à jour d'une catégorie, cliquez sur **Suivant** pour enregistrer les modifications ou sur **Annuler** pour annuler les modifications.

REMARQUE : Pour obtenir des informations détaillées sur le BIOS, y compris les options et les explications des paramètres, voir le *Manuel du propriétaire du matériel* du serveur sélectionné.

9. Dans la page **Ordre de démarrage**, procédez comme suit, puis cliquez sur **Suivant** :
- a) Pour afficher les options de séquence de démarrage, développez **Ordre de démarrage**, puis cliquez sur **Modifier** pour effectuer les mises à jour suivantes :
 1. Dans la liste **Mode d'amorçage**, sélectionnez **BIOS** ou **UEFI**.
 2. Dans la liste **Vue**, sous **Séquence de périphériques de démarrage**, pour modifier la séquence de périphériques de démarrage, sélectionnez le périphérique, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
 3. Sélectionnez **Autoriser une nouvelle tentative de séquence de démarrage** pour que le serveur retente automatiquement la séquence.
 4. Pour appliquer les modifications, cliquez sur **OK**. Pour les annuler, cliquez sur **Annuler**.
 - b) Pour afficher les options de séquence de disques durs, développez **Séquence de disques durs** et cliquez sur **Modifier**. Mettez à jour les éléments suivants :
 1. Pour modifier la séquence de disques durs affichée, sélectionnez le périphérique et cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
 2. Pour appliquer les modifications, cliquez sur **OK**. Pour les annuler, cliquez sur **Annuler**.

REMARQUE : Pour les serveurs de génération antérieure à la 13^e génération, les deux modes UEFI et BIOS s'affichent. Pour ceux de la 13^e génération ou ultérieures, l'un ou l'autre des deux modes (BIOS ou UEFI) s'affiche.

10. Dans la page **Paramètres iDRAC**, procédez comme suit :
- a) Développez une catégorie pour afficher les options de paramètres, puis cliquez sur **Modifier** :
Mettez à jour l'un des éléments suivants :
 - **Paramètres réseau**
 - **Réseau**
 - **Média virtuel**
 - b) Sous la **Liste d'utilisateurs** iDRAC locale, effectuez l'une des opérations suivantes :
 - **Ajouter un utilisateur** : entrez manuellement un utilisateur iDRAC et les informations requises. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications, ou cliquez sur **Annuler** pour annuler les modifications.
 - **Supprimer un utilisateur** : supprimez l'utilisateur sélectionné. Sélectionnez un utilisateur à l'aide de la souris, puis cliquez sur **Supprimer**. Pour confirmer la suppression, cliquez sur **Oui**.
 - **Modifier un utilisateur** : modifiez manuellement les informations d'un utilisateur iDRAC. Lorsque vous avez terminé, cliquez sur **Appliquer** pour enregistrer vos paramètres (ou sur **Annuler**, si vous souhaitez annuler).

Après avoir effectué toutes les mises à jour d'une catégorie, cliquez sur **Suivant** pour enregistrer les modifications ou sur **Annuler** pour annuler les modifications.



REMARQUE : Pour obtenir des informations détaillées sur l'iDRAC, y compris les options et explications des paramètres, voir le *Guide de l'utilisateur iDRAC* du serveur sélectionné.

11. Cliquez sur **Suivant**.
12. Dans la page **Récapitulatif**, cliquez sur **Terminer**.

Le profil est enregistré automatiquement et s'affiche dans la fenêtre **Profils matériels**.

Création ou clonage de profil matériel

1. Dans l'onglet **Gérer > Déploiement** d'OpenManage Integration for VMware vCenter, sélectionnez **Modèles de déploiement > Profils matériels**.
2. Cliquez sur **+**.
3. Dans l'**Assistant Profil matériel**, cliquez sur **Suivant** sur la page **Bienvenue** et effectuez les actions suivantes :
 - Dans la zone de texte **Nom de profil**, entrez le nom du profil.
 - Dans la zone de texte **Description**, entrez une *Description*. La description est facultative.
4. Cliquez sur **Suivant**.
5. Pour sélectionner un serveur de référence compatible, géré par vCenter et correctement inventorié par le plug-in Dell EMC OpenManage, sur la page **Serveur de référence**, cliquez sur **Parcourir**.
6. Pour extraire tous les paramètres matériels du serveur de référence, cliquez sur l'option **Cloner les paramètres du serveur de référence**.
7. Cliquez sur **Suivant**.
L'extraction des paramètres prend quelques minutes.
8. Cliquez sur **Suivant**.
Les paramètres sont renseignés et le nom, l'adresse IP iDRAC et le numéro de service du serveur sélectionné s'affichent dans la fenêtre **Serveur de référence**.


Le profil est enregistré et s'affiche dans la fenêtre **Profils matériels** sous **Profils disponibles**.

Gestion des profils matériels

Les profils matériels définissent la configuration matérielle d'un serveur en utilisant un serveur de référence. À partir d'OpenManage Integration for VMware vCenter, vous pouvez effectuer plusieurs actions de gestion sur les profils matériels existants, y compris :

- Affichage ou modification du profil matériel
- Suppression d'un profil matériel


Affichage ou modification du profil matériel

1. Dans l'onglet **Gérer > Déploiement** d'OpenManage Integration for VMware vCenter, sélectionnez **Modèles de déploiement > Profils matériels**.
Les profils matériels s'affichent.
2. Pour modifier un profil, sélectionnez-en un et cliquez sur .
3. Dans l'**Assistant Profil matériel**, pour configurer avec différentes valeurs, cliquez sur **Modifier**.
4. Cliquez sur **Enregistrer** pour appliquer les modifications ou sur **Annuler** pour annuler les modifications.

Suppression d'un profil matériel



REMARQUE : La suppression d'un profil matériel faisant partie d'une tâche de déploiement en cours d'exécution peut entraîner l'échec de la tâche de suppression.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement Profils matériels**.
2. Sélectionnez un profil et cliquez sur .
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui** pour supprimer le profil ou sur **Non** pour annuler la suppression.

Création d'un profil d'hyperviseur

Pour déployer et configurer ESXi sur un serveur, créez un profil d'hyperviseur. Un profil d'hyperviseur exige les informations suivantes :

- Un emplacement de support logiciel ISO personnalisé Dell sur un partage NFS ou CIFS
 - L'instance vCenter qui gère les hôtes déployés et un profil d'hôte facultatif
 - Le centre de données ou cluster de destination sur lequel le plug-in déploie les serveurs dans vCenter
1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils d'hyperviseur**.
 2. Dans la page **Profils d'hyperviseur**, cliquez sur **+**.
 3. Dans la boîte de dialogue **Profil d'hyperviseur**, effectuez les sous-tâches suivantes :
 - Dans la zone de texte **Nom de profil**, entrez le nom du profil.
 - Dans la zone de texte **Description**, entrez une description (facultatif).
 4. Sous **Choisir la version et le chemin d'accès de l'ISO de référence**, dans la zone de texte **Source d'installation (ISO)**, saisissez le chemin d'accès à l'emplacement de partage de l'hyperviseur.

Une copie de l'image de l'hyperviseur est modifiée pour permettre une installation par script. L'emplacement de l'ISO de référence peut avoir l'un des formats suivants :

- Format NFS : `host:/share/hypervisor.iso`
- Format CIFS : `\\host\share\hypervisor.iso`

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

Si vous utilisez un partage CIFS, saisissez le **Nom d'utilisateur**, le **Mot de passe** et **Vérifier le mot de passe**. Assurez-vous que les mots de passe sont identiques.


5. Dans la liste **Sélectionner une version**, sélectionnez une version ESXi.
Tous les serveurs déployés avec ce profil d'hyperviseur ont cette image, et si les serveurs sont issus de versions antérieures à la 12e génération, la dernière version recommandée d'OMSA est également installée.
6. Pour vérifier le chemin d'accès et l'authentification, cliquez sur **Démarrer le test** sous **Paramètres de test**.
7. Cliquez sur **Appliquer**.

Gestion des profils d'hyperviseur

Vous pouvez effectuer plusieurs actions de gestion sur les profils d'hyperviseur existants, y compris :


- Affichage ou modification des profils d'hyperviseur
- Suppression des profils d'hyperviseur

Affichage ou modification des profils d'hyperviseur

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils d'hyperviseur**.
Les profils d'hyperviseur s'affichent.
2. Sélectionnez un profil et cliquez sur .
3. Dans la boîte de dialogue **Profil d'hyperviseur**, fournissez des valeurs à jour.
4. Cliquez sur **Enregistrer** pour appliquer les modifications ou sur **Annuler** pour annuler les modifications.

Suppression d'un profil d'hyperviseur

REMARQUE : La suppression d'un profil d'hyperviseur faisant partie d'une tâche de déploiement en cours d'exécution peut entraîner l'échec de la tâche.

1. Dans OpenManage Integration for VMware vCenter, accédez à l'onglet **Gérer > Déploiement** et sélectionnez **Modèles de déploiement > Profils d'hyperviseur**.
2. Sélectionnez un profil et cliquez sur .
3. Dans la boîte de dialogue de confirmation, pour supprimer le profil, cliquez sur **Supprimer**, ou pour annuler, cliquez sur **Annuler**.

Création de modèles de déploiement

Un modèle de déploiement contient un profil système, un profil matériel, un profil d'hyperviseur, une combinaison de profil système et de profil d'hyperviseur, ou une combinaison de profil matériel et de profil d'hyperviseur. L'**Assistant Déploiement** utilise ce modèle pour allouer le matériel de serveur et déployer les hôtes dans vCenter.

1. Dans l'onglet **Gérer > Déploiement** d'OpenManage Integration for VMware vCenter, sélectionnez **Modèles de déploiement**.

2. Cliquez sur **+**.

3. Dans la boîte de dialogue **Modèle de déploiement**, attribuez un nom au modèle.

4. Entrez une **Description** pour le modèle de déploiement (facultatif).

5. Cliquez sur **Profil système** ou **Profil matériel** et sélectionnez le profil approprié dans le menu déroulant.

REMARQUE : Il est recommandé d'utiliser le profil système pour les serveurs de 14e génération et le profil matériel pour les serveurs de 13e génération et versions antérieures.

6. Sélectionnez un **Profil d'hyperviseur** à partir du menu déroulant.

7. Pour appliquer les sélections de profil et enregistrer les modifications, cliquez sur **Enregistrer**. Pour annuler, cliquez sur **Annuler**.

Gestion des modèles de déploiement

Dans OpenManage Integration, vous pouvez effectuer plusieurs actions de gestion sur les modèles de déploiement existants, y compris :

- Affichage ou modification des modèles de déploiement
- Suppression des modèles de déploiement

Affichage ou modification des modèles de déploiement

1. Dans l'onglet **Gérer > Déploiement** d'OpenManage Integration for VMware vCenter, sélectionnez **Modèles de déploiement**. Les profils du modèle de déploiement s'affichent.

2. Dans la boîte de dialogue **Modèle de déploiement**, saisissez le nouveau nom du modèle et la description.

Assurez-vous que le modèle possède un nom unique.

3. Modifiez le **Profil matériel** ou le **Profil système** à partir du menu déroulant.

4. Modifiez le **Profil d'hyperviseur** dans le menu déroulant et cliquez sur **Enregistrer**.

Suppression des modèles de déploiement

1. Dans l'onglet **Gérer > Déploiement** d'OpenManage Integration for VMware vCenter, sélectionnez **Modèles de déploiement**.

2. Dans la page **Modèle de déploiement**, sélectionnez un modèle, puis cliquez sur **X**.

3. Pour confirmer la suppression du modèle, cliquez sur **Supprimer** dans la boîte de message ou sur **Annuler** pour annuler.

À propos de l'Assistant Déploiement

L'Assistant Déploiement décrit le processus de déploiement, qui est le suivant :

- Sélection des serveurs sans système d'exploitation conformes.

REMARQUE : Si vous sélectionnez des serveurs de 14e génération pour le déploiement, la liste du modèle de déploiement comprend un profil matériel, un profil système ou un profil hyperviseur, ou une combinaison de profils matériel et hyperviseur ou une combinaison de profils système et hyperviseur.

REMARQUE : Si vous sélectionnez des serveurs qui ne sont pas de 14e génération ou une combinaison de serveurs qui en sont et qui n'en sont pas, la liste du modèle de déploiement comprend un profil matériel ou un profil hyperviseur, ou une combinaison de profils matériel et hyperviseur.

- La sélection d'un modèle de déploiement, constitué de profils de matériel et d'hyperviseur.
- Sélection de la cible d'installation (disque dur ou iSDSDM).

Lorsque vous déployez l'hyperviseur, vous pouvez le déployer sur un double module SD interne. Le double module SD interne doit être activé à partir du BIOS avant de déployer un hyperviseur avec OMIVV.

- Sélection du profil de connexion à associer à l'hôte.
- Attribution des détails du réseau pour chaque hôte.

- Sélection du vCenter, du datacenter de destination ou du cluster et d'un profil d'hôte facultatif.
- Planification de l'exécution de travaux de déploiement de serveur.

REMARQUE : Si vous déployez uniquement un profil matériel, les options d'identification du serveur, de profil de connexion et d'informations sur le réseau de l'Assistant Déploiement sont ignorées et vous accédez directement à la page Planifier le déploiement.

REMARQUE : Avec la licence d'essai/évaluation, vous pouvez utiliser l'Assistant Déploiement tant que la licence n'a pas expiré.

Prise en charge de la technologie VLAN

OMIVV prend en charge le déploiement d'hyperviseur sur un VLAN routable. Vous pouvez configurer la prise en charge VLAN dans l'Assistant Déploiement. Dans cette section de l'Assistant Déploiement, vous avez la possibilité de spécifier l'utilisation des VLAN et de spécifier un ID VLAN. Lorsqu'un ID VLAN est fourni, il est appliqué à l'interface de gestion de l'hyperviseur lors du déploiement et marque tout le trafic doté de l'ID VLAN.

Assurez-vous que le VLAN fourni lors du déploiement communique avec l'appliance virtuelle et le serveur vCenter. Le déploiement d'un hyperviseur vers un VLAN qui ne peut pas communiquer vers une des/les deux destinations provoque l'échec du déploiement.

Si vous avez sélectionné plusieurs serveurs sans système d'exploitation dans une tâche de déploiement unique et que vous souhaitez appliquer le même ID VLAN à tous les serveurs, utilisez l'option **Appliquer les paramètres à tous les serveurs sélectionnés** située dans la section Identification de serveur de l'Assistant Déploiement. Cette option vous permet d'appliquer le même ID VLAN ainsi que d'autres paramètres réseau à tous les serveurs de cette tâche de déploiement.

REMARQUE : OMIVV ne prend pas en charge une configuration multiconnexions. L'ajout d'une deuxième interface réseau à l'appliance pour une communication avec un deuxième réseau entraîne des problèmes pour les flux de travail liés au déploiement d'hyperviseur, à la conformité du serveur et aux mises à jour de micrologiciel.

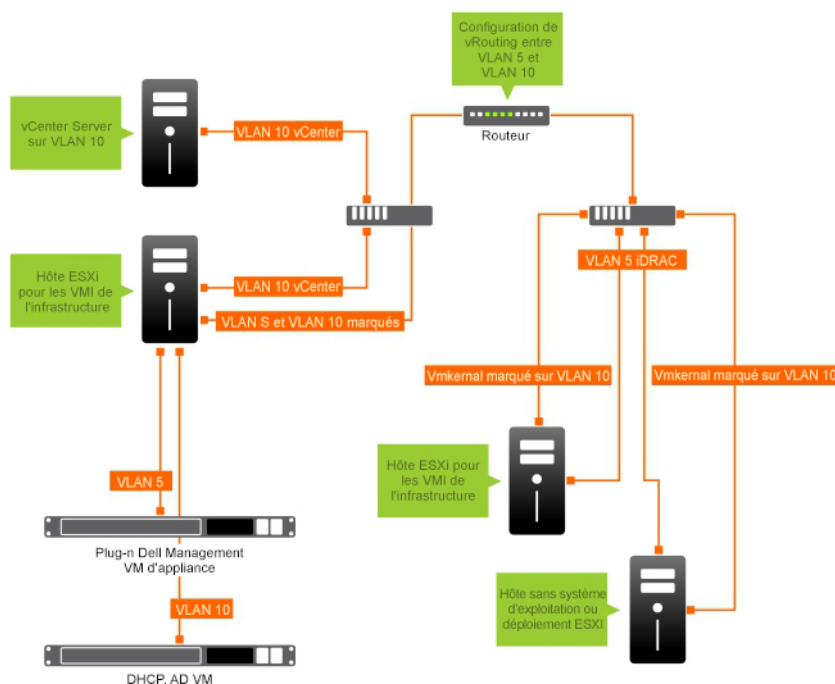


Figure 2. Réseau VLAN.

Dans cet exemple de réseau, l'appliance OMIVV se trouve sur VLAN 5, alors que le vCenter et le VMkernel des hôtes ESXi en cours de déploiement sont sur VLAN 10. Comme OMIVV ne prend pas en charge la connexion de plusieurs VLAN, VLAN 5 doit se router vers VLAN 10 pour que tous les systèmes communiquent entre eux correctement. Si le routage n'est pas activé entre ces VLAN, le déploiement échoue.

Exécution de l'Assistant Déploiement

Veillez à créer un modèle de déploiement avec un profil matériel, un profil système, un profil d'hyperviseur et un profil de connexion pour le vCenter avant d'exécuter l'Assistant Déploiement.

