OpenManage Integration for VMware vCenter version 5.2

Guide de l'utilisateur

October 2020
Rév. A00

Remarques, précautions et avertissements

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

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

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

Table des matières

Chapitre 1: Introduction..... 10
Nouveautés de cette version.....10
Fonctions OpenManage Integration for VMware vCenter.....10

Chapitre 2: Connexion à la console d'administration OMIVV Dell EMC..... 13
Enregistrement d'un nouveau serveur vCenter.....13
Enregistrement d'un serveur vCenter à l'aide d'un compte non-administrateur.....14
Privilèges requis pour les utilisateurs non administrateurs.....15
Attribution de privilèges Dell à un rôle existant.....16
Mise à jour des certificats des serveurs vCenter inscrits.....16
Modification des informations d'identification pour la connexion à vCenter.....16
Annulation de l'enregistrement de Dell OpenManage Integration for VMware vCenter.....17
Chargement d'une licence sur la Console Administration OMIVV..... 17
Gestion de l'appliance OMIVV.....17
Configuration des alertes globales.....25
À propos de la console de machine virtuelle OMIVV.....26

Chapitre 3: Suivi des hôtes et des châssis à l'aide du tableau de bord..... 36

Chapitre 4: Gestion des hôtes à l'aide du profil d'identification d'hôte.....39
Profil d'identification d'hôte.....39
Création du profil d'identification d'hôte.....39
Modification du profil d'identification d'hôte..... 40
Affichage du profil d'identification d'hôte..... 42
Test du profil d'identification d'hôte..... 42
Suppression d'un profil d'identification d'hôte.....42

Chapitre 5: Gestion des châssis à l'aide d'un profil d'identification de châssis.....44
Profil d'identification de châssis..... 44
Création d'un profil d'identification de châssis..... 44
Modification d'un profil d'identification de châssis..... 45
Affichage du profil d'identification de châssis..... 46
Test d'un profil d'identification de châssis..... 46
Suppression d'un profil d'identification de châssis.....46

Chapitre 6: Gestion des logithèques de micrologiciels et de pilotes à l'aide du profil de logithèque.....48
Profil de logithèque.....48
Création d'un profil de logithèque..... 48
Modification d'un profil de logithèque.....49
Modification ou personnalisation du catalogue Dell par défaut..... 50
Modification d'un catalogue de piles MX validé.....50
Synchronisation avec l'emplacement de la logithèque..... 50
Affichage d'un profil de logithèque..... 50
Suppression d'un profil de logithèque.....51

Chapitre 7: Capture de la configuration de base à l'aide d'un profil de cluster....52
Profil de cluster....52
Création d'un profil de cluster....52
Modification d'un profil de cluster....53
Affichage d'un profil de cluster....53
Mise à jour d'un profil de cluster....54
Suppression d'un profil de cluster....54

Chapitre 8: Gestion des serveurs sur matériel vierge....55
Affichage des serveurs sur matériel vierge....55
Détection de périphériques....55
Découverte automatique....56
Conditions préalables à la détection automatique....56
Activation ou désactivation de comptes administratifs dans iDRAC....56
Configuration manuelle des serveurs PowerEdge en vue d'une découverte automatique....57
Découverte manuelle des serveurs sur matériel vierge....57
Suppression d'un serveur sur matériel vierge....58
Actualisation des serveurs sur matériel vierge....58
Achat ou renouvèlement de la licence d'iDRAC....59

Chapitre 9: Gestion des profils de déploiement....60
Profil système....60
Création d'un profil système....60
Modification du profil système....62
Afficher un profil système....63
Suppression d'un profil système....63
Profil ISO....63
Création d'un profil ISO....63
Modification d'un profil ISO....63
Affichage d'un profil ISO....64
Suppression d'un profil ISO....64
Téléchargement des images ISO Dell EMC personnalisées....64

Chapitre 10: Déploiement de profil système et de profil ISO....65
Check-list de déploiement....65
Déploiement d'un profil système (configuration du matériel)....66
Déploiement d'un profil ISO (installation ESXi)....67
Déploiement du profil système et du profil ISO....68
Prise en charge de la technologie VLAN....69
Synchronisation de la tâche de déploiement....69

Chapitre 11: Conformité....71
Gestion de la conformité....71
Affichage des hôtes non conformes....71
Résolution d'un hôte non conforme....72
Conformité de la configuration....74
Affichage de la conformité de configuration....74
Affichage du rapport de dérive....75

Chapitre 12: Gestion des tâches OMIVV..... 76
Tâches de déploiement..... 76
Tâches de détection..... 77
Tâches de mise à jour du firmware du châssis..... 77
Tâches de mise à jour du firmware de l'hôte..... 78
Tâches du mode de verrouillage du système..... 78
Tâche de détection de dérive..... 79
Affichage de la tâche d'inventaire de l'hôte..... 80
Exécution de la tâche d'inventaire..... 80
Modification de la tâche d'inventaire des hôtes..... 81
Affichage de la tâche d'inventaire du châssis..... 81
Exécution d'une tâche d'inventaire du châssis..... 82
Affichage de la garantie des hôtes..... 82
Modification de la tâche de garantie de l'hôte..... 82
Affichage de la garantie du châssis..... 83

Chapitre 13: Gestion des journaux..... 84
Afficher l'historique du journal..... 84

Chapitre 14: Gestion des paramètres de l'appliance OMIVV..... 85
Gestion de plusieurs appliances..... 85
Configuration des notifications d'expiration de la garantie..... 85
Configuration de la notification relative à la dernière version de l'appliance..... 86
Configuration des informations d'identification de déploiement..... 86
Intégrité de la redondance des composants matériels - Proactive HA..... 86
Événements Proactive HA..... 87
Configuration de Proactive HA pour les serveurs rack et tour..... 88
Activation de Proactive HA sur des clusters..... 89
Remplacement de la gravité des notifications de mise à jour de l'intégrité..... 90
Configuration initiale..... 90
Afficher l'état de la configuration initiale..... 91
Paramètres de mise à jour de firmware..... 91
Affichage des informations de licence..... 91
Gestion des licences d'OpenManage Integration pour VMware vCenter (OMIVV)..... 92
Achat d'une licence logicielle..... 93
Accès aux informations de support..... 93
Création et téléchargement d'un lot de dépannage..... 93
Réinitialisation de l'iDRAC..... 93

Chapitre 15: Gestion des paramètres de vCenter..... 95
À propos des événements et des alarmes..... 95
Configuration des événements et alarmes..... 96
Affichage des événements du châssis..... 96
Affichage des alarmes de châssis..... 96
Affichage des paramètres d'alarmes et d'événements..... 97
Événements relatifs à la virtualisation..... 97
Gestion de la planification de la récupération des données..... 109
Planification d'une tâche d'inventaire..... 109