Pour exécuter l'Assistant Déploiement :

1. Dans OpenManage Integration for VMware vCenter, cliquez sur l'onglet **Gérer > Déploiement**.
2. Dans la fenêtre **Serveurs sans système d'exploitation**, cliquez sur le lien **Exécuter l'Assistant Déploiement**. La page **Bienvenue** de l'Assistant Déploiement s'affiche.
3. Lisez les informations indiquées dans la page **Bienvenue**, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner les serveurs à déployer**, cliquez sur les cases à cocher en regard de la liste des serveurs pour attribuer des serveurs sans système d'exploitation conformes à une tâche de déploiement.
5. Cliquez sur **Suivant**.
6. Sur la page **Sélectionner le modèle/profil**, procédez comme suit :

- a) Sous **Modèle de déploiement**, pour affecter un modèle de déploiement aux serveurs sélectionnés, sélectionnez un modèle de déploiement existant dans **Sélectionner un modèle de déploiement**.

REMARQUE : Le modèle basé sur le profil système s'affiche uniquement si vous sélectionnez la 14e génération des serveurs sur la page **Sélectionner les serveurs à déployer**.

Vous pouvez sélectionner un des modèles de déploiement suivants dans la liste déroulante :

- Si vous sélectionnez un modèle de déploiement relatif à un profil matériel ou un profil système uniquement pour configurer le matériel serveur, passez à l'étape 10.
- Si vous sélectionnez un modèle de déploiement relatif à un profil d'hyperviseur pour déployer un hyperviseur, poursuivez à partir de l'étape 6 (b).

REMARQUE : Si vous sélectionnez un déploiement relatif à un profil matériel ou un profil système uniquement, vous êtes automatiquement invité à renseigner la page **Planifier le déploiement**.

- b) Sous **Installation de l'hyperviseur**, sélectionnez l'une des options suivantes :

- **Premier disque d'amorçage** - déploie un hyperviseur sur le disque dur (HDD), le disque dur SSD (solid-state), le disque virtuel créé par contrôleurs RAID.
- **Double module SD interne** : déploie un hyperviseur sur le module IDSDM.

REMARQUE : Si un module IDSDM équipe au moins l'un des serveurs sélectionnés, l'option **Double module SD interne** est activée. Si ce n'est pas le cas, seule l'option **Disque dur** est disponible.

Si la prise en charge d'un module IDSDM n'est pas assurée par l'un des serveurs sélectionnés, ou si aucun module IDSDM n'est présent lors du déploiement, effectuez l'une des opérations suivantes :

REMARQUE : Assurez-vous que l'option **Basculement automatique du disque dur** est activée lors du déploiement du système d'exploitation.

- Cochez la case **Déployer l'hyperviseur sur le premier disque dur des serveurs qui ne disposent pas d'un double module SD interne** si vous souhaitez déployer l'hyperviseur sur le premier disque dur des serveurs.
- **PRÉCAUTION :** Si vous sélectionnez cette option et effectuez le déploiement de l'hyperviseur sur le premier disque dur des serveurs, toutes les données présentes sur le lecteur de disque sont effacées.
- Pour ignorer le déploiement sur les serveurs sélectionnés et poursuivre le déploiement de l'hyperviseur sur le serveur suivant, décochez **Déployer l'hyperviseur sur le premier disque dur des serveurs qui ne disposent pas d'un double module SD interne**.

- c) Sous **Profil de référence**, effectuez l'une des opérations suivantes :

- Sélectionnez le bouton d'option **Utiliser ce profil de référence pour tous les serveurs** et sélectionnez le profil de connexion dans la liste déroulante pour affecter tous les serveurs au même profil.
- Cliquez sur le bouton d'option **Sélectionner un profil de connexion pour chaque serveur**, puis sélectionnez un profil de connexion particulier pour chaque serveur de la liste déroulante.

7. Cliquez sur **Suivant**.

La page **Identification du serveur** s'affiche.

L'identification du serveur peut être fournie de deux manières :


- Entrez les informations réseau (adresse IP, masque de sous-réseau et passerelle) ; un nom de domaine complet (FQDN) est obligatoire pour le nom d'hôte. L'utilisation de *localhost* n'est pas prise en charge pour le FQDN. Le FQDN est utilisé lors de l'ajout de l'hôte à vCenter.

- Utilisez le protocole de configuration dynamique des hôtes (DHCP, Dynamic Host Configuration Protocol) pour configurer les adresses IP, le masque de sous-réseau, l'IP de passerelle, le nom d'hôte et les serveurs DNS préférés/de remplacement. Le DHCP attribué à l'adresse IP est utilisé lors de l'ajout de l'hôte à vCenter. Lorsque vous utilisez DHCP, Dell vous recommande d'utiliser une réservation IP pour les adresses MAC des cartes réseau sélectionnées.

REMARQUE : Utilisez un nom de domaine complet (FQDN, Fully Qualified Domain Name) pour le nom d'hôte au lieu de l'hôte local. À partir d'ESXi 5.1, une valeur d'hôte local empêche le plug-in OMIVV de traiter des événements envoyés de l'hôte. Créez un enregistrement DNS qui résout l'adresse IP avec le FQDN. Pour que les alertes SNMP d'ESXi 5.1 soient correctement identifiées, configurez le serveur DNS pour prendre en charge les demandes de recherche inversée. Les réservations DHCP et noms d'hôte DNS doivent être en place et vérifiés avant l'exécution de la tâche de déploiement planifiée.

8. Dans la page **Identification du serveur**, procédez comme suit :

La page permet de spécifier un ID VLAN. Lorsqu'un ID VLAN est fourni, il est appliqué à l'interface de gestion de l'hyperviseur lors du déploiement et marque l'ensemble du trafic doté de l'ID VLAN. La fonctionnalité Identification du serveur attribue de nouveaux noms et une identification réseau aux serveurs déployés. Voir [VLAN pris en charge](#).

- Pour développer et afficher les informations relatives à un serveur particulier, sous **Serveurs sélectionnés**, cliquez sur l'icône .
- Sous **Nom d'hôte et carte réseau**, entrez un **Nom de domaine pleinement qualifié** pour le serveur.
- Dans la liste déroulante **Carte réseau pour les tâches de gestion**, sélectionnez la carte réseau utilisée pour gérer le serveur.
- Entrez les adresses IP, masque de sous-réseau, passerelle par défaut et les informations de DNS ou cochez la case **Obtenir à l'aide de DHCP**.
- Lors d'un déploiement vers un réseau exigeant un ID VLAN, cochez la case **VLAN** et entrez l'ID VLAN. Pour l'ID VLAN, utilisez les numéros de 1 à 4094. L'ID VLAN 0 est réservé au marquage de la priorité des trames.
- Répétez les étapes a à h pour tous les serveurs à déployer ou cochez la case **Appliquer les paramètres à tous les serveurs sélectionnés**.

Si vous cochez **Appliquer les paramètres à tous les serveurs sélectionnés**, entrez le nom FQDN et l'adresse IP des autres serveurs.

REMARQUE : Lors de la spécification du nom FQDN des serveurs, veuillez fournir des noms d'hôte uniques pour chaque serveur.

9. Cliquez sur **Suivant**.

10. Sur la page **Planifier le déploiement**, procédez comme suit :

- Entrez une **Nom de tâche** et une **Description de tâche**.
- Pour **Paramètres vCenter**, entrez les informations suivantes :
 - Dans **Instance vCenter**, sélectionnez l'instance de serveur qui gère un hôte après le déploiement.
 - Dans **Conteneur de destination vCenter**, cliquez sur **Parcourir** pour rechercher les destinations vCenter.
 - Dans **Profil d'hôte vCenter**, sélectionnez un profil qui englobe et aide à gérer la configuration de l'hôte (facultatif).
- Déterminez le moment d'exécution d'une tâche de déploiement en sélectionnant un calendrier des tâches :
 - Sélectionnez **Planifier la tâche de déploiement**
 - Servez-vous du calendrier pour sélectionner la date.
 - Entrez l'heure.
 - Pour démarrer immédiatement la tâche, sélectionnez **Exécuter la tâche de déploiement maintenant**.

Pour accéder à la file d'attente des tâches une fois la tâche de déploiement démarrée, sélectionnez **Accéder à la file d'attente des tâches après la soumission de la tâche**.

11. Cliquez sur **Terminer**.

Une fois les tâches de l'Assistant Déploiement terminées, vous pouvez gérer les tâches de déploiement en utilisant la **File d'attente des tâches**.

Gestion des tâches de déploiement à l'aide de la file d'attente des tâches :

1. Dans OpenManage Integration for VMware vCenter, sur l'onglet **Surveiller** > **File d'attente des tâches**, cliquez sur **Tâches de déploiement**.

Les détails des tâches de déploiement répertoriés ci-dessous apparaissent sur la grille supérieure :

- Nom
- Description

- Heure planifiée
- État
- Taille de la collection
- Récapitulatif d'avancement

2. Pour mettre à jour les **Détails des tâches de déploiement**, cliquez sur l'icône **Actualiser**.

3. Pour afficher les détails d'une tâche de déploiement, qui contiennent des informations détaillées sur les serveurs inclus dans la tâche de déploiement, sélectionnez une tâche de déploiement sur la grille supérieure.

Les détails suivants apparaissent sur la grille inférieure :

- Numéro de service
- Adresse IP iDRAC
- État de la tâche
- Avertissements
- Détails de la tâche de déploiement (pointez la souris pour obtenir des informations supplémentaires).
- Heure de début et de fin
- Plus de détails

Vous pouvez afficher les informations complètes concernant une tâche de déploiement dans une fenêtre contextuelle en sélectionnant la tâche et en passant le curseur de la souris sur la colonne **Détails** de la tâche de déploiement.

Pour obtenir plus de détails sur l'échec des tâches basées sur le profil système, cliquez sur **Plus de détails**. La page **Plus de détails** affiche les informations suivantes :

- Descripteur de périphérique entièrement qualifié (FQDD) du composant
- Valeur de l'attribut
- Ancienne valeur
- Nouvelle valeur
- Message et ID du message de l'échec (non affiché pour quelques types d'erreurs)

La fenêtre n'est pas la même pour quelques-uns des attributs affichés sous **Nom de l'attribut** dans la fenêtre **Appliquer le profil système - Détails de l'échec** que le **Nom de l'attribut** du profil du système lorsque vous cliquez sur **Plus de détails**.

Pour exporter les détails vers un fichier .CSV, dans l'angle droit de la grille de données, cliquez sur .

4. Pour abandonner la tâche de déploiement, cliquez sur l'icône .

5. Lorsque le message s'affiche, cliquez sur **Abandonner la tâche** pour abandonner la tâche ou sur **Ne pas abandonner la tâche** pour annuler.

6. Pour afficher la fenêtre **Vider la file d'attente des tâches du déploiement**, cliquez sur . Sélectionnez **Plus anciennes que la date et l'état de tâche**, puis cliquez sur **Appliquer**.

Les tâches sélectionnées sont alors supprimées de la file d'attente.

Tâches du mode de verrouillage du système

1. Sur la page **OpenManage Integration for VMware vCenter**, cliquez sur l'onglet **Surveiller** > **File d'attente des tâches** et cliquez sur **Tâches du mode de verrouillage du système**.

Les informations suivantes sur les tâches du mode de verrouillage du système sont affichées dans la partie supérieure de la grille :

- Nom
- Description
- Heure planifiée
- vCenter
- Condition
- Taille de la collection
- Récapitulatif d'avancement

2. Pour mettre à jour les **Détails des tâches du mode de verrouillage du système**, cliquez sur l'icône **Actualiser**.

3. Pour afficher les détails d'une tâche du mode de verrouillage du système, qui contiennent des informations détaillées sur les serveurs inclus dans cette tâche, sélectionnez une tâche du mode de verrouillage du système dans la grille supérieure.

Les détails suivants apparaissent sur la grille inférieure :

- Numéro de service
- IP iDRAC
- Nom d'hôte


- Condition
- Détails

REMARQUE : Si la colonne **État** indique **Réussite**, la colonne **Détails** est vide.

Si la colonne État indique Échec, des informations sur l'échec s'affichent dans la colonne Détails.

- Date et heure de début
- Date et heure de fin

Vous pouvez afficher les informations complètes concernant une tâche du mode de verrouillage du système dans une fenêtre contextuelle en sélectionnant la tâche et en passant le curseur de la souris sur la colonne **Détails** de cette tâche.

4. Pour vider les tâches du mode de verrouillage du système, cliquez sur . Sélectionnez **Plus anciennes que la date et l'état de tâche**, puis cliquez sur **Appliquer**.

Les tâches sélectionnées sont alors supprimées de la file d'attente.

Tâches de détection de dérive

Une tâche de découverte de dérive est exécutée pour trouver la comparaison entre la ligne de base validée et la configuration du serveur qui inclut la configuration du matériel, et les versions du micrologiciel et du pilote.

1. Sur la page **OpenManage Integration for VMware vCenter**, cliquez sur l'onglet **Surveiller** > **File d'attente des tâches**, puis cliquez sur **Tâches de détection de dérive**.

Les informations suivantes sur les tâches de détection de dérive sont affichées dans la partie supérieure de la grille :

- Nom
- Dernière exécution
- Prochaine exécution
- Statut
- Taille de la collection
- Récapitulatif d'avancement

2. Afin d'afficher la mise à jour **Détails sur la tâche de détection de dérive**, cliquez sur **Actualiser**.

3. Pour afficher les détails d'une tâche de détection de dérive, qui contiennent des informations détaillées sur les serveurs inclus dans la tâche de détection de dérive, sélectionnez une tâche de détection de dérive sur la grille supérieure.

Les détails suivants apparaissent sur la grille inférieure :

- Numéro de service
- IP iDRAC
- Nom d'hôte
- Cluster
- vCenter
- Statut
- Date et heure de début
- Date et heure de fin

4. Pour exécuter la tâche **Détection des dérives** à la demande, cliquez sur .

REMARQUE : Dans un cluster de la ligne de base, après l'ajout d'un périphérique hôte au profil de connexion, la tâche de détection de dérive est automatiquement exécutée sur un périphérique hôte nouvellement ajouté.

Gestion des tâches de mise à jour de micrologiciel -

Pour afficher les informations de cette page, exécutez une tâche de mise à jour de micrologiciel pour un cluster. Voir [Exécution de l'Assistant Mise à jour du micrologiciel pour les clusters](#).

La page affiche toutes les tâches de mise à jour de micrologiciel. Sur cette page vous pouvez afficher, actualiser, purger ou annuler vos tâches de mise à jour de micrologiciel.

1. Dans OpenManage Integration, sélectionnez **Surveiller** > **File d'attente des tâches** > **Mises à jour de micrologiciel**.
2. Pour afficher les informations les plus récentes, cliquez sur l'icône **Actualiser**.
3. Affichez l'état dans la grille de données.

La grille fournit les informations suivantes à propos des tâches de mise à jour de micrologiciel :

- État

- Heure planifiée
 - Nom
 - Description
 - vCenter
 - Taille de la collection (nombre de serveurs dans cette tâche d'inventaire de micrologiciel)
 - Récapitulatif de l'avancement (informations sur la progression de la mise à jour du micrologiciel)
4. Pour afficher des informations plus détaillées sur une tâche spécifique, sélectionnez cette tâche dans la grille de données.

Vous trouverez ci-dessous les détails suivants :

- Nom d'hôte
- État
- Heure de début
- Heure de fin

5. Pour annuler une mise à jour de micrologiciel planifiée mais non exécutée, sélectionnez la tâche à annuler puis cliquez sur .

REMARQUE : Si vous annulez une tâche de mise à jour de micrologiciel déjà soumise au contrôleur iDRAC, le micrologiciel peut encore être mis à jour sur l'hôte, mais OMIVV signale que la tâche a été annulée.

6. Pour purger des tâches de mise à jour de micrologiciel antérieures ou planifiées, cliquez sur .

La boîte de dialogue **Purger des tâches de mise à jour de micrologiciel** s'affiche. Seules les tâches ayant été annulées ou réussies ou celles ayant échoué peuvent être purgées. En effet, vous ne pouvez pas purger des tâches planifiées ou actives.

7. Dans la boîte de dialogue **Purger des tâches de mise à jour de micrologiciel**, sélectionnez **Antérieure à**, puis cliquez sur **Appliquer**.

Les tâches sélectionnées sont alors supprimées de la file d'attente.

Synchronisation de la tâche de déploiement

Le provisionnement et le déploiement de serveurs sans système d'exploitation peuvent prendre de 30 minutes à plusieurs heures, en fonction de plusieurs facteurs. Avant de démarrer une tâche de déploiement, il est conseillé de planifier l'heure de déploiement à partir des indications fournies. La durée nécessaire au provisionnement et au déploiement varie en fonction du type de déploiement, de la complexité et du nombre de tâches de déploiement exécutées simultanément. Le tableau suivant indique la durée approximative d'une tâche de déploiement : les tâches de déploiement sont exécutées par lots de jusqu'à cinq serveurs simultanés afin de raccourcir la durée totale de la tâche de déploiement. Le nombre exact de tâches simultanées dépend des ressources disponibles.