Planification des tâches de récupération de la garantie....109

Chapitre 16: Gestion de châssis....111
Affichage des informations sur les châssis Dell EMC.... 111
Affichage des informations sur l'inventaire du châssis....111
Affichage des informations d'inventaire matériel du châssis....112
Affichage des informations sur l'inventaire du firmware.... 114
Affichage des informations sur le contrôleur de gestion.... 114
Affichage des informations sur l'inventaire de stockage....115
Afficher les informations sur la garantie.... 116
Affichage de l'hôte associé à un châssis....116
Affichage des informations sur le châssis lié.... 117
Gestion d'un châssis MX PowerEdge.... 117
Gestion du châssis et de l'hôte à l'aide de l'IP de gestion unifiée des châssis.... 118
Ajout d'un châssis PowerEdge MX....118
mise à jour de firmware d'un châssis MX.... 119

Chapitre 17: Gestion des hôtes.... 121
Affichage des hôtes OMIVV....121
Surveillance d'un seul hôte.... 121
Affichage du résumé des informations de l'hôte.... 121
Affichage des informations sur l'hôte OMIVV....123
Surveillance des hôtes sur des clusters et des datacenters....128
Mise à jour du micrologiciel....134
Mise à jour du firmware et du pilote sur un hôte vSAN.... 134
Mise à jour du firmware et du pilote sur le cluster vSAN.... 137
Mise à jour du firmware sur l'hôte vSphere....139
Mise à jour du firmware sur le cluster vSphere....141
Mise à jour du même type de composant de firmware....142
Présentation de vSphere Lifecycle Manager.... 143
Afficher l'état du vSphere LifeCycle Manager dans la console d'administration Dell EMC....144
Inscription de vSphere Lifecycle Manager dans la Console Administration Dell EMC.... 144
Annulation de l'enregistrement de vSphere Lifecycle Manager dans la Console Administration Dell EMC.... 144
Gestion des clusters à l'aide de vSphere Lifecycle Manager....144
Utilisation d'OMIVV en tant que fournisseur de module complémentaire de firmware dans vSphere LifeCycle Manager : interface utilisateur.... 145
Afficher l'état de conformité du cluster....145
Résoudre les problèmes de conformité de cluster....146
Vérification de compatibilité matérielle....146
Exécuter une vérification préalable aux mesures correctives.... 146
Correction de cluster dans vSphere LifeCycle Manager....147
Utilisation d'OMIVV en tant que fournisseur de modules complémentaires de firmware dans vSphere Lifecycle Manager — API d'automatisation vSphere....147
Configuration de l'indicateur de clignotement.... 151
Configuration du mode de verrouillage du système.... 151

Chapitre 18: Autorisations et rôles de sécurité....152
Intégrité des données....152
Rôles, autorisation et authentification de contrôle d'accès....152
Rôle opérationnel Dell....152

Rôle de déploiement de l'infrastructure Dell....153
À propos des privilèges....153

Chapitre 19: Questions fréquemment posées (FAQ)....155
Questions fréquemment posées (FAQ)....155
Le type de licence iDRAC et sa description ne s'affichent pas correctement pour les hôtes vSphere non conformes....155
Le fournisseur Dell Inc ne s'affiche pas en tant que fournisseur de mise à jour d'intégrité....155
La connexion test ou l'inventaire d'hôte échoue en raison d'une adresse IP non valide ou inconnue de l'iDRAC....156
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....156
Les privilèges Dell attribués lors de l'enregistrement de l'appliance OMIVV ne sont pas supprimés après le désenregistrement d'OMIVV....156
Comment puis-je résoudre le code d'erreur 2000000 provoqué par VMware Certificate Authority (VMCA) ?....156
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....157
Que faire lorsqu'une erreur de communication Web dans le client vCenter HTML-5 s'ouvre après la modification des paramètres DNS dans OMIVV ?....157
La date d'installation s'affiche sous la forme 12-31-1969 pour certains firmwares sur la page du firmware....157
Je ne vois pas l'icône OpenManage Integration dans le client HTML-5, même si l'enregistrement du plug-in auprès de vCenter a réussi....157
Pourquoi les paramètres de configuration de DNS sont-ils restaurés à leurs paramètres d'origine après le redémarrage de l'appliance si les paramètres IP de l'appliance et DNS sont remplacés par des valeurs de DHCP....158
L'exécution de la mise à jour du firmware peut afficher un message d'erreur, le fichier de la logithèque de firmwares n'existe pas ou est non valide....158
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....158
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....158
Pourquoi le portail d'administration affiche-t-il un emplacement de référentiel des mises à jour inaccessible ?....159
Pourquoi le système n'est pas passé en mode maintenance lorsque j'ai effectué la mise à jour du micrologiciel de un à plusieurs ?....159
L'intégrité globale du châssis reste en bon état lorsqu'une partie de l'état du bloc d'alimentation passe à l'état critique....159
La version du processeur s'affiche comme « Non applicable » dans la vue du processeur de la page de présentation du système....159
OMIVV prend-il en charge vCenter en mode lié ?....159
Quels sont les paramètres de port requis pour OMIVV ?....159
Le mot de passe utilisé pour la détection sans système d'exploitation ne change pas pour l'utilisateur après l'application réussie du profil système comportant le même utilisateur doté de nouvelles données d'identification modifiées dans la liste d'utilisateurs d'iDRAC....161
Impossible d'afficher les détails des nouvelles versions de l'iDRAC répertoriés dans la page des hôtes et des clusters vCenter....161
OMIVV peut-il prendre en charge l'ESXi avec le mode de verrouillage activé ?....161
Quand j'ai essayé d'utiliser le mode de verrouillage, celui-ci a échoué....161
Les tentatives de déploiement d'ESXi sur un serveur échouent....162
Les systèmes détectés automatiquement s'affichent sans information de modèle dans l'assistant Déploiement....162