Tableau 37. Durée approximative du déploiement

Type de déploiement	Durée approximative par déploiement
Hyperviseur uniquement	De 30 à 130 minutes
Profils matériel et d'hyperviseur	De 1 à 4 heures
Profil système uniquement	De 5 à 6 minutes
Profil système et profil d'hyperviseur	De 30 à 40 minutes

États du serveur dans la séquence de déploiement

Quand un travail d'inventaire est exécuté, les serveurs sans système d'exploitation détectés sont classés selon différents états pour déterminer si le serveur est nouveau dans le datacenter ou s'il est associé à une tâche de déploiement prévue. Les administrateurs peuvent utiliser les états suivants pour déterminer si un serveur doit être inclus dans une tâche de déploiement. Les états suivants existent :

Tableau 38. États du serveur dans la séquence de déploiement

État du serveur	Description
Non configuré	Le serveur a contacté OMIVV et attend d'être configuré.
Configuré	Le serveur est configuré avec toutes les informations matérielles requises pour réussir le déploiement de l'hyperviseur.

Téléchargement d'images ISO EMC Dell personnalisées

Les images ESXi personnalisées qui contiennent tous les pilotes Dell sont requises pour le déploiement.

1. Accédez à support.dell.com.
2. Cliquez sur **Choisir parmi tous les produits > Serveurs, stockage, et mise en réseau**.
3. Sous **Sélectionner un produit**, cliquez sur **PowerEdge**.
4. Cliquez sur un modèle de serveur PowerEdge.
5. Cliquez sur la page **Pilotes et téléchargements** du modèle de serveur.
6. Cliquez sur le lien **Changer de système d'exploitation**, puis sélectionnez le système ESXi souhaité.
7. Cliquez sur **Solutions d'entreprise**.
8. Dans la liste **Solutions d'entreprise**, sélectionnez la version d'ISO requise, puis cliquez sur **Télécharger**.

À propos de la conformité des hôtes, des serveurs sans système d'exploitation et des iDRAC

Pour gérer les hôtes et les serveurs sans système d'exploitation avec OMIVV, ceux-ci doivent satisfaire certains critères minimum. S'ils ne sont pas conformes, ils ne sont pas gérés correctement par OMIVV. OMIVV affiche des informations sur la non-conformité d'un serveur sans système d'exploitation ou d'un hôte et vous permet de corriger ce problème, le cas échéant.

Dans chaque cas, vous pouvez afficher et corriger les problèmes de conformité en exécutant une des opérations suivantes :

- Pour afficher et corriger les problèmes de conformité des hôtes vSphere, voir [Exécution de l'Assistant Correction des hôtes vSphere non conformes](#).
- Pour afficher et corriger les problèmes de conformité des serveurs sans système d'exploitation, voir [Exécution de l'Assistant Correction des serveurs sans système d'exploitation non conformes](#).

Sujets :

- [Rapport et résolution de conformité des hôtes vSphere](#)
- [Affichage de la conformité de ligne de base](#)
- [Utilisation d'OMSA avec les serveurs de 11e génération](#)
- [Rapports et correction de conformité pour les serveurs sans système d'exploitation](#)

Rapport et résolution de conformité des hôtes vSphere

Un hôte est non conforme lorsque :

- l'hôte n'est pas attribué à un profil de connexion ;
- la fonction de collecte de l'inventaire système au redémarrage (CSIOR) est désactivée ou n'a pas été exécutée, ce qui nécessite un redémarrage manuel ;
- L'agent OMSA n'est pas installé, est obsolète ou n'est pas correctement configuré. Le redémarrage d'un hôte ESXi est requis si OMSA est installé ou mis à jour pour des serveurs de 11e génération.
- La destination d'interruption SNMP de l'hôte n'est pas configurée pour l'adresse IP de l'appliance OMIVV. L'échec de la configuration de la destination d'interruption SNMP de l'hôte est peut-être dû à des informations d'identification de l'iDRAC ou de l'hôte non valides dans le profil de connexion. Il est également possible qu'il n'existe aucun logement disponible dans l'iDRAC ou que le mode de verrouillage de l'iDRAC soit activé (uniquement pour les hôtes de 14e génération).
- OMIVV n'a pas activé le service WBEM sur les hôtes exécutant ESXi 6.5.

⚠ PRÉCAUTION : Les hôtes en mode verrouillage ne s'affichent pas dans les contrôles de conformité, même s'ils ne sont pas conformes. Ils ne s'affichent pas parce que leur état de conformité ne peut pas être déterminé. Vérifiez la conformité de ces systèmes manuellement. Dans ce cas, un message d'avertissement s'affiche.

Vous pouvez exécuter l'Assistant Correction des hôtes vSphere non conformes pour corriger les hôtes non conformes. Certains hôtes ESXi non conformes exigent un redémarrage. Le redémarrage d'un hôte ESXi est requis si OMSA doit être installé ou mis à jour. De plus, un redémarrage est requis sur tout hôte qui n'a jamais exécuté CSIOR. Si vous choisissez de redémarrer automatiquement un hôte ESXi, les actions suivantes sont effectuées :

- Pour une correction de l'état CSIOR :
Si CSIOR n'a jamais été exécuté sur l'hôte, CSIOR est configuré sur **ON** sur l'hôte, et l'hôte est configuré en mode maintenance et redémarré.
- Pour les hôtes qui ne disposent pas de l'agent OMSA ou qui exécutent une version non prise en charge de celui-ci :
 - OMSA est installé sur l'hôte.

- L'hôte est configuré en mode de maintenance et redémarré.
- Au terme du redémarrage, l'agent OMSA est configuré pour que les modifications s'appliquent.
- L'hôte sort du mode de maintenance.
- L'inventaire est exécuté pour actualiser les données.
- Pour corriger l'état de l'agent OMSA lorsqu'une version prise en charge de celui-ci est installée mais nécessite une configuration :
 - L'agent OMSA est configuré sur l'hôte.
 - L'inventaire est exécuté pour actualiser les données.

Pour afficher et corriger les hôtes non conformes :

1. Dans OpenManage Integration for VMware vCenter, dans l'onglet **Gérer**, cliquez sur **Conformité > Hôtes vSphere**.
 - a) Dans la page **Hôtes vSphere**, affichez la liste des hôtes non conformes.
Un tableau répertorie les hôtes non conformes, ainsi que l'IP ou le nom de l'hôte, le modèle, le profil de connexion, l'état CSIOR, l'état OMSA, l'état WBEM, l'état d'interruption SNMP, l'hyperviseur et l'état de la licence iDRAC.
 - b) Pour afficher plus de détails sur un hôte non conforme, sélectionnez un hôte non conforme.
 - c) Pour permuter les colonnes dans le tableau, glissez et déplacez les colonnes dans la grille de données.
2. Pour corriger les hôtes non conformes, cliquez sur **Corriger les hôtes vSphere non conformes**.
L'Assistant **Correction des hôtes vSphere non conformes** est lancé. Il s'agit d'un Assistant dynamique qui affiche uniquement les pages relatives aux hôtes non conformes sélectionnés.
Si tous les hôtes non conformes sélectionnés sont conformes à CSIOR, vous pouvez consulter la page **Activer CSIOR** de l'Assistant.
3. Dans l'Assistant **Correction des hôtes vSphere non conformes**, cliquez sur **Suivant** dans la page **Bienvenue**.
4. Dans la page **Assistant Sélection des hôtes vSphere pour corriger leur conformité**, sélectionnez les cases à cocher des hôtes que vous souhaitez corriger.
5. Cliquez sur **Suivant**.
Un message d'avertissement s'affiche si des hôtes sélectionnés ne sont pas affectés à un profil de connexion et vous invite à continuer avec l'Assistant Conformité ou à annuler l'Assistant Conformité. Pour corriger la non-conformité du profil de connexion, effectuez l'une des opérations suivantes :
 - Pour exclure les hôtes sans profil de connexion attribué depuis l'Assistant Conformité, cliquez sur **Continuer avec l'Assistant Conformité**.
 - Pour quitter l'Assistant et corriger les systèmes sur la page **Profil de connexion**, cliquez sur **Annuler**. Voir [Création d'un profil de connexion](#). Lorsqu'un profil de connexion est créé, vous pouvez retourner à l'Assistant.
6. Si vous cliquez sur **Continuer avec l'Assistant Conformité** dans le message d'avertissement, dans la fenêtre **Activer CSIOR**, sélectionnez les cases à cocher pour activer **CSIOR** pour les hôtes sélectionnés.
7. Cliquez sur **Suivant**.
8. Dans la fenêtre **Corriger OMSA**, cochez les cases pour corriger **OMSA** pour les hôtes sélectionnés.
9. Cliquez sur **Suivant**.
10. Dans la fenêtre **Redémarrer les hôtes**, visualisez les hôtes ESXi devant être redémarrés.
Le redémarrage d'un hôte ESXi est requis, si OMSA est installé ou mis à jour. De plus, un redémarrage est requis sur tout hôte qui n'a jamais exécuté CSIOR. Effectuez l'une des opérations suivantes :
 - Si vous voulez mettre automatiquement les hôtes en mode de maintenance et les redémarrer au besoin, sélectionnez la case **Mettre automatiquement les hôtes en mode de maintenance et les redémarrer au besoin**.
 - Si vous voulez effectuer un redémarrage manuel, redémarrez l'hôte après l'installation d'OMSA, configurez OMSA manuellement ou via l'Assistant Conformité lorsque l'hôte est en cours d'exécution et si OMSA n'est pas configuré, puis réexécutez l'inventaire. Voir la section [Exécution des tâches d'inventaire](#).
11. Cliquez sur **Suivant**.
12. Dans la fenêtre **Récapitulatif**, examinez les actions qui ont lieu sur les hôtes non conformes.
Des redémarrages manuels sont requis pour que les actions de la page Récapitulatif prennent effet.
13. Cliquez sur **Terminer**.

L'Assistant définit l'état de la destination d'interruption SNMP sur **Configuré** lorsque que vous avez corrigé les informations d'identification de l'hôte ou de l'iDRAC en indiquant les informations valides dans le profil de connexion et libéré l'un des quatre premiers logements disponibles dans la destination d'interruption de l'iDRAC ou si vous avez désactivé le mode de verrouillage du système dans l'iDRAC.

 **REMARQUE : Le mode de verrouillage du système s'applique uniquement aux serveurs de 14e génération.**

S'il existe des hôtes non conformes WBEM, corrigez manuellement les conditions d'utilisation des hôtes qui provoquent l'échec de l'activation du service WBEM. Vous pouvez résoudre les erreurs de conditions en les consultant dans les journaux utilisateur, puis en autorisant OMIVV à activer le service WBEM pour ces hôtes durant l'inventaire.

Résolution de la conformité de la licence iDRAC des hôtes vSphere

Les hôtes vSphere répertoriés sur les pages de conformité des hôtes vSphere sont non conformes car ils ne disposent d'aucune licence iDRAC compatible. Ce tableau présente l'état de la licence iDRAC. Vous pouvez cliquer sur un hôte non conforme pour afficher des informations supplémentaires, comme le nombre de jours restants avant l'expiration de la licence iDRAC et, si nécessaire, procéder à sa mise à jour. Le lien **Exécuter une tâche d'inventaire** est actif si l'état de conformité de l'iDRAC est « Non conforme » ou « Inconnu » pour l'un des hôtes associés à un profil de connexion.

1. Dans OpenManage Integration for VMware vCenter, dans l'onglet **Gérer**, cliquez sur **Conformité > Hôtes vSphere**.
2. Sélectionnez un hôte dont l'**État de la licence iDRAC** est **Non conforme**.
3. Si la licence a expiré, cliquez sur le lien **Acheter/Renouveler une licence iDRAC**.
4. Connectez-vous à la page **Gestion de licences Dell** et mettez à jour ou achetez une nouvelle licence iDRAC. Utilisez les informations sur cette page pour identifier et mettre à jour votre iDRAC.
5. Après avoir installé une licence iDRAC, exécutez une tâche d'inventaire pour l'hôte vSphere et revenez sur cette page une fois l'hôte identifié comme conforme.

Affichage de la conformité de ligne de base

La page **Conformité de la ligne de base** affiche l'état de conformité de la ligne de base basé sur la détection de dérive pour tous les hôtes vSAN gérés par OMIVV associés à un profil de cluster.

- Conformité de la configuration : affiche la dérive des attributs entre le profil de système utilisé dans le profil de cluster et les hôtes vSAN associés.
 - Conformité du micrologiciel et des pilotes : affiche la dérive de la version du micrologiciel et du pilote entre les profils de logithèque de micrologiciels et/ou des pilotes utilisés dans le profil de cluster et les hôtes vSAN associés.
1. Dans la page **OpenManage Integration for VMware vCenter**, cliquez sur **Gérer > Conformité > Conformité de ligne de base**. Un tableau qui s'affiche répertorie les hôtes non conformes associés à la ligne de base, ainsi que l'IP ou le FQDN de l'hôte, l'IP ou le FQDN du vCenter, le nom du cluster, le nom de profil du cluster, et l'état de conformité de la configuration, du micrologiciel et du pilote.

REMARQUE : Seuls les hôtes non conformes sont affichés sur la page **Conformité de la ligne de base**.

Les catégories de conformité sont les suivantes :

- **Conforme** : indique que les composants de l'hôte sont conformes avec les profils associés dans la ligne de base.
- **Non conforme** : indique que les composants de l'hôte ne sont pas conformes aux profils associés dans la ligne de base.
- **Non applicable** : indique que les profils de micrologiciel, de pilote ou système ne sont pas associés au profil de cluster.

- a. Pour afficher plus de détails sur un hôte, sélectionnez l'hôte de votre choix.

Vous pouvez afficher le **nom d'hôte** et l'**heure de détection de la dernière dérive** dans le volet inférieur.

- b. Pour permuter les colonnes dans le tableau, faites glisser les colonnes dans la grille de données.
- c. Pour filtrer le contenu de la grille de données, utilisez **Filtre**.

REMARQUE : Vous pouvez consulter les informations suivantes à propos de la page **Conformité de la ligne de base** :

- **Nombre total d'hôtes non conformes**
- **Nombre total de clusters non conformes**
- **Nombre total d'hôtes et de clusters associés à la ligne de base**
- **Nombre total de distributions d'hôtes non conformes de type dérive**

2. Lorsque la tâche de détection de dérive a été correctement exécutée, les hôtes associés à la ligne de base sont répertoriés dans le tableau. Pour afficher les détails sur la dérive, sélectionnez un hôte de votre choix, puis cliquez sur **Afficher les détails sur la dérive**. La boîte de dialogue **Détails sur la dérive** s'affiche.

3. Dans la boîte de dialogue **Détails sur la dérive**, vous pouvez afficher les éléments suivants :

- En cas d'échec de la tâche de détection de dérive de conformité, l'état de conformité indique « Non conforme » ainsi que le motif de l'échec. Utilisez la raison indiquée pour résoudre le problème.
- En cas d'exécution réussie de la tâche de détection de dérive, l'état de conformité indique « Non conforme » et les informations suivantes s'affichent sur la page **Détails sur la dérive** :

Pour le matériel :

- Instance : indique le nom du composant matériel.
- Groupe : indique le nom du groupe des attributs.
- Nom d'attribut : indique le nom d'attribut.
- Valeur actuelle : indique la valeur de l'hôte.
- Valeur de la ligne de base : indique la valeur de la ligne de base.
- Type de dérive : indique le motif de non-conformité. Pour plus d'informations sur le type de dérive, voir [Matrice de comparaison de la version du composant avec la version de ligne de base](#).

Pour le micrologiciel et le pilote :

- Nom du composant : affiche le nom du composant.
- Valeur actuelle : indique la valeur de l'hôte.
- Valeur de la ligne de base : indique la valeur de la ligne de base.
- Type de dérive : indique le motif de non-conformité. Pour plus d'informations sur le type de dérive, voir [Matrice de comparaison de la version du composant avec la version de ligne de base](#).
- Importance (pour le micrologiciel) : indique le niveau d'importance de la mise à jour de la version d'un composant identifié.
- Recommandation (pour le pilote) : indique le niveau d'importance de la mise à jour de la version d'un composant identifié.
- Redémarrage requis : indique si l'appliance doit être redémarrée ou non.

REMARQUE : Si plusieurs versions du micrologiciel sont disponibles, la version la plus récente est toujours utilisée pour la comparaison de conformité.

4. Cliquez sur **Terminer**.

Utilisation d'OMSA avec les serveurs de 11e génération

Pour gérer les serveurs PowerEdge de 11e génération avec OMIVV, OMSA doit être exécuté sur ceux-ci. Pour un hôte de 11e génération déployé via OMIVV, OMSA est installé automatiquement. Pour les hôtes de 11e génération déployés manuellement, vous pouvez choisir l'une des méthodes suivantes :

- Installez et configurez OMSA à l'aide d'OMIVV. Voir [Configuration d'une destination d'interruption OMSA](#).
- Installez et configurez OMSA manuellement. Voir [Déploiement de l'agent OMSA sur un système ESXi](#).

REMARQUE : Lors du déploiement de l'agent OMSA via OMIVV, ce dernier démarre le service HttpClient et active le port 8080 (pour les versions ultérieures à ESXi 5.0) pour télécharger le VIB OMSA et l'installer. Une fois l'installation d'OMSA terminée, le service s'arrête automatiquement et le port se ferme.

REMARQUE : Outre les options ci-dessus, vous pouvez utiliser la conformité de l'hôte du client Web qui installe et configure l'agent OMSA.

Déploiement de l'agent OMSA sur un système ESXi

Installez le VIB OMSA sur un système ESXi pour rassembler les informations d'inventaire et d'alerte des systèmes.

REMARQUE : Des agents OpenManage doivent être installés sur les hôtes Dell antérieurs aux serveurs Dell PowerEdge de 12e génération. Installez OMSA à l'aide d'OpenManage Integration for VMware vCenter ou installez-le manuellement sur les hôtes avant d'installer OpenManage Integration for VMware vCenter. Vous trouverez des informations détaillées sur l'installation manuelle des agents OMSA à l'adresse <http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx>

1. Si OMSA n'est pas installé, installez l'outil de ligne de commande vSphere (vSphere CLI) depuis <http://www.vmware.com>.
2. Entrez la commande suivante :

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

REMARQUE : L'installation d'OMSA peut prendre quelques minutes. Cette commande exige le redémarrage de l'hôte lorsqu'elle est terminée.

REMARQUE : La chaîne de communauté SNMP peut être configurée à partir de **Gérer > Paramètres > Paramètres de l'appliance > Chaîne de communauté d'interruption SNMP OMSA**. Pour plus d'informations à propos de la chaîne de communauté d'interruption SNMP, voir [Configurer la chaîne de communauté d'interruption SNMP](#).

Configuration d'une destination d'interruption OMSA

L'agent OMSA doit être configuré sur tous les hôtes de 11e génération.

REMARQUE : L'agent OMSA est uniquement requis sur les serveurs Dell EMC antérieurs aux serveurs PowerEdge de 12e génération.

Pour configurer une destination d'interruption OMSA :

1. Accédez à l'agent OMSA à partir d'un navigateur Web en fournissant l'URL `https://<HostIP>:1311/`.
2. Connectez-vous à l'interface et sélectionnez l'onglet **Gestion des alertes**.
3. Sélectionnez **Actions d'alerte** et vérifiez que l'option **Diffuser le message** est activée pour tous les événements à surveiller, afin que ces événements soient envoyés.
4. Sélectionnez l'option **Événements de plate-forme** en haut de l'onglet.
5. Cliquez sur le bouton **Configurer les destinations**, puis cliquez sur le lien **Destination**.
6. Cochez la case **Activer la destination**.
7. Entrez l'adresse IP de l'appliance OMIVV dans le champ **Adresse IP de destination**.
8. Cliquez sur **Appliquer les modifications**.
9. Répétez les étapes 1 à 8 pour configurer d'autres événements.


REMARQUE : La chaîne de communauté SNMP peut être configurée à partir de **Gérer > Paramètres > Paramètres de l'appliance > Chaîne de communauté d'interruption SNMP OMSA**. Pour plus d'informations à propos de la chaîne de communauté d'interruption SNMP, voir [Configurer la chaîne de communauté d'interruption SNMP](#).

Rapports et correction de conformité pour les serveurs sans système d'exploitation

Un serveur sans système d'exploitation est non conforme dans les cas suivants :

- Il ne s'agit pas d'un serveur pris en charge.
- Il ne possède aucune licence iDRAC prise en charge (iDRAC Express étant l'exigence minimale).
- Il ne dispose d'aucune version prise en charge du contrôleur iDRAC, du BIOS ou du contrôleur LC.
- LOM ou rNDC n'est pas présent.
- Le mode de verrouillage du système est activé.

Pour afficher et corriger la liste de serveurs sans système d'exploitation non conformes :

1. Dans OpenManage Integration for VMware vCenter, sélectionnez l'onglet **Gérer > Déploiement**.
 - a) Dans la page **Serveurs sans système d'exploitation**, affichez la liste des serveurs non conformes.
Le tableau qui s'affiche répertorie les serveurs non conformes ainsi que le numéro de service, le modèle, l'adresse IP iDRAC, l'état du serveur, le mode de verrouillage du système, l'état de conformité et l'état de la licence iDRAC.
 - b) Pour afficher davantage de détails sur un serveur, sélectionnez un serveur non conforme.
 - c) Pour exporter les informations non conformes d'un serveur dans un fichier CSV, dans l'angle droit du tableau, cliquez sur .
 - d) Pour filtrer le contenu de la grille de données, cliquez sur le champ **Filtre**.
 - e) Pour permuter les colonnes dans le tableau, glissez et déplacez les colonnes dans la grille de données.
2. Pour corriger les serveurs non conformes, cliquez sur **Corriger les serveurs non conformes**.

REMARQUE : Le lien **Corriger les serveurs non conformes** est activé uniquement pour serveurs non conformes de 11e génération.

3. Dans l'Assistant **Corriger la conformité des serveurs sans système d'exploitation**, cliquez sur **Suivant** dans la page **Bienvenue**.
4. Dans l'Assistant **Corriger la conformité**, cochez les cases correspondant aux serveurs à corriger.

Les serveurs non conformes sont répertoriés, accompagnés des composants de micrologiciel pour lesquels ils sont non conformes. Les serveurs non conformes répertoriés requièrent la mise à jour d'au moins un des composants de micrologiciel suivants :

- IP iDRAC

REMARQUE : OMIVV ne vous permet pas de corriger les serveurs sans système d'exploitation dont les licences iDRAC sont non conformes. Chargez la licence iDRAC prise en charge sur ces serveurs en dehors d'OMIVV, puis cliquez sur **Actualiser les serveurs sans système d'exploitation**. Voir **Actualisation d'un serveur sans système d'exploitation**.

- BIOS

- LC

- Mode de verrouillage du système

REMARQUE : Pour afficher les détails les plus récents sur les serveurs sans système d'exploitation non conformes à partir de l'iDRAC correspondant, cliquez sur **Actualiser les informations des serveurs sans système d'exploitation**. Si l'option Mode de verrouillage du système est activée, le serveur est non conforme, et inversement.

5. Pour afficher les détails des problèmes de conformité, cliquez sur **Problèmes de conformité**.

REMARQUE : Si un serveur sans système d'exploitation est non conforme en raison du mode de verrouillage du système activé, configurez manuellement le mode de verrouillage du système du serveur à partir de la console iDRAC.

6. Cliquez sur **Suivant**.

7. Dans la fenêtre **Récapitulatif**, examinez les actions qui ont lieu sur les composants de micrologiciel des serveurs sans système d'exploitation non conformes.

8. Cliquez sur **Terminer**.

Résolution de la conformité de la licence iDRAC des serveurs sans système d'exploitation

Les serveurs sans système d'exploitation répertoriés sur la page **Serveurs sans système d'exploitation** sont non conformes car ils ne disposent d'aucune licence iDRAC compatible. Un tableau présente l'état de la licence iDRAC. Vous pouvez cliquer sur un serveur sans système d'exploitation non conforme pour afficher des informations supplémentaires, comme le nombre de jours restants avant l'expiration de la licence iDRAC et, si nécessaire, procéder à sa mise à jour. Si le lien **Actualiser les serveurs sans système d'exploitation** est activé sur la page **Serveurs sans système d'exploitation**, des serveurs sans système d'exploitation sont non conformes en raison de la licence iDRAC.

1. Dans OpenManage Integration for VMware vCenter, sélectionnez l'onglet **Gérer > Déploiement**.
Sur la page **Serveurs sans système d'exploitation**, consultez la liste des serveurs non conformes présentée sous forme de tableau.
2. Sélectionnez un serveur sans système d'exploitation dont l'**État de la licence iDRAC** est **Non conforme** ou **Inconnu**.
3. Si la licence a expiré, cliquez sur le lien **Acheter/Renouveler une licence iDRAC**.
4. Connectez-vous à la page **Gestion de licences Dell** et mettez à jour ou achetez une nouvelle licence iDRAC.
Utilisez les informations sur cette page pour identifier et mettre à jour votre iDRAC.
5. Après avoir installé une licence iDRAC, cliquez sur **Actualiser les serveurs sans système d'exploitation**.

Actualisation d'un serveur sans système d'exploitation

1. Sur la page **OpenManage Integration for VMware vCenter**, cliquez sur **Gérer > Déploiement > Serveurs sans système d'exploitation**, puis cliquez sur **Actualiser les serveurs sans système d'exploitation**.
2. Dans la fenêtre **Actualiser les serveurs sans système d'exploitation**, sélectionnez les serveurs dont vous souhaitez actualiser les données, puis cliquez sur **Actualiser la sélection des serveurs**.

L'actualisation des données des serveurs sans système d'exploitation peut prendre quelques minutes.

Toutes les données des serveurs sans système d'exploitation sélectionnés sont actualisées sur la page **Serveurs sans système d'exploitation**.

Autorisations et rôles de sécurité

OpenManage Integration for VMware vCenter stocke les informations d'identification utilisateur sous forme cryptée. Il ne fournit aucun mot de passe aux applications clientes afin d'éviter toute demande abusive. Dans la mesure où la base de données de sauvegarde est totalement cryptée à l'aide de phrases de sécurité personnalisées, les données ne peuvent pas être utilisées de manière abusive.

Par défaut, les utilisateurs du groupe Administrateurs disposent de tous les privilèges. Les administrateurs peuvent utiliser toutes les fonctions d'OpenManage Integration for VMware vCenter au sein du client Web VMware vSphere. Si vous souhaitez qu'un utilisateur doté des privilèges nécessaires gère le produit, effectuez les opérations suivantes :

1. Créez un rôle avec les privilèges nécessaires.
2. Enregistrez un serveur vCenter avec l'utilisateur.
3. Ajoutez les deux rôles Dell : le rôle opérationnel Dell et le rôle de déploiement de l'infrastructure Dell.

Sujets :

- [Intégrité des données](#)
- [Rôles, autorisation et authentification de contrôle d'accès](#)
- [Rôle opérationnel Dell](#)
- [Rôle de déploiement de l'infrastructure Dell](#)
- [À propos des privilèges](#)

Intégrité des données

La communication entre OpenManage Integration for VMware vCenter, la Console Administration et vCenter est effectuée à l'aide de SSL/HTTPS. L'OpenManage Integration for VMware vCenter génère un certificat SSL utilisé pour la communication de confiance entre vCenter et l'appliance. Il vérifie également et reconnaît le certificat du serveur vCenter avant la communication et l'enregistrement d'OpenManage Integration for VMware vCenter. L'onglet Console d'OpenManage Integration for VMware vCenter utilise des procédures de sécurité pour éviter le traitement des mauvaises requêtes alors que les clés sont transférées de la Console Administration vers les services dorsaux et inversement. Ce type de sécurité entraîne l'échec des requêtes entre sites.

Une session de Console Administration sécurisée possède une durée d'inactivité de 5 minutes. Elle est valide uniquement dans la fenêtre et/ou l'onglet actuel du navigateur. Si vous essayez d'ouvrir la session dans une nouvelle fenêtre ou un nouvel onglet, un message d'erreur de sécurité demandant une session valide s'affiche. Cette action empêche également l'utilisateur de cliquer sur une URL malveillante susceptible d'entraîner une attaque dans la session de Console Administration.

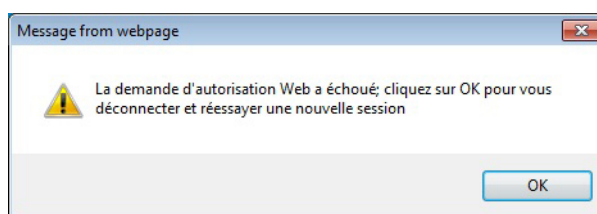


Figure 3. Message d'erreur de sécurité

Rôles, autorisation et authentification de contrôle d'accès

Pour effectuer les opérations vCenter, OpenManage Integration for VMware vCenter utilise la session utilisateur actuel du client Web et les informations d'identification d'administration enregistrées pour OpenManage Integration. OpenManage Integration for VMware vCenter utilise le modèle de privilèges et de rôles intégré du serveur vCenter pour autoriser les actions de l'utilisateur auprès d'OpenManage Integration et des objets gérés vCenter (hôtes et clusters).

Rôle opérationnel Dell

Le rôle comprend les privilèges/groupes permettant d'effectuer les tâches d'appliance et de serveurs vCenter, notamment les mises à jour de micrologiciel, les inventaires de matériel, le redémarrage d'un hôte, le placement d'un hôte en mode maintenance ou la création d'une tâche de serveur vCenter.

Ce rôle comprend les groupes de privilèges suivants.

Tableau 39. Groupes de privilèges

Nom du groupe	Description
Groupe de privilèges : Dell.Configuration	Effectuer les tâches associées à l'hôte, Effectuer les tâches associées à vCenter, Configurer SelLog, Configurer ConnectionProfile, Configurer ClearLed, Mettre à jour le micrologiciel
Groupe de privilèges : Dell.Inventory	Configurer l'inventaire, Configurer la récupération de garantie, Configurer ReadOnly
Groupe de privilèges : Dell.Monitoring	Configurer la surveillance, le moniteur
Groupe de privilèges : Dell.Reporting (Non utilisé)	Créer un rapport, Exécuter un rapport

Rôle de déploiement de l'infrastructure Dell

Le rôle comprend les privilèges associés aux fonctionnalités de déploiement d'hyperviseur.

Les privilèges fournis par ce rôle sont Créer un modèle, Configurer le profil de configuration matérielle, Configurer le profil de déploiement d'hyperviseur, Configurer le profil de connexion, Attribuer une identité et Déployer

Groupe de privilèges : Dell.Deploy-Provisioning

Créer un modèle, Configurer le profil de configuration matérielle, Configurer le profil de déploiement d'hyperviseur, Configurer le profil de connexion, Attribuer une identité et Déployer

À propos des privilèges

Chaque action effectuée par OpenManage Integration for VMware vCenter est associée à un privilège. Les sections suivantes répertorient les actions disponibles et les privilèges associés :

- Tâches relatives à Dell.Configuration.Perform vCenter
 - Sortir et entrer en mode de maintenance
 - Obtenir le groupe d'utilisateurs vCenter pour demander les autorisations
 - Enregistrer et configurer les alertes ; par exemple, activer / désactiver les alertes sur la page Event Settings (Paramètres d'événement).
 - Publier les événements / alertes sur vCenter
 - Configurer les paramètres d'événement sur la page Event Settings (Paramètres d'événement).
 - Restaurer les alertes par défaut sur la page Event Settings (Paramètres d'événement).
 - Vérifier l'état DRS sur les clusters lors de la configuration des paramètres d'alertes / événements.
 - Redémarrer l'hôte après l'exécution de mise à jour ou de toute autre action de configuration
 - Surveiller l'état / le progrès des tâches vCenter
 - Créer des tâches vCenter ; par exemple, la tâche de mise à jour du micrologiciel, la tâche de configuration d'hôte, et la tâche d'inventaire.
 - Mettre à jour l'état / le progrès des tâches vCenter
 - Obtenir les profils d'hôte
 - Ajouter un hôte au centre de données
 - Ajouter un hôte au cluster
 - Appliquer un profil à un hôte
 - Obtenir les informations d'identification CIM
 - Configurer la conformité des hôtes
 - Obtenir l'état des tâches de conformité

- Dell.Inventory.Configure ReadOnly
 - Obtenir tous les hôtes vCenter pour construire l'arborescence lors de la configuration des profils de connexion vCenter
 - Vérifier si l'hôte est un serveur Dell lorsque l'onglet est sélectionné
 - Obtenir l'adresse IP vCenter
 - Obtenir l'adresse IP de l'hôte
 - Obtenir l'utilisateur de la session vCenter actuelle à partir de l'ID de session du client vSphere
 - Obtenir l'arborescence d'inventaire vCenter pour afficher l'inventaire vCenter dans une structure arborescente
- Dell.Monitoring.Monitor
 - Obtenir le nom d'hôte pour publier l'événement
 - Effectuer des opérations sur le journal d'événements ; par exemple, obtenir le nombre d'événements, ou modifier les paramètres du journal d'événements
 - Enregistrer, désenregistrer et configurer les événements / alertes — Recevoir des interruptions SNMP et publier des événements
- Dell.Configuration.Firmware Update
 - Effectuer mise à jour du micrologiciel
 - Charger les informations de référentiel du micrologiciel et de fichier DUP sur la page de l'assistant de mise à jour du micrologiciel
 - Interroger l'inventaire du micrologiciel
 - Configurer les paramètres de l'espace de stockage du micrologiciel
 - Configurer le dossier de préparation et effectuer une mise à jour à l'aide de la fonctionnalité de préparation
 - Tester les connexions réseau et de l'espace de stockage
- Dell.Deploy-Provisioning.Create Template
 - Configurer le profil de configuration matérielle
 - Configurer le profil de déploiement d'hyperviseur
 - Configurer le profil de connexion
 - Attribuer des identités
 - Déployer
- Tâches relatives à l'hôte Dell.Configuration.Perform
 - Faire clignoter un voyant, Éteindre un voyant, Configurer l'URL OMSA à partir de l'onglet Dell Server Management
 - Lancer la console OMSA
 - Lancer la console iDRAC
 - Afficher et effacer le journal SEL
- Dell.Inventory.Configure Inventory
 - Afficher l'inventaire du système dans l'onglet Dell Server Management
 - Obtenir les détails du stockage
 - Obtenir les détails de la surveillance de l'alimentation
 - Créer, afficher, modifier, supprimer et tester les profils de connexion sur la page Connection Profiles (Profils de connexion)
 - Planifier, mettre à jour et supprimer la planification de l'inventaire
 - Exécuter l'inventaire sur les hôtes

Questions fréquemment posées (FAQ)

Utilisez cette section pour trouver les réponses à des questions de dépannage. Cette section comprend :

- [Questions fréquemment posées \(FAQ\)](#)
- [Problèmes de déploiement de serveurs sans système d'exploitation](#)

Sujets :

- [Questions fréquemment posées \(FAQ\)](#)
- [Problèmes de déploiement de serveurs sans système d'exploitation](#)

Questions fréquemment posées (FAQ)

Cette section répertorie certaines questions et solutions courantes.