Le partage NFS est configuré avec l'ISO ESXi, mais le déploiement échoue avec des erreurs de montage de l'emplacement du partage....162
Comment puis-je forcer la suppression de l'appliance OMIVV de vCenter....162
La saisie d'un mot de passe sur l'écran Backup Now (Sauvegarder maintenant) produit un message d'erreur....163
Que dois-je faire en cas d'échec d'une mise à jour de micrologiciel ?....163
Que dois-je faire en cas d'échec de l'enregistrement de vCenter ?....163
Performances au cours de la lecture des informations d'identification du test de profil d'informations d'identification d'hôte ralenties ou absence de réponse....163
Est-ce qu'OMIVV prend en charge l'appliance VMware vCenter Server ?....163
Un serveur peut apparaître comme non conforme avec l'état CSIOR, « Inconnu »....164
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....164
L'hôte s'affiche sous le châssis, même après la suppression de l'hôte de l'arborescence de vCenter....164
Après la sauvegarde et la restauration d'OMIVV, les paramètres de l'alarme ne sont pas restaurés....164
Échec du déploiement du système d'exploitation lorsqu'un NPAR est activé sur un nœud cible et désactivé sur le profil système....164
La version disponible de l'appliance OMIVV affiche des informations erronées lorsque la version disponible est inférieure à la version actuelle....164
L'exception 267027 est générée lors de l'ajout d'un serveur sans système d'exploitation de 12e génération et ultérieur....165
Lors du déploiement, l'application du profil matériel échoue en raison d'une erreur iDRAC....165
La mise à niveau RPM OMIVV échoue si le proxy est configuré avec une authentification d'utilisateur de domaine....165
Impossible d'appliquer un profil système si la carte PCIe est dans le châssis FX....165
La détection de dérive montre une non-conformité pour les serveurs modulaires qui ont une carte PCIe dans le châssis FX....165
Impossible de déployer un système d'exploitation sur des serveurs PowerEdge lorsque l'iDRAC ne remplit pas l'adresse MAC de la carte réseau sélectionnée....166
Lors de la création d'un profil d'informations d'identification pour l'hôte ayant ESXi 6.5 U1, le numéro de série de l'hôte n'est pas affiché sur la page Sélectionner les hôtes....166
L'icône Dell ne s'affiche pas après la sauvegarde et la restauration d'une version d'OMIVV précédente vers une version d'OMIVV ultérieure....166
Lors de la mise à niveau ou de la rétrogradation de certaines versions du firmware iDRAC utilisant OMIVV, et même lorsque la mise à jour du firmware a réussi, OMIVV peut indiquer que la tâche a échoué....166
La configuration du mode System Lockdown à un niveau cluster affiche parfois le message « Aucun hôte sous le cluster ne dispose d'inventaire réussi »....167
Après la mise à niveau RPM de l'appliance OMIVV, plusieurs entrées de journaux sont parfois visibles dans les tâches récentes de vCenter....167
Après l'enregistrement de vCenter, le logo Dell EMC d'OMIVV ne s'affiche pas sur la page d'accueil de VMware....167
Les serveurs PowerEdge 11G non conformes sont conservés dans l'inventaire OMIVV après la sauvegarde et la restauration....167
Impossible de lancer vCenter depuis le client Flex après la mise à niveau de l'appliance OMIVV....167
Lors de l'ajout ou de la suppression de cartes réseau dans OMIVV, les cartes réseau existantes disparaissent de la console OMIVV....168
Après l'ajout ou le retrait de la deuxième carte réseau, la page Configuration réseau affiche trois cartes réseau....168
Un serveur dont l'état est inconnu dans la version antérieure n'est pas répertorié sur la page serveurs sans système d'exploitation après la sauvegarde et la restauration vers la version OMIVV la plus récente....168

Après le déploiement du SE, OMIVV n'a pas pu ajouter l'hôte ESXi à vCenter, n'a pas pu ajouter un profil d'hôte ou le passage en mode maintenance de l'hôte échoue.... 169
L'état de la licence iDRAC s'affiche comme étant conforme sur la page Gestion de la conformité lorsque l'adresse IP iDRAC n'est pas accessible....169
L'hôte ESXi est déconnecté ou ne répond pas après un déploiement réussi du SE à l'aide d'OMIVV.... 169
La tâche de déploiement expire lorsque la carte d'interface réseau (NIC) d'OMIVV n'est pas connectée au réseau de l'hôte ESXi.... 169
La tâche de garantie ne s'exécute pas pour certains hôtes....169
L'initialisation de Proactive HA ne se produit pas après l'exécution de la sauvegarde et de la restauration....169
La page OMIVV affiche des erreurs de session non valide, d'expiration de délai d'attente ou 2 millions dans le navigateur Firefox....170
Dans vCenter, le volet Tâches récentes n'affiche pas la colonne Détails pour certaines notifications de tâche OMIVV....170
Lors de l'utilisation de vCenter 6.5 U2, un message d'erreur 2000002 peut s'afficher sur toutes les pages d'OMIVV.... 170
L'erreur 2000002 s'affiche sur toutes les pages d'OMIVV après la mise à niveau ou la sauvegarde du RPM et la restauration d'OMIVV vers une version ultérieure.... 170
Parfois, OMIVV prend beaucoup de temps à désenregistrer vCenter....171
Après la mise à jour du certificat OMIVV, le message d'erreur « Échec de la connexion de l'appliance OMIVV. Le certificat SSL n'est pas valide » s'affiche.... 171
Échec de la tâche de déploiement dans OMIVV....171
Échec du test de connexion et de l'inventaire dans OMIVV après la modification du mot de passe vCenter....171
L'instance OMIVV n'est pas supprimée de vCenter après la réinitialisation de l'appliance OMIVV sur les paramètres d'usine....171
OMIVV affiche uniquement les attributs du BIOS et de l'iDRAC sur la page Paramètres de profil du profil du système....172
Le déploiement du système d'exploitation s'est terminé avec une erreur inconnue.... 172
Échec de la mise à jour de firmware du contrôleur CMC (Chassis Management Controller) dans le châssis FX2.... 172
Échec du déploiement du profil ISO dans OMIVV....172
Problèmes de déploiement de serveurs sur matériel vierge.... 172
Activation de la détection automatique sur un système récemment acheté.... 173

Annexe A : Attributs spécifiques au système.... 174

Annexe B : Informations supplémentaires....178

Annexe C : Attributs de personnalisation....179

Annexe D : Matrice de comparaison de la version du composant avec la version de ligne de base.....180

Annexe E : Codes de réponse.... 182

1

Introduction

Les administrateurs informatiques utilisent VMware vCenter en tant que console principale pour gérer et surveiller les hôtes VMware vSphere ESX/ESXi. OpenManage Integration pour Vmware vCenter (OMIVV) vous permet de réduire la complexité de la gestion de votre centre de données en rationalisant les tâches associées à la gestion et à la surveillance de l'infrastructure de serveur Dell EMC dans l'environnement vSphere.

Nouveautés de cette version

Cette version d'OpenManage Integration for VMware vCenter 5.2 fournit les fonctionnalités suivantes :

- Présentation des API RESTFul OMIVV

  Pour en savoir plus, consultez le *Guide API d'OpenManage Integration for VMware vCenter version 5.2* disponible à l'adresse **https://www.dell.com/support/**.
- Support de vSphere 7.0 U1
- Support des serveurs PowerEdge XE2420
- Support pour la restauration sur matériel vierge basée sur IPv4
- Améliorations de la sécurité
- Ajout d'une option de filtre sur les pages **Châssis Dell EMC** et **Hôtes Dell EMC** pour filtrer l'hôte et le châssis en fonction de l'état d'intégrité
- Amélioration de la création de rapport de garantie pour l'hôte possédant plusieurs ou différentes garanties.

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	La fonction d'inventaire fournit les éléments suivants : Détails du serveur PowerEdge, comme la mémoire (quantité et type), la carte réseau, le bloc d'alimentation, les processeurs et le Remote Access Controller (RAC) les informations de garantie, le serveur, le cluster et la vue du niveau du datacenter. Détails du châssis, tels que les informations du contrôleur CMC (Chassis Management Controller) ou du module de gestion, l'alimentation du châssis, l'état du KVM, les détails thermiques ou du ventilateur, les informations de garantie, le commutateur, le serveur ou les détails de stockage. Prise en charge d'une relation de châssis MX dans la configuration MCM (Multi-Chassis Management). Informations sur la structure pour une configuration MCM d'un châssis MX. Informations sur le matériel QuickSync pour un châssis MX.

Tableau 1. Fonctions OMIVV (suite)

Fonctionnalités	Description
Surveiller et envoyer des alertes	La surveillance et l'envoi d'alertes comprennent les fonctionnalités suivantes : 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 tels que l'inventaire, les événements, les alarmes pour diagnostiquer les problèmes de serveur et de châssis. Prise en charge de la fonctionnalité VMware Proactive HA.
Mises à jour de firmware	La mise à jour de firmware de serveur prenant en charge les clusters comprend les éléments suivants : Mettre à jour les serveurs pris en charge vers la version la plus récente du BIOS et du firmware. Vous pouvez également utiliser OMIVV avec vSphere Lifecycle Manager pour effectuer la mise à jour de firmware (applicable pour vCenter 7.0 et versions ultérieures).
Détection de dérive pour les clusters	Conformité du firmware pour les clusters Conformité des pilotes pour les clusters vSAN Conformité matérielle **REMARQUE :** La conformité matérielle n'est pas prise en charge pour les hôtes qui sont gérés à l'aide d'un profil d'informations d'identification de châssis.
Mises à jour des pilotes	Mises à jour des pilotes pour les clusters vSAN.
Déploiement	Déploiement, incluant : Créer et déployer des profils système. Déployer à distance un système d'exploitation sur les serveurs sans système d'exploitation à l'aide de VMware vCenter sans utiliser PXE.
Informations de service	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 facile en ligne de la garantie.
Rôles et autorisations de sécurité	Les rôles et autorisations de sécurité comprennent les fonctionnalités suivantes : S'intègre avec les règles, autorisations et l'authentification vCenter standard. Prise en charge du mode de verrouillage par les serveurs basés sur l'iDRAC9. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.
Prise en charge du serveur OEM	Les fonctionnalités OMIVV suivantes sont prises en charge : Inventaire Surveiller et envoyer des alertes mise à jour de firmware Déploiement

Tableau 1. Fonctions OMIVV (suite)

Fonctionnalités	Description
	Informations de service Rôles et autorisations de sécurité
mise à jour de firmware d'un châssis MX	Fournit une option pour mettre à jour le firmware du module de gestion pour les châssis MX.

REMARQUE : À partir d'OMIVV 5.0 et versions ultérieures, seul le client VMware vSphere (HTML-5) est pris en charge, pas le client Web vSphere (FLEX).

2

Connexion à la console d'administration OMIVV Dell EMC.

Vous pouvez administrer OpenManage Integration pour Vmware vCenter et son environnement virtuel en utilisant l'un des deux portails d'administration mentionnés ci-dessous :

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

1. Accédez à https://<ApplianceIP/hostname/>.

   La durée de verrouillage du compte est d'une minute.

   Vous ne pouvez pas démarrer une nouvelle session lorsque le compte est verrouillé. Cependant, une ancienne session active sera active.

2. Entrez le mot de passe.

   Si le mot de passe saisi est non valide, la tentative de connexion échoue. Après six tentatives de connexion infructueuses consécutives, le compte se verrouille. Les six tentatives de connexion infructueuses comprennent l'échec des tentatives de connexion dans la console d'administration ou l'API REST ou l'utilisation d'un jeton non valide pour accéder à l'API REST.

   La durée de verrouillage du compte est d'une minute.

   Vous ne pouvez pas créer de session lorsque le compte est verrouillé, mais une session active en cours reste active.

   Si vous vous connectez pour la première fois, vous êtes invité à accepter le CLUF.

3. Sur la page **Contrat de Licence Utilisateur Final Dell EMC**, lisez les conditions générales, puis cochez la case **J'accepte les termes du contrat de licence**.

   Pour en savoir plus sur le CLUF relatif à la télémétrie, cliquez sur **CLUF relatif à la télémétrie Dell EMC**.

4. Cliquez sur **Accepter**.

Enregistrement d'un nouveau serveur vCenter

Pour créer un utilisateur, votre compte vCenter doit disposer des privilèges nécessaires. Pour en savoir plus sur les privilèges requis, voir Privilèges requis pour les utilisateurs non administrateurs , page 15.

Vous pouvez enregistrer l'appliance OMIVV après avoir installé OMIVV. OMIVV utilise le compte d'utilisateur administrateur ou un compte d'utilisateur non-administrateur disposant des privilèges nécessaires pour les opérations vCenter. Une seule instance de l'appliance OMIVV peut prendre en charge 15 serveurs vCenter et jusqu'à 2 000 hôtes ESXi.

Si vous tentez d'inscrire plus de 15 vCenters, le message d'erreur suivant s'affiche :

Votre licence autorise uniquement <x> vCenters et tous sont déjà inscrit.

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

1. Accédez à https://<ApplianceIP/hostname/>.
2. Sur la page **ENREGISTREMENT VCENTER**, cliquez sur **Enregistrer un nouveau serveur vCenter** dans le volet de droite.
   La page **ENREGISTRER UN NOUVEAU vCENTER** s'affiche.
3. Dans la boîte de dialogue **ENREGISTRER UN NOUVEAU SERVEUR VCENTER**, sous **Nom du serveur vCenter**, effectuez les tâches suivantes :
   a. Dans la zone **Nom d'hôte ou IP du serveur vCenter**, saisissez l'adresse IP du serveur vCenter ou le FQDN de l'hôte.

      Dell EMC vous recommande d'enregistrer OMIVV dans VMware vCenter en utilisant le nom de domaine complet (FQDN). Pour tous les enregistrements, le nom d'hôte du serveur 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 informations du nom d'hôte OMIVV sont présentes dans les zones de recherches directes et inversées sur votre serveur DNS.

b. Dans la zone **Description**, saisissez une description (facultatif).

4. Sous **Compte d'utilisateur vCenter**, procédez comme suit :
   a. Dans la case **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 **Mot de passe**, saisissez le mot de passe.
   c. Dans la zone **Vérifier le mot de passe**, saisissez à nouveau le mot de passe.
   d. Cochez la case **Enregistrer vSphere Lifecycle Manager**.

      La sélection de la case à cocher **Enregistrer vSphere Lifecycle Manager** vous permet d'utiliser la fonctionnalité vSphere Lifecycle Manager à partir de vCenter 7.0 et versions ultérieures.
5. Cliquez sur **S'inscrire**.