Le bouton Exporter tout ne permet pas d'exporter vers un fichier .CSV dans Google Chrome

Après l'enregistrement d'un serveur vCenter, si vous ajoutez un hôte et créez un profil de connexion, puis consultez les détails de l'inventaire de l'hôte, le bouton **Exporter tout** renvoie un échec. Le bouton **Exporter tout** n'exporte pas les informations dans un fichier .CSV.

REMARQUE :

Pour toutes les versions du navigateur Google Chrome, le bouton Exporter tout n'exporte pas les informations dans un fichier .CSV en mode navigation privée.

Résolution : pour exporter des informations vers un fichier .CSV à l'aide du bouton **Exporter tout** dans Google Chrome, désactivez le **mode navigation privée** dans le navigateur Chrome.

Version concernée : 4.0

La description et le type de licence iDRAC s'affichent de façon incorrecte pour les hôtes vSphere non conformes

Si un hôte est non conforme lorsque la fonction CSIOR est désactivée ou n'a pas été exécutée, les informations de licence iDRAC s'affichent incorrectement, bien qu'une licence iDRAC valide soit disponible. Par conséquent, vous pouvez afficher l'hôte dans liste d'hôtes vSphere, mais lorsque vous cliquez sur l'hôte pour plus de détails, les informations contenues dans **Type de licence iDRAC** sont absentes et **Description de la licence iDRAC** affiche le message « Votre licence doit être mise à niveau ».

Solution : pour résoudre ce problème, activez la fonction CSIOR sur un serveur de référence.

Version concernée : 4.0

L'icône Dell EMC ne s'affiche pas après l'annulation de l'enregistrement de vCenter sur une version d'OMIVV précédente et son enregistrement avec une version OMIVV ultérieure

Si vous désenregistrez une ancienne version OMIVV avec vCenter Server, puis enregistrez une version OMIVV ultérieure avec le même vCenter Server, il y a une entrée dans le dossier vsphere-client-serenity, qui correspond à d'anciennes données de la version OMIVV

antérieure. Par conséquent, l'icône Dell ne s'affiche pas après l'enregistrement de la version plus récente d'OMIVV, tant que des données anciennes, spécifiques à la version antérieure d'OMIVV, existent dans le dossier vsphere-client-serenity de l'appliance vCenter.

Résolution : effectuez les opérations suivantes :

1. Pour VMware vCenter, accédez à `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` et pour la version Windows de vCenter, accédez au dossier `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` sur l'appliance vCenter et remarquez que des anciennes données sont présentes, telles que :
 - `com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-3.0.0.197`
2. Supprimez manuellement le dossier correspondant à la version antérieure d'OMIVV.
3. Redémarrez le client Web de service vSphere sur le vCenter Server.

Versions concernées : toutes

Le fournisseur Dell ne s'affiche pas en tant que fournisseur de mise à jour d'intégrité

Lorsque vous enregistrez un serveur vCenter avec OMIVV, puis que vous effectuez une mise à niveau de la version de vCenter Server, en passant par exemple de vCenter 6.0 à vCenter 6.5, le fournisseur Dell ne s'affiche pas dans la liste **Fournisseur Proactive HA**.

Solution : vous pouvez mettre à niveau un vCenter enregistré pour les utilisateurs non-administrateurs ou pour les utilisateurs administrateurs. Pour effectuer la mise à niveau vers la dernière version de vCenter Server, reportez-vous à la documentation VMware, puis effectuez l'une ou l'autre des options suivantes, comme il convient :

- Pour les utilisateurs non-administrateurs :
 1. Attribuez des privilèges supplémentaires aux utilisateurs non-administrateurs, si nécessaire. Voir [Privilèges requis pour les utilisateurs non administrateurs](#).
 2. Redémarrez l'appliance OMIVV enregistrée.
 3. Fermez la session dans le client Web, puis connectez-vous à nouveau.
- Pour les utilisateurs administrateurs :
 1. Redémarrez l'appliance OMIVV enregistrée.
 2. Fermez la session dans le client Web, puis connectez-vous à nouveau.

Le fournisseur Dell est maintenant répertorié dans la liste **Fournisseur HA Proactive**.

Version concernée : 4.0

Échec de l'inventaire lors de la réalisation d'une tâche de mise à jour du micrologiciel sur un hôte ESXi 5.x

Après l'enregistrement d'un serveur vCenter, si vous effectuez une tâche de mise à jour du micrologiciel sur un hôte ESXi 5.x et sélectionnez iDRAC en tant que composant à partir de l'écran **Sélectionner un composant**, l'ESXi sur l'hôte peut ne pas être synchronisé avec la nouvelle adresse IP de l'iDRAC, ce qui entraîne une adresse IP non valide de l'iDRAC, fournie à OMIVV. Par conséquent, vous ne pouvez pas exécuter l'inventaire avec succès sur cet hôte.

Résolution : pour résoudre ce problème, redémarrez le processus sfcdb sur l'hôte ESXi. Pour plus d'informations, voir https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693.

Version concernée : 4.0

La connexion test ou l'inventaire d'hôte échoue en raison d'une adresse IP non valide ou inconnue de l'iDRAC.

La connexion test ou l'inventaire de l'hôte échoue en raison d'une adresse IP non valide ou inconnue de l'iDRAC et vous recevez des messages tels que « latences du réseau ou hôte inaccessible », « connexion refusée », « l'opération a expiré », « WSMAN », « pas de route vers l'hôte » et « adresse IP : nulle ».

1. Ouvrez la console virtuelle de l'iDRAC.
2. Appuyez sur la touche F2 et accédez à **Options de dépannage**.

3. Dans **Options de dépannage**, accédez à **Redémarrer les agents de gestion**.
4. Pour redémarrer les agents de gestion, appuyez sur la touche F11.

Une adresse IP valide de l'iDRAC est désormais disponible.

REMARQUE : L'inventaire de l'hôte peut également échouer lorsque OMIVV ne parvient pas à activer les services WBEM sur les hôtes exécutant ESXi 6.5. Pour plus d'informations sur le service WBEM, voir [Création d'un profil de connexion](#).

Lors de l'exécution de l'assistant de correction des hôtes vSphere non conformes, l'état d'un hôte spécifique s'affiche comme étant Inconnu

Lorsque vous exécutez l'assistant de correction des hôtes vSphere non conformes, l'état d'un hôte spécifique s'affiche comme étant « Inconnu ». L'état inconnu s'affiche lorsqu'iDRAC n'est pas accessible.

Résolution : vérifiez la connectivité iDRAC de l'hôte et assurez-vous que l'inventaire est exécuté avec succès.

Version concernée : 4.0

Les privilèges Dell attribués lors de l'enregistrement de l'appliance OMIVV ne sont pas supprimés après le désenregistrement d'OMIVV

Après l'enregistrement de vCenter avec une appliance OMIVV, plusieurs privilèges Dell sont ajoutés à la liste de privilèges de vCenter. Une fois que vous désenregistrez vCenter à partir de l'appliance OMIVV, les privilèges Dell ne sont pas supprimés.

REMARQUE : Le fait que les privilèges Dell ne soient pas supprimés ne présente toutefois aucune incidence sur les opérations d'OMIVV.

Version concernée : 3.1

OMIVV n'affiche pas tous les fichiers log pertinents lors des tentatives de filtrage d'une catégorie de gravité

Lorsque vous sélectionnez une catégorie de gravité pour filtrer les données de fichier log en choisissant **Toutes les catégories** dans le menu déroulant, tous les fichiers logs appartenant à une catégorie spécifique s'affichent correctement. Toutefois, si vous filtrez en choisissant **Informations** dans le menu déroulant, les fichiers log de mise à jour du micrologiciel ne sont pas affichés et seuls les fichiers log de lancement de tâche s'affichent.

Résolution : pour afficher tous les fichiers log dans OMIVV, sélectionnez **Toutes les catégories** à partir du menu déroulant Filtre.

Version concernée : 3.1

Comment puis-je résoudre le code d'erreur 2000000 provoqué par VMware Certificate Authority (VMCA) ?

Lorsque vous exécutez le gestionnaire de certificats vSphere et remplacez le certificat du serveur vCenter ou de Platform Controller Service (PSC) par un nouveau certificat d'autorité de certification et une nouvelle clé pour vCenter 6.0, OMIVV affiche un code d'erreur 2000000 et déclenche une exception.

Résolution : pour résoudre l'exception, vous devez mettre à jour les ancres ssl pour les services. Vous pouvez les mettre à jour en exécutant les scripts `ls_update_certs.py` sur PSC. Le script utilise l'ancienne empreinte du certificat en tant qu'argument de saisie et le nouveau certificat est installé. L'ancien certificat est le certificat antérieur au remplacement et le nouveau certificat est le certificat postérieur au remplacement. Pour en savoir plus, voir http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 et http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689.

Mise à jour des ancrages ssl dans Windows vSphere 6.0

1. Téléchargez le fichier Istoolutil.py.zip depuis http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701.
2. Copiez le fichier Istoolutil.py dans le dossier %VMWARE_CIS_HOME%\VMware Identity Services\Istool\scripts\.

REMARQUE : Ne réinstallez pas le fichier Istoolutil.py si vous utiliser la mise à jour 1 de vSphere 6.0.

Vous pouvez utiliser les procédures pertinentes suivantes pour mettre à jour les ancrages ssl :

- Mise à jour des ancrages ssl pour vCenter installés sur le système d'exploitation Windows : remplacez les certificats de l'installation Windows vCenter à l'aide de l'utilitaire vSphere Certificate Manager. Voir la section [Remplacement des certificats sur l'installation vCenter Windows](#).
- Mise à jour des ancrages ssl pour le serveur vCenter : remplacez les certificats sur le serveur vCenter à l'aide de l'utilitaire vSphere Certificate Manager. Voir la section [Remplacement des certificats sur l'appliance vCenter Server](#).

Le résultat obtenu à partir des procédures susmentionnées doit afficher Updated 24 service (s) et Updated 26 service (s) respectivement. Si le résultat affiché est Updated 0 service (s), l'ancienne empreinte du certificat est incorrecte. Vous pouvez réaliser les étapes suivantes pour récupérer l'ancienne empreinte du certificat. Utilisez également la procédure suivante pour récupérer l'ancienne empreinte du certificat, si **vCenter Certificate Manager** n'est pas utilisé pour remplacer les certificats :

REMARQUE : Exécutez le script ls_update_certs.py avec l'ancienne empreinte obtenue.

1. Récupérez l'ancien certificat à partir du MOB (Managed Object Browser). Voir la section [Récupération de l'ancien certificat à partir de Managed Object Browser \(MOB\)](#).
2. Extrayez l'empreinte de l'ancien certificat. Voir la section [Extraction de l'empreinte de l'ancien certificat](#).

Versions concernées : 3.0 et versions ultérieures, vCenter 6.0 et versions ultérieures

Remplacement des certificats sur l'installation vCenter Windows

Effectuez les étapes suivantes si l'utilitaire vSphere Certificate Manager est utilisé pour remplacer les certificats sur l'installation vCenter Windows :

1. Connectez-vous à l'External Platform Services Controller (contrôleur des services de plateforme externes) via la connexion Bureau à distance.
2. Ouvrez l'invite de commande en mode administratif.
3. Créez le dossier c:\certificates en utilisant la commande suivante : `mkdir c:\certificates`
4. Récupérez l'ancien certificat en utilisant la commande suivante : `"%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output c:\certificates\old_machine.crt`
5. Récupérez l'ancienne empreinte numérique de certificat en utilisant la commande suivante : `"%VMWARE_OPENSSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

REMARQUE : L'empreinte numérique de certificat récupérée est au format suivant : SHA1

Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

L'empreinte numérique est une séquence de nombres et de lettres qui se présente comme

suit :13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

6. Récupérez le nouveau certificat en utilisant la commande suivante : `"%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
7. Effectuez les opérations suivantes :
 - a) Exécutez le script `ls_update_certs.py` à l'aide de la commande suivante : `"%VMWARE_PYTHON_BIN%" ls_update_certs.py --url`
 - b) Remplacez `psc.vmware.com` par `Lookup_Service_FQDN_of_Platform_Services_Controller` et l'empreinte numérique `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` par celui obtenu à l'étape 5 à l'aide de la commande suivante : `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`

REMARQUE : Assurez-vous de fournir des informations d'identification valides.

8. Déconnectez-vous du client Web vCenter, puis reconnectez-vous une fois tous les services mis à jour.

Le lancement d'OMIVV s'effectue désormais normalement.

Remplacement des certificats sur l'appliance vCenter Server

Procédez comme suit en cas d'utilisation de l'utilitaire vSphere Certificate Manager pour remplacer les certificats sur l'appliance vCenter Server :

1. Connectez-vous à l'appliance External Platform Services Controller par le biais de la console ou d'une session Secure Shell (SSH).
2. Pour activer l'accès au shell Bash, exécutez la commande suivante : `shell.set - -enabled true`
3. Saisissez `shell`, puis appuyez sur **Entrée**.
4. Créez des dossiers ou des certificats en exécutant la commande suivante : `mkdir /certificates`
5. Récupérez l'ancien certificat en exécutant la commande suivante : `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output /certificates/old_machine.crt`
6. Récupérez l'empreinte de l'ancien certificat en exécutant la commande suivante : `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

**REMARQUE : L'empreinte numérique de certificat récupérée est au format suivant : SHA1
Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88**
**L'empreinte numérique est une séquence de nombres et de lettres qui se présente comme
suit :13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88**

7. Récupérez le nouveau certificat en exécutant la commande suivante : `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`
8. Exécutez la commande suivante pour changer de répertoire : `cd /usr/lib/vmidentity/tools/scripts/`
9. Effectuez les opérations suivantes :
 - a) Exécutez `ls_update_certs.py` à l'aide de la commande suivante : `python ls_update_certs.py --url`
 - b) Remplacez `psc.vmware.com` par `Lookup_Service_FQDN_of_Platform_Services_Controller` et l'empreinte `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` par celle obtenue à l'étape 6 en exécutant la commande suivante : `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Mot de passe"`

REMARQUE : Assurez-vous de fournir des informations d'identification valides.

10. Déconnectez-vous du client Web vCenter, puis reconnectez-vous une fois tous les services mis à jour.

Le lancement d'OMIVV s'effectue désormais normalement.

Récupération de l'ancien certificat à partir de Managed Object Browser (MOB)

Vous pouvez récupérer l'ancien certificat du système vCenter Server en vous connectant à Platform Service Controller (PSC) à l'aide de Managed Object Browser (MOB).

Pour récupérer l'ancien certificat, vous devez trouver le champ `sslTrust` de l'objet géré `ArrayOfLookupServiceRegistrationInfo` en effectuant les étapes suivantes :

REMARQUE : Dans ce guide, l'emplacement du dossier `C:\certificates\` est utilisé pour stocker tous les certificats.

1. Créez le dossier `C:\certificates\` dans PSC en exécutant la commande suivante : `mkdir C:\certificates\`.
2. Ouvrez le lien suivant dans un navigateur : `https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List`
3. Ouvrez une session avec le nom d'utilisateur `administrator@vsphere.local` et saisissez le mot de passe lorsque vous y êtes invité.

REMARQUE : Si vous utilisez un nom personnalisé pour le domaine vCenter Single Sign-On (SSO), utilisez ce nom d'utilisateur et le mot de passe associé.

4. Dans **filterCriteria**, modifiez le champ de valeur pour afficher uniquement les balises `<filtercriteria></filtercriteria>`, puis cliquez sur **Méthode d'appel**.
5. Recherchez les noms d'hôte suivants en fonction des certificats que vous remplacez°:

Tableau 40. Informations sur les critères de recherche

Ancrages d'approbation	Critères de recherche
vCenter Server	Utilisez la combinaison de touches Ctrl+F pour rechercher, nomhôte_vc_ou_IP.exemple.com sur la page
Platform Services Controller	Utilisez la combinaison de touches Ctrl+F pour rechercher, nomhôte_psc_ou_IP.exemple.com sur la page

- Repérez la valeur du champ sslTrust correspondant. La valeur du champ sslTrust est la chaîne codée en base 64 de l'ancien certificat.
- Utilisez les exemples suivants pour la mise à jour des ancrages d'approbation de Platform Services Controller ou vCenter Server.

REMARQUE : La chaîne réelle est réduite façon significative pour améliorer sa lisibilité.

- Pour vCenter Server

Tableau 41. Exemple de vCenter Server

Nom	Type	Valeur
url	anyURI	https://vcenter.vmware.local:443/sdk

- Pour Platform Services Controller

Tableau 42. Exemple de Platform Services Controller

Nom	Type	Valeur
url	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

- Copiez le contenu du champ sslTrust dans un document texte et enregistrez le document sous le nom `old_machine.txt`.
- Ouvrez le fichier `old_machine.txt` dans un éditeur de texte.
- Ajoutez les éléments suivants au début et à la fin du fichier `old_machine.txt` :
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
- Enregistrez maintenant `old_machine.txt` sous le nom `old_machine.crt`.

Vous pouvez à présent extraire l'empreinte de ce certificat.