   Le message d'erreur suivant s'affiche en cas d'échec de l'inscription de vCenter :

   Impossible de contacter le serveur vCenter <x> en question en raison d'informations d'identification incorrectes. Vérifiez le nom d'utilisateur et le mot de passe.

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

REMARQUE : Pour toutes les opérations de vCenter réalisées à partir de l'appliance OMIVV, OMIVV utilise les privilèges de l'utilisateur inscrit et non les privilèges de l'utilisateur connecté à VMware vCenter ou aux comptes locaux de l'appliance OMIVV.

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 de firmware à partir d'OMIVV. Lors de l'exécution de la tâche de mise à jour de firmware, OMIVV utilise les privilèges de l'utilisateur X pour mettre la machine en mode maintenance ou redémarrer l'hôte.

REMARQUE : Si vous souhaitez charger un certificat personnalisé signé par une autorité de certification (AC) sur OMIVV, assurez-vous de charger le nouveau certificat avant l'inscription de vCenter. Si vous chargez le nouveau certificat personnalisé après l'enregistrement dans vCenter, des erreurs de communication s'affichent dans le client vSphere. Pour résoudre ce problème, annulez l'enregistrement et recommencez l'enregistrement de l'appliance dans vCenter.

Enregistrement d'un serveur vCenter à l'aide d'un compte non-administrateur

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

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

1. Créez un rôle ou modifiez le rôle existant avec les privilèges obligatoires pour le rôle.

   Pour plus d'informations sur la liste des privilèges obligatoires pour le rôle, voir Privilèges obligatoires pour les utilisateurs non-administrateurs.

   Pour connaître les étapes obligatoires à suivre pour créer ou modifier un rôle et sélectionner des privilèges dans le client vSphere (HTML-5), reportez-vous à la documentation de VMware vSphere.
2. Après avoir créé et défini un rôle, attribuez-lui un utilisateur et sélectionnez les privilèges correspondants.

   Pour plus d'informations sur l'attribution de privilèges à un rôle, reportez-vous à la documentation VMware vSphere.

   Un utilisateur non-administrateur du vCenter Server doté des privilèges requis peut alors enregistrer et/ou annuler l'enregistrement du vCenter Server, modifier les informations d'identification ou procéder à la mise à jour du certificat.
3. Enregistrez un serveur vCenter à l'aide d'un utilisateur non-administrateur disposant des privilèges requis.
4. Une fois l'enregistrement terminé, attribuez les privilèges Dell au rôle créé ou modifié à l'étape 1. Voir la section Attribution de privilèges Dell à un rôle existant , page 16.

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

Privilèges requis pour les utilisateurs non administrateurs

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

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

- Alarmes
  - Créer l'alarme
  - Modifier l'alarme
  - Supprimer l'alarme
- Poste
  - Enregistrer le poste
  - Annuler l'enregistrement du poste
  - Mettre à jour le poste
- Global
  - Annuler la tâche
  - Événement journal
  - Paramètres
- Fournisseur de mise à jour de l'intégrité
  - Enregistrer
  - Annuler l'enregistrement
  - Mettre à jour
- Hôte
  - CIM
    - Interaction CIM
- Host.Config
  - Paramètres avancés
  - Modifier les paramètres
  - 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
- Lifecycle Manager : privilèges généraux
  - Lecture

  REMARQUE : Les privilèges généraux de vSphere Lifecycle Manager s'appliquent uniquement à vCenter 7.0 et versions ultérieures.
- Profil d'hôte
  - Modifier
  - Afficher
- Droits
  - Modifier les droits
  - Modifier le rôle
- Sessions
  - Valider la session
- Tâche
  - Créer
  - Mettre à jour

REMARQUE : Si un serveur vCenter est enregistré à l'aide d'un utilisateur non administrateur pour accéder à des fonctionnalités OMIVV, l'utilisateur non-administrateur doit disposer des privilèges Dell. Pour en savoir plus sur l'affectation de privilèges Dell, voir Attribution de privilèges Dell à un rôle existant , page 16.

Attribution de privilèges Dell à un rôle existant

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

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

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

   Pour plus d'informations sur les rôles OMIVV disponibles au sein du vCenter, voir la section sur les rôles et les autorisations de sécurité.
7. Modifiez le nom du rôle et saisissez une description pour le rôle sélectionné, le cas échéant.
8. Cliquez sur **TERMINER**.
   Déconnectez-vous, puis connectez-vous depuis vCenter. L'utilisateur disposant des privilèges requis peut désormais effectuer les opérations OMIVV.

Mise à jour des certificats des serveurs vCenter inscrits

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 chiffrement 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. OMIVV utilise ce certificat numérique pour activer HTTPS sur le serveur Web afin de sécuriser la communication.

Si le certificat est modifié sur un serveur vCenter, utilisez les tâches suivantes pour importer le nouveau certificat pour OMIVV :

1. Accédez à https://<ApplianceIP/hostname/>.
2. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**.
   Les serveurs vCenter enregistrés s'affichent dans le volet de travail.
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**.

Modification des informations d'identification pour la connexion à vCenter

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

Si une fonction Proactive HA est activée sur un cluster, vous ne devez pas modifier l'utilisateur qui est associé à ce dernier. Modifier l'enregistrement avec un autre utilisateur vCenter interrompt la fonctionnalité Proactive HA. Si les informations d'identification doivent être modifiées, annulez l'enregistrement des anciennes informations d'identification et enregistrez-vous à l'aide des nouvelles informations d'identification.

1. Accédez à 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 s'affichent dans le volet de travail.

4. Pour ouvrir la fenêtre **MODIFIER LE COMPTE UTILISATEUR**, sous **Références**, cliquez sur **Modifier** pour un vCenter enregistré.
5. Si des informations d'identification incorrectes sont saisies, un message s'affiche. Saisissez un nom d'utilisateur vCenter valide, un mot de passe, puis saisissez à nouveau le mot de passe pour le vérifier.
6. Pour modifier le mot de passe, cliquez sur **Appliquer**. Pour annuler une mise à jour, cliquez sur **Annuler**.

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

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

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

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

1. Accédez à https://<ApplianceIP/hostname/>.
2. Sur la page **ENREGISTREMENT DE VCENTER**, puis dans le tableau **Nom d'hôte ou adresse IP du serveur vCenter**, cliquez sur **Annuler l'enregistrement**.

   REMARQUE : Assurez-vous de sélectionner le bon serveur vCenter car OMIVV peut être associé à plusieurs serveurs vCenter.

3. Pour confirmer l'annulation de l'enregistrement du serveur vCenter sélectionné, accédez à la boîte de dialogue **DÉSENREGITRER UN VCENTER**, puis cliquez sur **Désenregistrer**.

   REMARQUE : Une fois le désenregistrement d'OMIVV effectué, déconnectez-vous, puis connectez-vous à partir du client vSphere (HTML-5). Si l'icône OMIVV est toujours visible, redémarrez les services clients pour le client vSphere (HTML-5) et le client Web (FLEX).

Chargement d'une licence sur la Console Administration OMIVV

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

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

   REMARQUE : Si vous modifiez le fichier de licence de quelque façon que ce soit, le fichier de licence (fichier .XML) ne fonctionne pas. Vous pouvez télécharger le fichier .XML (clé de licence) à partir de Dell Digital Locker. Si vous ne parvenez pas à télécharger vos clés de licence, contactez le service de support Dell en vous rendant sur Contact Technical Support à l'adresse **https://www.dell.com/support** pour trouver le numéro de téléphone du service du support Dell de votre zone géographique pour votre produit.

Gestion de l'appliance OMIVV

La gestion de l'appliance OMIVV vous permet de gérer le réseau, le protocole NTP et les informations HTTPS concernant OpenManage Integration pour Vmware vCenter. En outre, cette gestion permet à un administrateur d'exécuter les actions suivantes :

- Redémarrez l'appliance OMIVV. Voir la section Redémarrage de l'appliance OMIVV , page 18.
- Mettre à jour l'appliance OMIVV et configurer un emplacement pour la logithèque de mise à jour. Voir Mise à niveau de l'appliance OMIVV et de l'emplacement de la logithèque , page 18
- Mise à niveau de l'appliance OMIVV à l'aide de RPM. Voir la section Mise à niveau de l'appliance OMIVV à l'aide de RPM (via Internet). , page 19.
- Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations. Voir la section Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations , page 20.
- Génération et téléchargement du lot de dépannage. Voir la section Génération et téléchargement du lot de dépannage , page 23.
- Configuration du proxy HTTP. Voir la section Configuration du proxy HTTP , page 23.
- Configuration des serveurs NTP (Network Time Protocol). Voir la section Configuration des serveurs NTP (Network Time Protocol) , page 23.
- Configuration du mode de déploiement. Voir la section Configuration du mode de déploiement , page 23.
- Surveillance étendue Voir Surveillance étendue , page 24.
- Génération d'une requête de signature de certificat (CSR). Voir la section Génération d'une requête de signature de certificat (CSR) , page 25.
- Chargement d'un certificat HTTPS. Voir la section Chargement d'un certificat HTTPS , page 25.
- Configuration des alertes globales. Voir la section Configuration des alertes globales , page 25.

Accès à la gestion de l'appliance

Dans Dell OpenManage Integration pour Vmware vCenter, exécutez les étapes suivantes pour accéder à la page **GESTION DE L'APPLIANCE** à l'aide du Portail Administration :

1. Accédez à 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 OMIVV

1. Sur la page **GESTION DE L'APPLIANCE**, cliquez sur **Redémarrer l'appliance virtuelle**.
2. Pour redémarrer l'appliance OMIVV, accédez à la boîte de dialogue **Redémarrer l'appliance virtuelle** et cliquez sur **Appliquer**.

Mise à niveau de l'appliance OMIVV et de l'emplacement de la logithèque

- Pour garantir la protection de toutes les données, sauvegardez la base de données OMIVV avant de mettre à jour l'appliance OMIVV. Voir la section Gestion des sauvegardes et restaurations , page 21.
- 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. Si vous avez besoin d'un réseau proxy, en fonction des paramètres réseau de l'environnement, activez les paramètres proxy et saisissez les données proxy. Voir la rubrique .Configuration du proxy HTTP.
- Vérifiez que le **Chemin d'accès au référentiel de mise à jour** est valide.
- N'oubliez pas de vous déconnecter de toutes les sessions du client vSphere (HTML-5) avec les serveurs vCenter enregistrés.
- Avant de vous connecter à l'un des serveurs vCenter enregistrés, pensez à mettre simultanément à jour toutes les appliances appartenant au même contrôleur PSC (Platform Service Controller) avant de vous connecter à l'un des serveurs vCenter enregistrés. Sinon, vous êtes susceptible de voir des informations incohérentes sur les instances d'OMIVV.

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

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

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

Option	Description
1	Si une coche s'affiche en regard de RPM, vous pouvez effectuer une mise à niveau RPM de la version existante à la dernière version disponible. Voir la section Mise à niveau de l'appliance OMIVV à l'aide de RPM (via Internet). , page 19.

Option	Description
2	Si une coche s'affiche en regard d'OVF, vous pouvez sauvegarder la base de données OMIVV depuis la version existante et la restaurer dans la dernière version d'appliance disponible. Voir la section Mise à niveau de l'appliance OMIVV à l'aide des sauvegardes et restaurations , page 20.
3	Si une coche s'affiche en regard de RPM et OVF, vous pouvez effectuer l'une des tâches ci-dessus pour mettre à niveau votre appliance. Dans ce cas, la tâche recommandée est une mise à niveau RPM.

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

Options de mise à niveau d'OMIVV

Sauvegarde et restauration

Vous pouvez exécuter des sauvegardes et des restaurations à partir d'OMIVV 5.0 ou version ultérieure vers la version la plus récente (avec vCenter 6.5 et versions supérieures).

Mise à niveau du RPM

Vous pouvez exécuter la mise à niveau du RPM à partir d'OMIVV 5.0 vers la version la plus récente.

Mise à niveau de l'appliance OMIVV à l'aide de RPM (via Internet).

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

Il est recommandé de réaliser un snapshot de l'appliance avant de mettre à niveau l'appliance OMIVV.

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

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

2. Pour mettre à niveau le plug-in OMIVV à partir d'une version existante vers la version disponible, effectuez l'une des opérations suivantes :

   - Pour effectuer une mise à niveau avec RPM, disponible dans **Chemin d'accès au référentiel de mise à jour**, assurez-vous que le chemin défini dans **Chemin d'accès au référentiel de mise à jour** est : https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

   Si le chemin est différent, dans la fenêtre **Gestion de l'appliance**, dans la zone **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Modifier** pour mettre à jour le chemin d'accès vers https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ dans la zone de texte **Chemin d'accès au référentiel de mise à jour** et cliquez sur **Appliquer**.

3. Comparez la version de l'appliance OMIVV disponible avec la version actuelle.
4. Pour appliquer la mise à jour à l'appliance OMIVV, sous **Paramètres d'appliance**, cliquez sur **Mettre à jour l'appliance virtuelle**.
5. Dans la boîte de dialogue **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Mettre à jour**.
   En cliquant sur **Mettre à jour**, vous vous déconnectez de la fenêtre **CONSOLE ADMINISTRATION**.
6. Fermez le navigateur Web.

   Au cours du processus de mise à niveau, l'appliance redémarre une ou deux fois. Une fois que l'appliance est mise à niveau avec RPM, assurez-vous d'effacer le cache du navigateur avant de vous connecter au portail Administration Dell.