Extraction de l'empreinte de l'ancien certificat

Vous pouvez extraire l'empreinte de l'ancien certificat et la charger dans Platform Services en procédant de l'une des manières suivantes :

- Extraire l'empreinte à l'aide d'un outil de visualisation de certificats. Voir [Extraction de l'empreinte de certificat à l'aide d'un outil de visualisation de certificats](#).
- Extraire l'empreinte à l'aide d'une ligne de commande sur l'appliance. Voir [L'extraction de l'empreinte numérique à l'aide de la ligne de commande](#).

Extraction de l'empreinte de certificat à l'aide d'un outil de visualisation de certificats

Procédez comme suit pour extraire l'empreinte de certificat :

- Sous Windows, double-cliquez sur le fichier `old_machine.txt` pour l'ouvrir dans l'outil de visualisation de certificats Windows (Windows Certificate Viewer).
- Dans Windows Certificate Viewer, sélectionnez le champ **Empreinte SHA1**.
- Copiez la chaîne de caractères de l'empreinte dans un éditeur de texte brut, puis supprimez les espaces de la chaîne ou remplacez-les par le caractère deux-points.
Par exemple, la chaîne de caractères de l'empreinte peut se présenter de l'une des manières suivantes :
 - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
 - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

L'extraction de l'empreinte numérique à l'aide de la ligne de commande

Vous pouvez consulter les sections suivantes pour en savoir plus sur l'extraction de l'empreinte numérique à l'aide de la ligne de commande sur l'appareil et l'installation Windows.

Extraction de l'empreinte numérique à l'aide de la ligne de commande sur le serveur vCenter

Effectuez les opérations suivantes :

1. Déplacer ou charger les old_machine.crt certificat à PSC dans le c : \certificates\old_machine.crt emplacement qui est créé dans l'étape 1 de récupération de l'ancien certificat procédure. Vous pouvez utiliser WinSCP Windows copie sécurisée (SCP) ou un autre client pour déplacer ou télécharger le certificat.
2. Connectez-vous à l'appareil External Platform Services Controller via Secure Shell (SSH).
3. Exécutez la commande suivante pour activer l'accès au shell Bash : shell.set --enabled true.
4. Entrez y (o), puis appuyez sur Entrée.
5. Exécutez la commande suivante pour désinstaller le VIB :

REMARQUE : L'empreinte apparaît comme une séquence de nombres et les lettres après le signe égal, lequel est le suivant : **SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71**

Extraction de l'empreinte numérique à l'aide de la ligne de commande sur l'installation Windows

Effectuez les opérations suivantes :

1. Déplacer ou charger les old_machine.crt certificat à PSC dans le c : \certificates\old_machine.crt emplacement qui est créé dans l'étape 1 de récupération de l'ancien certificat procédure. Vous pouvez utiliser WinSCP Windows copie sécurisée (SCP) ou un autre client pour déplacer ou télécharger le certificat.
2. Connectez-vous à l'External Platform Services Controller (contrôleur des services de plateforme externes) via la connexion Bureau à distance.
3. Ouvrez l'invite de commande en mode administratif.
4. Exécutez la commande suivante pour désinstaller le VIB :

REMARQUE : L'empreinte apparaît comme une séquence de nombres et les lettres après le signe égal, lequel est le suivant : **SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B**

Exécutez le script ls_update_certs.py avec l'ancienne empreinte numérique obtenue. Déconnectez-vous du client Web vCenter, puis reconnectez-vous une fois tous les services mis à jour. Le plug-in Dell est lancé avec succès.

Dans l'Administration Console, le chemin d'accès vers l'espace de stockage des mises à jour est défini sur la valeur par défaut après que j'ai rétabli les paramètres d'usine

Après la réinitialisation de l'appliance, accédez à l'**Administration Console**, puis cliquez sur **GESTION DE L'APPLIANCE** dans le volet de gauche. Dans la page **Paramètres d'appliance**, le **chemin d'accès à l'espace de stockage des mises à jour** n'est pas remplacé par le chemin d'accès par défaut.

Solution : dans l'**Administration Console**, copiez manuellement le chemin d'accès dans le champ **Espace de stockage de mise à jour par défaut** et collez-le dans le champ **Chemin d'accès à l'espace de stockage des mises à jour**.

La planification de garantie et d'inventaire pour tous les vCenters ne s'applique pas lorsqu'elle est sélectionnée dans la page de file d'attente des tâches

Accédez à **Accueil Dell > Surveiller > File d'attente des tâches > Historique de garantie/d'inventaire > Planifier**. Sélectionnez un vCenter, puis sélectionnez le bouton de modification de planification. Lorsqu'une boîte de dialogue s'affiche, vous pouvez voir une case à cocher en regard du message **Appliquer à tous les vCenters enregistrés**. Lorsque vous sélectionnez la case à cocher et appuyez sur **Appliquer**, le paramètre est appliqué à un vCenter particulier que vous aviez initialement sélectionné, et non pas à tous les vCenters. L'option **Appliquer à tous les vCenters enregistrés** ne s'applique pas en cas de modification de la planification de garantie ou d'inventaire à partir de la page **File d'attente des tâches**.

Résolution : utilisez l'option Modifier la garantie ou l'inventaire depuis la file d'attente des tâches uniquement pour modifier le vCenter sélectionné.

Versions concernées : 2.2 et versions ultérieures

Que faire lorsqu'une erreur de communication Web dans le client Web vCenter s'affiche après la modification des paramètres DNS dans OMIVV ?

Si une erreur de communication Web s'affiche dans le client Web vCenter lors de l'exécution des tâches liées à OMIVV après la modification des paramètres DNS, effectuez l'une des opérations suivantes :

- Effacez le cache du navigateur.
- Fermez la session, puis ouvrez-en une autre dans le client Web.

La page Paramètres ne se charge pas, si je la quitte avant d'y revenir

Pour vSphere v5.5, dans le client Web, si vous quittez la page **Paramètres**, puis y revenez, elle peut ne pas se charger et la zone de sélections continue de s'afficher. Il s'agit d'un problème d'actualisation et la page ne s'actualise pas correctement.

Résolution : cliquez sur l'actualisation globale pour que l'écran s'actualise correctement.

Versions concernées : 2.2 et 3.0

Le message d'erreur « Une tâche ne peut pas être planifiée pour une heure dans le passé » s'affiche dans la page de planification d'inventaire et de garantie de l'Assistant Configuration initiale

Dans le client Web, le message d'erreur « Une tâche ne peut pas être planifiée pour une heure dans le passé » s'affiche :

- si vous sélectionnez « Tous les vCenters enregistrés » dans l'Assistant Configuration initiale et que certains vCenters n'ont aucun hôte.
- lorsque certains vCenters ont des tâches de garantie ou d'inventaire déjà planifiées.
- lorsque certains vCenters n'ont aucune planification d'inventaire ou de garantie définie.

Solution : exécutez à nouveau la configuration de la planification d'inventaire et de garantie séparément à partir de la page **Paramètres** pour les vCenters.

Versions concernées : 2.2 et versions ultérieures

La date d'installation s'affiche sous la forme 12-31-1969 pour certains micrologiciels sur la page du micrologiciel

Dans le client Web, la date d'installation s'affiche sous la forme 12/31/1969 pour certains micrologiciels sur la page du micrologiciel d'un hôte. Si la date d'installation du micrologiciel n'est pas disponible, l'ancienne date s'affiche.

Résolution : Si vous voyez cette ancienne date pour n'importe quel composant du micrologiciel, considérez que la date d'installation n'est pas disponible pour ce dernier.

Versions concernées : 2.2 et versions ultérieures

Une actualisation globale répétée génère une exception dans la fenêtre de tâches récentes.

Si vous essayez d'appuyer sur le bouton d'actualisation de façon répétée, l'interface utilisateur de VMware peut générer une exception.

Résolution : vous pouvez ignorer ce message d'erreur et continuer.

Versions concernées : 2.2 et versions ultérieures

Pourquoi l'interface utilisateur du client Web est-elle déformée dans quelques écrans Dell dans IE 10 ?

Lorsqu'une fenêtre contextuelle s'affiche, il arrive que les données en arrière-plan deviennent blanches et déformées.

Résolution : fermez la boîte de dialogue pour que l'écran redevienne normal.

Versions concernées : 2.2 et versions ultérieures

Je ne vois pas l'icône OpenManage Integration dans le client Web, même si l'enregistrement du plug-in auprès de vCenter a réussi

L'icône OpenManage Integration ne s'affiche pas dans le client Web à moins que les services du client Web vCenter soient redémarrés. Lorsque vous enregistrez l'appliance OpenManage Integration for VMware vCenter, elle est enregistrée auprès du client Web. Si vous annulez l'enregistrement de l'appliance et ensuite enregistrez à nouveau la même version ou enregistrez une nouvelle version de l'appliance, l'enregistrement est effectué correctement, mais l'icône OMIVV peut ne pas s'afficher dans le client Web. Ceci est dû à un problème de cache de VMware. Pour résoudre le problème, assurez-vous que vous redémarrez le service client Web sur le vCenter Server. Ensuite, le plug-in s'affiche dans l'interface utilisateur.

Résolution : redémarrez le service client Web sur le vCenter Server.

Versions concernées : 2.2 et versions ultérieures

La mise à jour du micrologiciel du système 11G montre qu'il n'existe aucun des lots conçus pour une telle mise à jour, même si le référentiel contient les bons lots

Quand l'hôte est ajouté au profil de connexion en mode de verrouillage, l'inventaire démarre, mais échoue en indiquant qu'« aucun contrôleur d'accès à distance n'a été trouvé ou que l'inventaire n'est pas pris en charge sur cet hôte ». L'inventaire est bien censé marcher pour un hôte en mode de verrouillage.

Si vous mettez l'hôte en mode de verrouillage ou retirez un hôte du mode verrouillage, vous devez attendre 30 minutes avant d'effectuer l'opération suivante. Si vous utilisez un hôte 11G pour la mise à jour du micrologiciel, l'assistant de mise à jour du micrologiciel n'affiche aucun lot, même si le référentiel contient les bons lots pour ce système. Ceci se produit parce que l'hôte 11G peut ne pas être configuré pour qu'OMSA envoie des interruptions à OpenManage Integration.

Résolution : assurez-vous que l'hôte est conforme à l'aide de l'assistant de conformité d'hôte du client Web OpenManage Integration. S'il n'est pas conforme, utilisez le correctif de conformité de l'hôte afin de rendre celui-ci conforme.

Versions concernées : 2.2 et versions ultérieures

Pourquoi est-ce que les paramètres de configuration du DNS sont restaurés à leurs valeurs d'origine après le redémarrage de l'appliance lorsque les paramètres de DNS et d'adresse IP de l'appliance sont écrasés par les valeurs DHCP

Il existe un défaut identifié avec lequel les paramètres DNS attribués de manière statique sont remplacées par des valeurs provenant du protocole DHCP. Cela peut se produire lorsque le protocole DHCP est utilisé pour obtenir les paramètres d'adresse IP, et lorsque les valeurs DNS sont attribuées de manière statique. Lorsque le bail DHCP est renouvelé ou lorsque l'appliance est redémarrée, les paramètres DNS attribués de manière statique sont supprimés.

Solution : attribuez statiquement les paramètres d'adresse IP lorsque les paramètres du serveur DNS sont différents de ceux du protocole DHCP.

Versions concernées : Toutes

L'utilisation d'OMIVV pour mettre à jour la carte réseau Intel avec la version 13.5.2 du micrologiciel n'est pas prise en charge

Il existe un problème connu avec les serveurs Dell PowerEdge de 12e génération et certaines cartes réseau Intel dotées de la version micrologicielle 13.5.2. La mise à jour de certains modèles de cartes réseau Intel avec cette version du micrologiciel échoue lorsque la mise à jour du micrologiciel est effectuée en utilisant Lifecycle Controller. Les clients possédant cette version du micrologiciel doivent mettre à jour le logiciel du pilote réseau en utilisant un système d'exploitation. Si la carte réseau Intel possède une version de micrologiciel autre que la version 13.5.2, vous pouvez effectuer la mise à jour à l'aide de l'appliance OMIVV. Pour plus d'informations, reportez-vous à <http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx>

REMARQUE : Remarque : lorsque vous utilisez la mise à jour de micrologiciel un à plusieurs, évitez de sélectionner des cartes réseau Intel de version 13.5.2, car la mise à jour échouera et empêchera la tâche de mise à jour du reste des serveurs.

L'utilisation d'OMIVV pour mettre à jour une carte réseau Intel de la version 14.5 ou 15.0 vers la version 16.x échoue en raison de la préparation exigée par le DUP

Il s'agit d'un problème connu avec NIC 14.5 et 15.0. Assurez-vous que vous utilisez le catalogue personnalisé pour mettre à jour le micrologiciel vers la version 15.5.0 avant de mettre à jour le micrologiciel vers la version 16.x.

Versions concernées : Toutes

Lors d'une tentative de mise à jour du micrologiciel avec un progiciel DUP non valide, l'état de la tâche de mise à jour matérielle sur la console vCenter ne présente ni un échec ni un temps d'attente pendant des heures, même si l'état de la tâche dans LC est ÉCHEC. Pourquoi ?

Lorsque le progiciel DUP non valide est collecté pour la mise à jour du micrologiciel, l'état de la tâche dans la fenêtre de la console vCenter reste « En cours », mais le message est modifié pour motif de panne. Il s'agit d'un bogue de VMware connu qui sera corrigé dans les futures versions de VMware vCenter.

Résolution : la tâche doit être annulée manuellement.

Versions concernées : Toutes

Pourquoi le portail d'administration affiche-t-il un emplacement de référentiel des mises à jour inaccessible ?

Si vous fournissez un chemin inaccessible pour le référentiel des mises à jour, le message d'erreur « Échec : erreur lors de la connexion à l'URL... » s'affiche en haut de la vue Mise à jour de l'appliance. Cependant, le chemin d'accès au référentiel des mises à jour n'est pas remplacé par la valeur antérieure à la mise à jour.

Résolution : passez de cette page à une autre page et assurez-vous que la page est actualisée.

Versions concernées : Toutes

Pourquoi le système n'est pas passé en mode maintenance lorsque j'ai effectué la mise à jour du micrologiciel de un à plusieurs ?

Certaines mises à jour du micrologiciel n'exigent pas le redémarrage de l'hôte. Dans ce cas, la mise à jour du micrologiciel est effectuée sans passer l'hôte en mode de maintenance.

L'intégrité globale du châssis reste en bon état lorsqu'une partie de l'état du bloc d'alimentation passe à l'état critique

L'intégrité globale du châssis concernant le bloc d'alimentation est basée sur les règles de redondance et dépend de la satisfaction des besoins en alimentation du châssis par les PSU qui sont toujours en ligne et fonctionnels. Par conséquent, même si plusieurs PSU sont hors tension, les besoins en alimentation globaux du châssis sont satisfaits. En conséquence, l'intégrité globale du châssis est préservée. Pour en savoir plus sur les blocs d'alimentation et la gestion de l'alimentation, référez-vous au document Guide for Dell PowerEdge M1000e Chassis Management Controller Firmware (Guide d'utilisation du micrologiciel Dell PowerEdge M1000e Chassis Management Controller).

La version du processeur s'affiche comme « Non applicable » dans la vue du processeur de la page de présentation du système

Dans les serveurs Dell PowerEdge de 12e génération et des générations ultérieures, la version du processeur se trouve dans la colonne Marque. Dans les serveurs de génération antérieure, la version du processeur est indiquée dans la colonne Version.

OMIVV prend-il en charge vCenter en mode lié ?

Oui, OMIVV prend en charge jusqu'à 10 serveurs vCenter, que ce soit en mode lié ou non. Pour plus d'informations sur la façon dont OMIVV fonctionne en mode lié, voir le livre blanc OpenManage Integration for VMware vCenter : fonctionnement en mode lié à l'adresse www.dell.com.

Quels sont les paramètres de port requis pour OMIVV ?

REMARQUE : Lors du déploiement de l'agent OMSA à l'aide du lien [Corriger les hôtes vSphere non conformes](#), disponible dans la fenêtre Conformité dans OMIVV, OMIVV démarre le service client http et active le port 8080 sur les versions ultérieures à ESXi 5.5 pour télécharger OMSA VIB et l'installer. Une fois l'installation d'OMSA VIB terminée, le service s'arrête automatiquement et le port se ferme.

Utilisez les paramètres de port suivants pour OMIVV :

Tableau 43. Appliance virtuelle

Numéro de port	Protocoles	Port Type (Type de port)	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
53	DNS	TCP	Aucun	Sortant	Appliance OMIVV vers serveur DNS	Client DNS	Connectivité au serveur DNS ou résolution des noms d'hôte.

Numéro de port	Protocoles	Port Type (Type de port)	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
69	TFTP	UDP	Aucun	Sortant	Appliance OMIV V vers serveur TFTP	Client TFTP	Utilisé pour la mise à jour du micrologiciel sur les serveurs de 11e génération avec un ancien micrologiciel.
80	HTTP	TCP	Aucun	Sortant	Appliance OMIV V 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 OMIV V	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 OMIV V	Agent SNMP (serveur)	Pour recevoir des traps SNMP à partir de nœuds gérés.
443	HTTPS	TCP	128 bits	Entrant	Interface utilisateur OMIV V vers appliance OMIV V	Serveur HTTPS	Services Web offerts par OMIVV. Ces services Web sont consommés par le client Web vCenter et le portail d'administration Dell.
443	WS-MAN	TCP	128 bits	Entrée/Sortie	Appliance OMIV V vers/depuis iDRAC/OMSA	Communication iDRAC/OMSA	Communications iDRAC, OMSA et CMC utilisées pour gérer et surveiller les nœuds gérés.
445	SMB	TCP	128 bits	Sortant	Appliance OMIV V vers CIFS	Communication CIFS	Pour communiquer avec le partage Windows.
4433	HTTPS	TCP	128 bits	Entrant	iDRAC vers appliance OMIV V	Découverte automatique	Serveur de provisionnement utilisé pour la découverte de nœuds gérés.
2049	NFS	UDP/TCP	Aucun	Entrée/Sortie	Appliance OMIV V 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 OMIV V vers NFS	Partage public	Partage public NFS exposé par l'appliance OMIVV vers les nœuds gérés, et utilisé dans la mise à jour du micrologiciel et les flux de déploiement du système d'exploitation.
11620	Agent SNMP	UDP	Aucun	Entrant	iDRAC vers appliance OMIV V	Agent SNMP (serveur)	Communications iDRAC, OMSA et CMC utilisées pour gérer et surveiller les nœuds gérés.
Défini par l'utilisateur	N'importe lequel	UDP/TCP	Aucun	Sortant	Appliance OMIV V vers serveur proxy	Proxy	Pour communiquer avec le serveur proxy

Tableau 44. Nœuds gérés (ESXi)

Numéro de port	Protocoles	Port Type (Type de port)	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
162, 11620	SNMP	UDP	Aucun	Sortant	ESXi vers appliance OMIV V	Événements matériels	Traps SNMP asynchrones envoyés à partir d'ESXi. Ce port doit s'ouvrir à partir d'ESXi.
443	WS-MAN	TCP	128 bits	Entrant	Appliance OMIV V vers ESXi (OMSA)	Communication iDRAC/OMSA	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.
443	HTTPS	TCP	128 bits	Entrant	Appliance OMIV V vers ESXi	Serveur HTTPS	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.
8080	HTTP	TCP	128 bits	Sortant	ESXi vers appliance OMIV V	Serveur HTTP ; télécharge OMSA VIB et répare les hôtes vSphere non conformes	Aide ESXi à télécharger l'OMSA/le pilote VIB.

Tableau 45. Nœuds gérés (iDRAC/CMC)

Numéro de port	Protocoles	Port Type (Type de port)	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
443	WSMAN /HTTPS	TCP	128 bits	Entrant	Appliance OMIV V vers iDRAC/CMC	Communication iDRAC	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir de l'iDRAC et du CMC.
4433	HTTPS	TCP	128 bits	Sortant	iDRAC vers appliance OMIV V	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 OMIV V	Partage public	Pour que l'iDRAC accède au partage public NFS qui est exposé par l'appliance OMIV V. 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'OMIV V. Utilisé dans le flux de déploiement.
4001 à 4004	NFS	UDP	Aucun	Entrée/Sortie	iDRAC vers/ depuis OMIV V	Partage public	Pour que l'iDRAC accède au partage public NFS qui est exposé par l'appliance OMIV V. 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'OMIV V. Utilisé dans le flux de déploiement.
69	TFTP	UDP	128 bits	Entrée/Sortie	iDRAC vers/ depuis OMIV V	Protocole simplifié de transfert de fichiers	Utilisé afin de gérer l'iDRAC avec succès à partir de la station de gestion.

Le mot de passe utilisé pour la découverte sans système d'exploitation ne change pas pour l'utilisateur après l'application réussie du profil matériel ou du profil système comportant le même utilisateur doté de nouvelles données d'identification modifiées dans la liste d'utilisateurs d'iDRAC

Le mot de passe utilisateur utilisé à la détection n'est pas actualisé avec les nouvelles informations d'identification si seul le modèle de profil matériel ou de profil système est sélectionné pour le déploiement. C'est intentionnel pour que le plug-in soit en mesure de communiquer avec l'iDRAC pour une utilisation ultérieure lors de déploiements.

Impossible d'afficher les détails des nouvelles versions de l'iDRAC répertoriés dans la page des hôtes et des clusters vCenter

Résolution : après l'achèvement avec succès d'une tâche de mise à jour du micrologiciel dans le client Web vSphere, actualisez la page **Mise à jour du micrologiciel** et vérifiez les versions de ce dernier. Si la page affiche les anciennes versions, accédez à la page **Conformité des hôtes** dans OpenManage Integration for VMware vCenter, et vérifiez l'état CSIOR de cet hôte. Si l'option CSIOR n'est pas activée, activez-la et redémarrez l'hôte. Si l'option CSIOR est déjà activée, connectez-vous à la console iDRAC, réinitialisez la console, attendez quelques minutes, puis actualisez la page **Mise à jour du micrologiciel**.

Comment puis-je tester les paramètres d'événements en utilisant OMSA pour simuler un défaut matériel de température ?

Pour vous assurer que les événements fonctionnent correctement, effectuez les étapes suivantes :

1. Dans l'interface utilisateur de l'OMSA, accédez à **Gestion des alertes > Événements de la plate-forme**.
2. Cochez la case **Activer les alertes du filtre d'événements de la plate-forme**.
3. Faites défiler vers le bas, puis cliquez sur **Appliquer les modifications**.
4. Pour vous assurer qu'un événement spécifique est activé, par exemple l'avertissement de température, à partir de l'arborescence à gauche, sélectionnez **Châssis principal du système**.
5. Sous **Châssis principal du système**, sélectionnez **Températures**.
6. Sélectionnez l'onglet **Gestion des alertes** et sélectionnez **Avertissement de capteur de température**.
7. Sélectionnez la case **Diffuser un message** et sélectionnez **Appliquer les modifications**.
8. Pour provoquer l'événement d'avertissement de la température, à partir de l'arborescence à gauche, sélectionnez **Châssis principal du système**.
9. Sélectionnez **Températures** sous **Châssis principal du système**.
10. Sélectionnez le lien **Température ambiante de la carte système**, et sélectionnez l'option **Définir les valeurs**.
11. Définissez le **Seuil maximal d'avertissement** sur une valeur précédant la valeur de lecture en cours affichée. Par exemple, si la valeur de lecture en cours est égale à 27, définissez le seuil sur **25**.
12. Sélectionnez **Appliquer les changements**, et l'événement d'avertissement de température est généré.

Pour provoquer un autre événement, restaurez les paramètres d'origine en utilisant la même option **Définir les valeurs**. Les événements sont générés comme des avertissements, puis reviennent à un état normal. Si tout fonctionne correctement, accédez à la vue **Tâches et Événements de vCenter** ; un événement d'avertissement de capteur de température doit être affiché.

REMARQUE : Il existe un filtre pour les événements en double ; si vous essayez de déclencher le même événement trop de fois consécutivement, vous ne recevrez qu'un seul événement. Attendez au moins 30 secondes entre les événements pour voir tous les événements.

Bien que l'agent OMSA soit installé sur le système hôte OMIVV, je reçois un message d'erreur indiquant qu'OMSA n'est pas installé.

Pour résoudre ce problème sur un serveur de 11e génération :

1. Installez **OMSA** avec le composant **Activation à distance** sur le système hôte.
2. Si vous utilisez l'invite de commandes pour installer OMSA, assurez-vous que vous spécifiez l'**option -c**. Si OMSA est déjà installé, réinstallez-le avec l'option -c et redémarrez le service :

```
srvadmin-install.sh -c  
srvadmin-services.sh restart
```

Pour un hôte ESXi, assurez-vous d'installer **OMSA VIB** à l'aide de l'outil **VMware Remote CLI**, et redémarrez le système.

OMIVV peut-il prendre en charge l'ESXi avec le mode de verrouillage activé ?

Oui, le mode de verrouillage est pris en charge dans la présente version sur les hôtes ESXi version 5.0 et les versions ultérieures.

Quand j'essaie d'utiliser le mode de verrouillage, celui-ci échoue.

Quand j'ai ajouté un hôte au profil de connexion en mode de verrouillage, l'inventaire a démarré, mais a échoué en indiquant qu'« aucun contrôleur d'accès à distance n'a été trouvé ou que l'inventaire n'est pas pris en charge sur cet hôte ».

Si vous mettez l'hôte en mode de verrouillage ou si vous retirez un hôte du mode verrouillage, vous devez attendre 30 minutes avant d'effectuer la prochaine opération dans OMIVV.

La création du profil matériel échoue si j'utilise un serveur de référence

Assurez-vous que les versions minimales recommandées du micrologiciel iDRAC, du micrologiciel Lifecycle Controller et du BIOS sont installées.

Pour vous assurer que les données récupérées à partir du serveur de référence sont à jour, activez **Collecter l'inventaire du système au redémarrage (CSIOR)** et redémarrez le serveur de référence avant l'extraction des données.

Les tentatives de déploiement d'ESXi sur un serveur échouent

1. Assurez-vous que l'**emplacement ISO (chemin NFS)** et les **chemins de dossiers** de préparation sont exacts.
2. Assurez-vous que la **carte réseau** sélectionnée lors de l'attribution de l'identité du serveur est sur le même réseau que l'appliance virtuelle.
3. Si vous utilisez une **adresse IP statique**, assurez-vous que les informations réseau fournies (y compris le masque de sous-réseau et la passerelle par défaut) sont exactes. En outre, assurez-vous que l'adresse IP n'est pas déjà attribuée sur le réseau.
4. Assurez-vous qu'au moins un **disque virtuel** est détecté par le système.
ESXi s'installe également sur une carte SD interne.

Échec des déploiements d'hyperviseur sur les machines Dell PowerEdge R210 II

Un problème d'expiration du délai sur les systèmes Dell PowerEdge R210 II produit une erreur d'échec de déploiement d'hyperviseur en raison de l'échec du démarrage du BIOS depuis un ISO relié.

Résolution : installez manuellement l'hyperviseur sur la machine.

Les systèmes détectés automatiquement s'affichent sans information de modèle dans l'assistant Déploiement

Cela indique généralement que la version du micrologiciel installé sur le système ne satisfait pas à la configuration minimale requise. Parfois, une mise à jour du micrologiciel n'a pas été enregistrée sur le système.

Résolution : le démarrage à froid du système ou la réinstallation de la lame résout ce problème. Le compte nouvellement activé sur l'iDRAC doit être désactivé, et la découverte automatique doit être relancée pour fournir les informations de modèle et de carte réseau à OMIVV.

Le partage NFS est configuré avec l'ISO ESXi, mais le déploiement échoue avec des erreurs de montage de l'emplacement du partage

Pour trouver la solution :

1. Assurez-vous que l'iDRAC est en mesure d'envoyer un ping à l'appliance.
2. Assurez-vous que votre réseau n'est pas trop lent.
3. Assurez-vous que les ports : 2049, 4001 - 4004 sont ouverts et que le pare-feu est défini en conséquence.

Comment puis-je forcer la suppression de l'appliance virtuelle de vCenter

1. Allez à **Https://<vcenter_serverIPAddress>/mob**
2. Entrez les informations d'identification de l'administrateur vCenter VMware.
3. Cliquez sur **Contenu**.
4. Cliquez sur **Gestionnaire d'extension**.
5. Cliquez sur **Désenregistrer l'extension**.
6. Entrez la clé d'extension pour désenregistrer `com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient`, puis cliquez sur **Appeler une méthode**.
7. Dans le client Web vSphere, mettez hors tension l'appliance OMIVV puis supprimez-la. La touche de désenregistrement doit être destinée au client Web.

La saisie d'un mot de passe sur l'écran Backup Now (Sauvegarder maintenant) produit un message d'erreur

Si vous utilisez un écran basse résolution, le champ Mot de passe de cryptage ne sera pas visible depuis la fenêtre SAUVEGARDER MAINTENANT. Vous devez faire défiler la page vers le bas pour entrer le mot de passe de cryptage.

Dans le client Web vSphere, si vous cliquez sur le portlet Dell Server Management ou sur l'icône Dell, l'erreur 404 est retournée.

Vérifiez si l'appliance OMIVV est en cours d'exécution ; si ce n'est pas le cas, redémarrez-la à partir du client vSphere. Attendez quelques minutes pour que le service Web de l'appliance virtuelle démarre, puis actualisez la page. Si l'erreur persiste, essayez d'envoyer un ping à l'appliance à l'aide de l'adresse IP ou d'un nom de domaine complet à partir d'une ligne de commande. Si le ping ne marche pas, vérifiez vos paramètres réseau pour vous assurer qu'ils sont corrects.

Que dois-je faire en cas d'échec d'une mise à jour de micrologiciel ?

Vérifiez les fichiers log de l'appliance virtuelle pour voir si les tâches ont expiré. Si c'est le cas, vous devez réinitialiser iDRAC en effectuant un redémarrage à froid. Une fois le système en cours de fonctionnement, vérifiez si la mise à jour a réussi en exécutant un inventaire ou à l'aide de l'onglet **Micrologiciel**.

Que dois-je faire en cas d'échec de l'enregistrement de vCenter ?

L'enregistrement de vCenter peut échouer en raison de problèmes de communication. Par conséquent, si vous rencontrez ces problèmes, une solution consiste à utiliser une adresse IP statique. Pour utiliser une adresse IP statique, sous l'onglet Console d'OpenManage Integration for VMware vCenter, sélectionnez **Configurer le réseau > Modifier les périphériques** et saisissez la **passerelle** et le **nom de domaine complet** (FQDN) appropriés. Saisissez le nom du serveur DNS sous Modifier la configuration DNS.

 **REMARQUE** : Assurez-vous que l'appliance virtuelle peut trouver le serveur DNS que vous avez entré.

Performances au cours de la lecture des informations d'identification du test de profil de connexion ralenties ou absence de réponse

L'iDRAC sur un serveur ne dispose que d'un seul utilisateur (*root* uniquement, par exemple) et l'état de l'utilisateur est défini sur désactivé, ou l'état de tous les utilisateurs est défini sur désactivé. La communication avec un serveur dont l'état est défini sur désactivé est ralentie. Pour résoudre ce problème, vous pouvez corriger l'état désactivé du serveur ou réinitialiser l'iDRAC sur le serveur pour réactiver les paramètres par défaut de l'utilisateur *root*.

Pour corriger un serveur se trouvant dans un état désactivé :

1. Ouvrez la console Chassis Management Controller et sélectionnez le serveur désactivé.
2. Pour ouvrir automatiquement la console iDRAC, cliquez sur **Lancer l'interface utilisateur iDRAC**.
3. Accédez à la liste des utilisateurs dans la console iDRAC et choisissez l'une des options suivantes :
 - iDRAC6 : sélectionnez **Paramètres de l'iDRAC > Onglet Réseau/Sécurité > Onglet Utilisateurs**.
 - iDRAC7 : sélectionnez **Paramètres de l'iDRAC > Onglet Utilisateurs**.
 - iDRAC8 : sélectionnez **Paramètres de l'iDRAC > Onglet Utilisateurs**.
4. Pour modifier les paramètres, dans la colonne ID d'utilisateur, cliquez sur le lien correspondant à l'utilisateur admin (*root*).
5. Cliquez sur **Configurer l'utilisateur**, puis cliquez sur **Suivant**.
6. Sur la page **Configuration de l'utilisateur** de l'utilisateur sélectionné, cochez la case située à côté de l'option Activer l'utilisateur, puis cliquez sur **Appliquer**.

Est-ce qu'OMIVV prend en charge l'appliance VMware vCenter Server ?

Oui, OMIVV prend en charge l'appliance VMware vCenter Server depuis la version 2.1.

Le niveau de micrologiciel n'est pas à jour lorsque j'ai effectué la mise à jour du micrologiciel à l'aide de l'option Appliquer au redémarrage suivant et que le système a été redémarré

Pour mettre à jour le micrologiciel, exécutez l'inventaire sur l'hôte dès que le redémarrage est terminé. Parfois, lorsque l'événement de redémarrage n'atteint pas l'appliance, l'inventaire n'est pas automatiquement déclenché. Dans ce type de situation, vous devez exécuter de nouveau l'inventaire manuellement pour obtenir les versions mises à jour du micrologiciel.

L'hôte s'affiche sous le châssis, même après la suppression de l'hôte de l'arborescence de vCenter

Les hôtes situés sous le châssis sont identifiés dans le cadre de l'inventaire du châssis. Après une opération réussie d'inventaire du châssis, la liste des hôtes sous le châssis est mise à jour. Par conséquent, même si l'hôte est supprimé de l'arborescence de vCenter, l'hôte est affiché sous le châssis jusqu'à ce que l'inventaire suivant du châssis soit exécuté.

Dans l'Administration Console, le chemin d'accès vers l'espace de stockage des mises à jour est défini sur la valeur par défaut après que j'ai rétabli les paramètres d'usine

Après la réinitialisation de l'appliance, accédez à l'**Administration Console**, puis cliquez sur **GESTION DE L'APPLIANCE** dans le volet de gauche. Dans la page **Paramètres d'appliance**, le **chemin d'accès à l'espace de stockage des mises à jour** n'est pas remplacé par le chemin d'accès par défaut.

Solution : dans l'**Administration Console**, copiez manuellement le chemin d'accès dans le champ **Espace de stockage de mise à jour par défaut** et collez-le dans le champ **Chemin d'accès à l'espace de stockage des mises à jour**.

Après la sauvegarde et la restauration d'OMIVV, les paramètres de l'alarme ne sont pas restaurés

La restauration de la sauvegarde de l'appliance OMIVV ne restaure pas tous les paramètres d'alarmes. Cependant, dans la GUI d'OpenManage Integration for VMware, le champ **Alarmes et événements** affiche les paramètres restaurés.