   Une fois la mise à niveau RPM terminée, vous pouvez afficher l'écran de connexion de la console OMIVV. Ouvrez un navigateur, saisissez le lien *https:\\<IPAppliance|nomhôte>*, puis accédez à la zone **MISE À JOUR DE L'APPLIANCE**. Vous pouvez vérifier si les versions de l'appliance OMIVV et de l'appliance disponible sont identiques.

   Toutes les personnalisations effectuées sur les alarmes Dell enregistrées et le fournisseur de mise à jour d'intégrité Dell pour le cluster PHA sont restaurées sur les valeurs par défaut après la mise à niveau du RPM.

Mise à niveau de l'appliance OMIVV à l'aide de RPM (sans Internet)

Créez un partage HTTP ou HTTPS. Vérifiez que le partage HTTP ou HTTPS prend en charge le nom de fichier qui inclut des caractères spéciaux tels que ++ et les espaces.

OMIVV ne prend en charge que les partages HTTP et HTTPS.

OMIVV prend en charge la mise à niveau de la version 5.1 vers 5.2 sans connexion Internet.

1. Téléchargez le package RPM.zip disponible sur **https://www.dell.com/support**.
2. Extrayez le package RPM. zip et copiez les fichiers et dossiers à partir de l'emplacement extrait vers le partage HTTP ou HTTPS.
3. Sur la page **GESTION DE L'APPLIANCE**, dans la zone **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Modifier**, puis saisissez le chemin d'accès à l'emplacement partagé dans le **Chemin d'accès au référentiel de mise à jour**.
4. Cliquez sur **Appliquer**.
5. Comparez la version de l'appliance OMIVV disponible avec la version actuelle.
6. Pour appliquer la mise à jour à l'appliance OMIVV, sous **Paramètres d'appliance**, cliquez sur **Mettre à jour l'appliance virtuelle**.
7. Dans la boîte de dialogue **MISE À JOUR DE L'APPLIANCE**, cliquez sur **Mettre à jour**.
   En cliquant sur **Mettre à jour**, vous vous déconnectez de la fenêtre **CONSOLE ADMINISTRATION OMIVV**.

   L'exécution de la mise à jour peut prendre 40 minutes en fonction de la vitesse de votre réseau.
8. Fermez le navigateur Web.
   Une fois la mise à jour de l'appliance terminée, assurez-vous d'effacer le cache du navigateur avant de vous connecter à la **CONSOLE ADMINISTRATION OMIVV**.

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

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

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

Il est recommandé de réaliser un snapshot de l'appliance avant de mettre à niveau l'appliance OMIVV.

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

1. Sauvegardez les données des versions antérieures.
2. Mettez l'ancienne appliance OMIVV hors tension depuis le vCenter.
3. Déployez la nouvelle appliance OVF OpenManage Integration.
4. Mettez la nouvelle appliance OpenManage Integration sous tension.
5. Configurez le réseau et le fuseau horaire de la nouvelle appliance.

   REMARQUE : Nous vous recommandons de conserver l'identité (IP ou FQDN) de l'appliance OMIVV précédente pour la nouvelle appliance OMIVV.
6. L'appliance OMIVV est livrée avec le certificat par défaut. Si vous souhaitez obtenir un certificat personnalisé pour votre appliance, mettez à jour les mêmes éléments. Reportez-vous aux sections Génération d'une requête de signature de certificat (CSR) , page 25 et Chargement d'un certificat HTTPS , page 25. Sinon, ignorez cette étape.
7. Restaurez la base de données sur la nouvelle appliance OMIVV. Voir Restauration de la base de données OMIVV à partir d'une sauvegarde.
8. Vérifiez l'appliance. Pour plus d'informations, voir . la section Vérification de l'installation du Guide d'installation
9. Après la mise à niveau, nous vous recommandons d'exécuter à nouveau l'inventaire sur tous les hôtes gérés par le plug-in OMIVV.

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

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

   Toutes les personnalisations effectuées sur les alarmes Dell enregistrées et le fournisseur de mise à jour d'intégrité Dell pour le cluster PHA sont restaurées sur les valeurs par défaut une fois que vous avez effectué une sauvegarde ou une restauration.

   Après la sauvegarde et la restauration d'une version d'OMIVV antérieure vers une version supérieure, procédez comme suit si vous observez l'un des problèmes suivants :

- 200 000 messages
- Logo Dell EMC manquant
- L'interface utilisateur d'OMIVV ne répond plus.
- Le plug-in OMIVV n'est pas supprimé de vCenter.
- Le certificat SSL n'est pas valide.

Résolution :

- Redémarrez les services clients vSphere pour le client vSphere (HTML-5) et le client Web vSphere (FLEX) sur le serveur vCenter.
- Si le problème persiste :
  - Pour l'appliance VMware vCenter Server : accédez à : `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`. Pour Windows vCenter, accédez aux dossiers suivants de l'appliance vCenter et vérifiez si les anciennes données correspondant à la version antérieure existent : dossier `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` dans l'appliance vCenter, et vérifiez si les anciennes données, telles que com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX, existent.
  - Supprimez manuellement le dossier correspondant à la version précédente d'OMIVV et redémarrez les services clients vSphere pour le client vSphere (HTML-5) et le client Web (FLEX).

Si l'adresse IP de la nouvelle appliance est différente de l'adresse IP de l'ancienne appliance, procédez comme suit :

- La fonctionnalité Proactive HA peut ne pas fonctionner correctement. Dans un tel cas de figure, désactivez et activez la fonctionnalité Proactive HA pour chaque cluster sur lequel l'hôte Dell EMC est présent.
- Configurez la destination d'interruption pour que les traps SNMP vous orientent vers la nouvelle appliance. Ce problème est réglé en exécutant l'inventaire sur ces hôtes. Lors de l'exécution de l'inventaire sur les hôtes, si des traps SNMP ne pointent pas vers la nouvelle adresse IP, ces hôtes sont répertoriés comme non conformes. Pour corriger les problèmes de conformité de l'hôte, voir Résolution d'un hôte non conforme , page 72.

Gestion des sauvegardes et restaurations

La Console Administration vous permet d'effectuer des tâches de sauvegarde et de restauration.

- Configuration des sauvegardes et restaurations
- Planification des sauvegardes automatiques
- Exécution d'une sauvegarde immédiate
- Restauration de la base de données à partir d'une sauvegarde
- Réinitialisation des paramètres de sauvegarde et de restauration , page 23

Dans OMIVV, effectuez les étapes suivantes pour accéder à la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION** à l'aide de la Console Administration :

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

Configuration des sauvegardes et restaurations

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

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

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

      Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#$%* ».
   e. Dans la zone de texte **Confirmer le mot de passe**, saisissez à nouveau le mot de passe crypté.

3. Pour enregistrer ces paramètres, cliquez sur **Appliquer**.
4. Configurez la planification des sauvegardes. Voir Planification des sauvegardes automatiques.

À l'issue de cette procédure, configurez une planification de sauvegarde.

Planification des sauvegardes automatiques

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

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Modifier les sauvegardes automatiques planifiées**.
   Les champs pertinents sont activés.
2. Pour activer les sauvegardes, cliquez sur **Activer**.
3. Cochez les cases **Jours de sauvegarde** correspondant aux jours de la semaine où vous voulez exécuter les tâches de sauvegarde.
4. Dans le champ **Heure de sauvegarde (24 heures, HH:mm)**, saisissez l'heure au format HH: mm.
   Le champ **Prochaine sauvegarde** est renseigné avec la date et l'heure de la prochaine sauvegarde planifiée.
5. Cliquez sur **Appliquer**.

Exécution d'une sauvegarde immédiate

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Sauvegarder maintenant**.
2. Pour utiliser l'emplacement et le mot de passe de cryptage des paramètres de sauvegarde, dans la boîte de dialogue **SAUVEGARDER MAINTENANT**, cochez la case **Utiliser l'emplacement et le mot de passe de cryptage des paramètres de sauvegarde**.
3. Entrez des valeurs pour l'**Emplacement de la sauvegarde**, le **Nom d'utilisateur**, le **Mot de passe** et le **Mot de passe de cryptage**.
   Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#$%* ». Il n'existe aucune limite de caractères pour former un mot de passe.
4. Cliquez sur **Sauvegarder**.

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

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

- Les serveurs de 11e génération ne sont pas pris en charge. Seuls les serveurs 12G et les générations suivantes sont conservés après restauration.
- Les profils matériels et les modèles de déploiement ne sont pas pris en charge. Nous vous recommandons d'utiliser le profil système pour le déploiement.
- Les tâches de déploiement planifiées sur des serveurs 11G et/ou utilisant des modèles de déploiement basés sur les profils matériels sont annulées.
- Tous les serveurs 11G sont supprimés des profils d'identification et les licences consommées sont abandonnées.
- Les profils de logithèque n'utiliseront que des ensembles 64 bits.

  REMARQUE : Si vous exécutez des sauvegardes et des restaurations depuis une version 4.x vers une 5.x, un symbole d'avertissement s'affiche en regard du nom du profil de cluster, car OMIVV ne prend pas en charge le lot de firmwares 32 bits dans les versions 5.x. Pour utiliser les dernières modifications apportées au profil de cluster, modifiez le profil de cluster.
- Les tâches de mise à jour de firmware planifiées sur les serveurs 11G sont annulées.

Assurez-vous que le mode de déploiement approprié est configuré avant d'effectuer l'opération de restauration. Pour en savoir plus sur la configuration du mode de déploiement, voir le document Configuration du mode de déploiement , page 23.

1. Sur la page **PARAMÈTRES DE SAUVEGARDE ET RESTAURATION**, cliquez sur **Restaurer maintenant**.
2. Dans la boîte de dialogue **RESTAURER MAINTENANT**, saisissez le chemin d'accès de l'**Emplacement du fichier** et du fichier .gz au format CIFS ou NFS.
3. Entrez un **Nom d'utilisateur**, un **Mot de passe** et un **Mot de passe de chiffrement** pour le fichier de sauvegarde.
   Le mot de passe de chiffrement peut contenir des caractères alphanumériques et des caractères spéciaux, tels que « !@#$%* ».
4. Pour enregistrer les modifications, cliquez sur **Appliquer**.
   L'opération de restauration entraîne le redémarrage de l'appliance OMIVV à la fin de la restauration. Pour vérifier l'installation, voir la rubrique vérification de l'installation dans le Guide d'installation.

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

Réinitialisation des paramètres de sauvegarde et de restauration

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

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

Génération et téléchargement du lot de dépannage

Pour générer le lot de dépannage, assurez-vous que vous vous connectez au portail Administration.

Le lot de dépannage contient des informations sur la consignation d'OMIVV qui peuvent être utilisées pour vous aider à résoudre des problèmes ou être envoyées au support technique.

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

Configuration du proxy HTTP

1. Sur la page **GESTION DE L'APPLIANCE**, faites défiler vers le bas jusqu'à **PARAMÈTRES DU PROXY HTTP** et cliquez sur **Modifier**.
2. Sélectionnez **Activé** pour activer l'utilisation des paramètres du proxy HTTP.
3. Entrez l'adresse du serveur proxy dans **Adresse du serveur proxy**.
4. Entrez le port du serveur proxy dans **Port du serveur proxy**.
5. Sélectionnez **Oui** pour utiliser les informations d'identification pour le proxy.
6. Si vous utilisez les informations d'identification pour le proxy, entrez le nom d'utilisateur dans **Nom d'utilisateur**.
7. Saisissez le mot de passe dans le champ **Mot de passe**.
8. Cliquez sur **Appliquer**.

Configuration des serveurs NTP (Network Time Protocol)

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

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

REMARQUE : La synchronisation de l'horloge d'OMIVV avec le serveur NTP dure quelques minutes.

REMARQUE : Si le portail d'administration OMIVV met beaucoup de temps à charger les informations, assurez-vous que les paramètres NTP sont corrects et que le serveur NTP est accessible pour la machine virtuelle OMIVV.

Configuration du mode de déploiement

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

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

Tableau 2. Configuration matérielle requise pour les modes de déploiement

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

Tableau 2. Configuration matérielle requise pour les modes de déploiement (suite)

Modes de déploiement	Nombre d'hôtes	Nombre de processeurs	Mémoire (Go)	Stockage minimal
Mode Très grand	Jusqu'à 2 000	12	32	95 Go

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

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

Pour intégrer le Pack de gestion OpenManage pour les opérations vRealize (vROPS) avec OMIVV, le mode de déploiement minimal requis est **Moyen**.

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

REMARQUE : Pendant le démarrage de l'appliance OMIVV, les ressources système allouées sont vérifiées par rapport au mode de déploiement défini. Si ces ressources système allouées sont insuffisantes pour le mode de déploiement défini, l'appliance OMIVV ne démarre pas sur l'écran de connexion. Pour démarrer l'appliance OMIVV, mettez-la hors tension, mettez à jour les ressources système pour les adapter au mode de déploiement défini existant, puis mettez l'appliance OMIVV sous tension.

Rétrogradation du mode de déploiement

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

Mise à niveau du mode de déploiement

1. Effacez le cache du navigateur avant de vous connecter au portail d'administration Dell.
2. Mettez l'appliance OMIVV sous tension.
3. Connectez-vous à la Console Administration.
4. Remplacez le mode de déploiement par le mode du niveau requis.

Surveillance étendue

Assurez-vous d'activer l'option Surveillance étendue pour prendre en charge OpenManage Management Pack for vRealize Operations Manager. Il est recommandé d'exécuter la surveillance étendue via le mode de déploiement « Moyen ».

Assurez-vous d'