Résolution : dans la GUI d'OpenManage Integration for VMware, dans l'onglet **Gérer > Paramètres**, modifiez manuellement les paramètres **Événements et alarmes**.

Échec du déploiement de l'hyperviseur lorsqu'un NPAR est activé sur un nœud cible et désactivé sur le profil système

Le déploiement de l'hyperviseur échoue lorsqu'un profil système avec un partitionnement de carte réseau (NPAR) désactivé est appliqué sur une machine cible. Ici, NPAR est activé sur le nœud cible et un seul des NIC partitionnés, à l'exception la partition 1, est sélectionné en tant que carte réseau (NIC) pour les tâches de gestion au cours du processus de déploiement via l'Assistant Déploiement.

Résolution : si vous modifiez l'état NPAR via le profil système lors du déploiement, assurez-vous de sélectionner uniquement la première partition pour le réseau de gestion dans l'Assistant de déploiement.

Version concernée : 4.1

La version disponible de l'appliance virtuelle affiche des informations erronées lorsque la version disponible est inférieure à la version actuelle

Dans la console d'administration OMIVV, dans **Gestion de l'appliance**, **Version de l'appliance virtuelle disponible** affiche les modes RPM et OVF comme étant disponibles.

 **REMARQUE** : Il est recommandé de configurer le chemin d'accès vers la logithèque des mises à jour sur la dernière version et de ne pas prendre en charge la rétrogradation de la version de l'appliance virtuelle.

L'exception 267027 est générée lors de l'ajout d'un serveur sans système d'exploitation de 12e génération avec une licence Express

Pendant la découverte sans système d'exploitation, si une information d'identification incorrecte est saisie, le compte utilisateur est verrouillé automatiquement pendant quelques minutes. Au cours de cette période, iDRAC ne répond plus et prend quelques minutes avant de fonctionner normalement.

Résolution : attendez quelques minutes et saisissez de nouveau les informations d'identification utilisateur.

Lors du déploiement du système d'exploitation sur les serveurs de 14e génération, l'application du profil matériel échoue en raison d'une erreur iDRAC

Au cours du déploiement du système d'exploitation sur les serveurs de 14e génération, une tâche de mise à jour de la configuration est créée dans iDRAC lorsque le profil matériel est appliqué. Cependant, la tâche échoue parfois et affiche un message indiquant qu'une tâche de configuration est déjà créée.

Résolution : pour effacer les entrées obsolètes et réessayer de déployer le système d'exploitation, exécutez la commande `racadm jobqueue delete -i JID_CLEARALL_FORCE`.

La mise à niveau RPM OMIVV échoue si le proxy est configuré avec une authentification d'utilisateur de domaine

Si l'appliance OMIVV est configurée avec le proxy pour accéder à Internet et si le proxy est authentifié à l'aide de l'authentification NTLM, la mise à jour RPM échoue en raison des problèmes présents dans l'outil yum sous-jacent.

Versions concernées : OMIVV 4.0 et ultérieures

Résolution/solution : procédez à une sauvegarde et à une restauration pour mettre à jour l'appliance OMIVV.

Impossible d'appliquer un profil système si la carte PCIe est dans le châssis FX

Le déploiement du système d'exploitation échoue sur un serveur cible si le serveur source a des informations sur la carte PCIe lors de l'utilisation d'un châssis FX. Les profils système sur le serveur source ont un `fc.chassislot` ID différent de celui présent sur le

serveur cible. OMIVV tente de déployer le même `fc.chassislot ID` sur le serveur cible mais échoue. Les profils système recherchent une instance exacte (FQDD) lors de l'application du profil, ce qui fonctionne avec succès sur les serveurs rack (identiques), mais peut avoir quelques restrictions sur les serveurs modulaires. Par exemple, dans FC640, les profils système créés à partir d'un serveur modulaire ne peuvent pas être appliqués sur d'autres serveurs modulaires dans le même châssis FX en raison de restrictions au niveau de la carte réseau.

Versions concernées : 4.1 et versions ultérieures

Résolution : un profil système provenant d'un serveur FC640 dans l'emplacement 1 d'un châssis FX2s peut uniquement être appliqué sur un autre serveur FC640 résidant dans l'emplacement 1 d'un autre châssis FX2s.

Problèmes de déploiement de serveurs sans système d'exploitation

Cette section traite des problèmes rencontrés au cours du processus de déploiement.

Conditions préalables à la détection automatique et l'établissement de liaisons

- Avant de lancer la détection automatique et l'établissement de liaisons, assurez-vous que les versions du micrologiciel iDRAC et Lifecycle Controller et du BIOS répondent aux recommandations minimales.
- La tâche CSIOR doit avoir été exécutée au moins une fois sur le système ou iDRAC.

Problème de configuration matérielle

- Avant de lancer une tâche de déploiement, assurez-vous que le système a terminé la tâche CSIOR et n'est pas en cours de redémarrage.
- La configuration du BIOS doit de préférence être exécutée en mode Clone, afin que le serveur de référence soit un système identique.
- Certains contrôleurs ne permettent pas la création d'une matrice RAID 0 avec un seul lecteur. Cette fonctionnalité est prise en charge uniquement sur les contrôleurs haut de gamme, et l'application d'un tel profil matériel peut causer des problèmes.

Activation de la découverte automatique sur un système acheté récemment

La fonction de découverte automatique d'un système hôte n'est pas activée par défaut : l'activation doit être demandée au moment de l'achat. Si l'activation de la découverte automatique est demandée au moment de l'achat, DHCP est activé sur l'iDRAC et les comptes Administrateur sont désactivés. Il n'est pas nécessaire de configurer une adresse IP statique pour l'iDRAC. Il en obtient une à partir d'un serveur DHCP sur le réseau. Pour utiliser la fonction de découverte automatique, un serveur DHCP ou un serveur DNS (ou les deux) doit être configuré pour prendre en charge le processus de détection. CSIOR doit déjà avoir été exécuté pendant le processus d'usine.

Si la découverte automatique n'a pas été demandée au moment de l'achat, elle peut être activée en procédant comme suit :

1. Au cours de la procédure d'amorçage, appuyez sur **Ctrl+E**.
2. Dans la fenêtre de configuration iDRAC, activez la carte réseau (serveurs lames uniquement).
3. Activez Auto-Discovery (Découverte automatique).
4. Activez DHCP.
5. Désactivez les comptes admin.
6. Activez **Obtention de l'adresse du serveur DNS via DHCP**.
7. Activez **Obtention du nom de domaine DNS via DHCP**.
8. Dans le champ **Serveur de provisionnement**, entrez :

```
<OpenManage Integration virtual appliance IPAddress>:4433
```

Documentation connexe

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

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

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

Sujets :

- [Accès aux documents à partir du site de support Dell EMC](#)

Accès aux documents à partir du site de support Dell EMC

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

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

Attributs spécifiques au système

iDRAC

Tableau 46. Attributs spécifiques au système iDRAC

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
Nom du RAC DNS	Nom du RAC DNS	Informations NIC
DataCenterName	Nom du centre de données	Topologie de serveurs
Nom de l'allée	Nom de l'allée	Topologie de serveurs
Nom du rack	Nom du rack	Topologie de serveurs
Logement de rack	Logement de rack	Topologie de serveurs
RacName	Nom RAC Active Directory	Active Directory
DNSDomainName	Nom de domaine DNS	Informations statiques sur le certificat NIC
Adresse :	Adresse IPv4	Informations statiques sur IPv4
Masque réseau	Masque réseau	Informations statiques sur IPv4
Passerelle	Passerelle	Informations statiques sur IPv4
DNS1	Serveur DNS 1	Informations statiques sur IPv4
DNS2	Serveur DNS 2	Informations statiques sur IPv4
Adresse 1	Adresse IPv6 1	Informations statiques sur IPv6
Passerelle	Passerelle IPv6	Informations statiques sur IPv6
Longueur du préfixe	Longueur de préfixe local de liaison IPv6	Informations statiques sur IPv6
DNS1	Serveur DNS IPV6 1	Informations statiques sur IPv6
DNS2	Serveur DNS IPV6 2	Informations statiques sur IPv6
DNSFromDHCP6	Serveur DNS à partir de DHCP6	Informations statiques sur IPv6
HostName	Nom d'hôte du serveur	Système d'exploitation du serveur
RoomName	RoomName	Topologie de serveurs
NodeID	ID du nœud système	Informations sur le serveur

BIOS

Tableau 47. Attributs spécifiques au système pour le BIOS

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
AssetTag	Asset Tag	Miscellaneous Settings (Paramètres divers)
IscsiDev1Con1Gateway	Passerelle de l'initiateur	Paramètres de la connexion 1
IscsiDev1Con1Ip	Adresse de l'initiateur IP	Paramètres de la connexion 1
IscsiDev1Con1Mask	Masque de sous-réseau de l'initiateur	Paramètres de la connexion 1
IscsiDev1Con1TargetIp	Adresse IP cible	Paramètres de la connexion 1
IscsiDev1Con1TargetName	Nom de la cible	Paramètres de la connexion 1

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
IscsiDev1Con2Gateway	Passerelle de l'initiateur	Paramètres de la connexion 1
IscsiDev1Con2Ip	Adresse de l'initiateur IP	Paramètres de la connexion 1
IscsiDev1Con2Mask	Masque de sous-réseau de l'initiateur	Paramètres de la connexion 1
IscsiDev1Con2TargetIp	Adresse IP cible	Paramètres de la connexion 1
IscsiDev1Con2TargetName	Nom de la cible	Paramètres de la connexion 1
iscsilInitiatorName	Nom de l'initiateur iSCSI	Paramètres réseau
Ndc1PcieLink1	Carte réseau intégrée 1 liaison PCIe Link1	Integrated Devices (Périphériques intégrés)
Ndc1PcieLink2	Carte réseau intégrée 1 liaison PCIe Link2	Integrated Devices (Périphériques intégrés)
Ndc1PcieLink3	Carte réseau intégrée 1 liaison PCIe Link3	Integrated Devices (Périphériques intégrés)
UefiBootSeq	Séquence de démarrage d'UEFI	UEFI Boot Settings (Paramètres de démarrage d'UEFI)

RAID

Tableau 48. Attributs spécifiques au système pour RAID

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
Mode de configuration demandée de l'enceinte	S/O	S/O
Mode de configuration actuelle de l'enceinte	S/O	S/O

CNA

Tableau 49. Attributs spécifiques au système pour CNA

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
ChapMutualAuth	Authentification mutuelle CHAP	Paramètres généraux iSCSI
ConnectFirstTgt	Se connecter	Paramètres de la première cible iSCSI
ConnectSecondTgt	Se connecter	Paramètres de la deuxième cible iSCSI
FirstFCoEBootTargetLUN	Numéro d'unité logique d'amorçage	Configuration de la carte FCoE
FirstFCoEWWPNTarget	Nom du port universel cible	Configuration de la carte FCoE
FirstTgtBootLun	Numéro d'unité logique d'amorçage	Paramètres de la première cible iSCSI
FirstTgtChapId	ID CHAP	Paramètres de la première cible iSCSI
FirstTgtChapPwd	Secret CHAP	Paramètres de la première cible iSCSI
FirstTgtIpAddress	Adresse IP	Paramètres de la première cible iSCSI
FirstTgtIscsiName	Nom iSCSI	Paramètres de la première cible iSCSI
FirstTgtTcpPort	Port TCP	Paramètres de la première cible iSCSI
Configuration automatique de l'IP	IpAutoConfig	Paramètres généraux iSCSI
IscsilInitiatorChapId	ID CHAP	Paramètres de l'initiateur iSCSI
IscsilInitiatorChapPwd	Secret CHAP	Paramètres de l'initiateur iSCSI
IscsilInitiatorGateway	Passerelle par défaut	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpAddr	Adresse IP	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv4Addr	Adresse IPv4	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv4Gateway	Passerelle IPv4 par défaut	Paramètres de l'initiateur iSCSI

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
IscsilInitiatorIpv4PrimDns	DNS principal IPv4	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv4SecDns	DNS secondaire IPv4	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv6Addr	Adresse IPv6	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv6Gateway	Passerelle IPv6 par défaut	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv6PrimDns	DNS principal IPv6	Paramètres de l'initiateur iSCSI
IscsilInitiatorIpv6SecDns	DNS secondaire IPv6	Paramètres de l'initiateur iSCSI
iscsilInitiatorName	Nom iSCSI	Paramètres de l'initiateur iSCSI
IscsilInitiatorPrimDns	DNS principal	Paramètres de l'initiateur iSCSI
IscsilInitiatorSecDns	DNS secondaire	Paramètres de l'initiateur iSCSI
IscsilInitiatorSubnet	Masque de sous-réseau	Paramètres de l'initiateur iSCSI
IscsilInitiatorSubnetPrefix	Préfixe du masque de sous-réseau	Paramètres de l'initiateur iSCSI
SecondaryDeviceMacAddr	Adresse MAC du périphérique secondaire	Paramètres du périphérique iSCSI secondaire
SecondTgtBootLun	Numéro d'unité logique d'amorçage	Paramètres de la deuxième cible iSCSI
SecondTgtChapPwd	Secret CHAP	Paramètres de la deuxième cible iSCSI
SecondTgtIpAddress	Adresse IP	Paramètres de la deuxième cible iSCSI
SecondTgtIscsiName	Nom iSCSI	Paramètres de la deuxième cible iSCSI
SecondTgtTcpPort	Port TCP	Paramètres de la deuxième cible iSCSI
UseIndTgtName	Utiliser un nom de cible indépendant	Paramètres du périphérique iSCSI secondaire
UseIndTgtPortal	Utiliser un portail cible indépendant	Paramètres du périphérique iSCSI secondaire
VirtFIPMacAddr	Adresse MAC FIP virtuelle	Page principale de configuration
VirtIscsiMacAddr	Adresse MAC du déchargement iSCSI virtuel	Page principale de configuration
VirtMacAddr	Adresse MAC virtuelle	Page principale de configuration
VirtMacAddr[Partition:n]	Adresse MAC virtuelle	Configuration n Partition
VirtWWN	Nom du nœud universel virtuel	Page principale de configuration
VirtWWN[Partition:n]	Nom du nœud universel virtuel	Configuration n Partition
VirtWWPN	Nom du port universel virtuel	Page principale de configuration
VirtWWPN[Partition:n]	Nom du port universel virtuel	Configuration n Partition
Nom du nœud universel	WWN	Page principale de configuration
Nom du nœud universel	WWN[Partition:n]	Configuration n Partition

FC

Tableau 50. Attributs spécifiques au système pour FC

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
VirtualWWN	Nom du nœud universel virtuel	Page Configuration du port
VirtualWWPN	Nom du port universel virtuel	Page Configuration du port

Attributs de personnalisation

Tableau 51. Attributs de personnalisation

FQDD	Attributs	Personnalisation OMIVV
BIOS	Virtualization Technology	Toujours activée
iDRAC	Collecte de l'inventaire système au redémarrage	Toujours activée
RAID	IncludedPhysicalDiskID	Si la valeur d'IncludedPhysicalDiskID est Sélection automatique, alors nous supprimons cette valeur
RAID	RAIDPState	Retiré
iDRAC	Mot de passe utilisateur Mot de passe	Seuls les utilisateurs ayant iDRAC activé auront le lien « mot de passe » pour saisir le mot de passe.

Informations supplémentaires

Les livres blancs techniques Dell suivants, disponibles à l'adresse **delltechcenter.com**, fournissent plus d'informations sur le modèle de configuration du profil système, les attributs et les flux de travail :

- *Clonage de serveur avec des profils de configuration du serveur*
- *Fichier XML de configuration de serveur*
- *Flux de travail XML de configuration*
- *Scripts de Flux de travail XML de configuration 133*
- *Fichiers exemples de configuration XML*

Matrice de comparaison de la version du composant avec la version de ligne de base

Tableau 52. Matrice de comparaison de la version du composant avec la version de ligne de base

Type de dérive				
Matériel	Ligne de base associée	Composant cible	Scénario	État de conformité
	Disponible	Disponible	Le composant matériel correspond à la ligne de base associée.	Conforme
	Disponible	Disponible	Le composant matériel ne correspond pas à la ligne de base associée.	Non conforme
	Non disponible	Disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme
	Disponible	Non disponible	La version du composant matériel est disponible dans la ligne de base associée, mais le composant ou l'attribut n'est pas disponible.	Non conforme
	Non disponible	Non disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme
Micrologiciel	Ligne de base associée	Composant cible	Scénario	État de conformité
	Disponible	Disponible	Le composant de micrologiciel correspond à la ligne de base associée.	Conforme
	Disponible	Disponible	Le composant de micrologiciel ne correspond pas à la ligne de base associée.	Non conforme
	Disponible	Non disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme
	Non disponible	Non disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme
Pilote	Ligne de base associée	Composant cible	Scénario	État de conformité
	Disponible	Disponible	Le composant de pilote correspond à la ligne de base associée.	Conforme
	Disponible	Disponible	Le composant de pilote ne correspond pas à la ligne de base associée.	Non conforme
	Non disponible	Disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme
	Disponible	Non disponible	La version du composant de pilote est disponible dans la ligne de base associée, mais le composant ou	Non conforme

			l'attribut n'est pas disponible ou un nouveau composant est disponible.	
	Non disponible	Non disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme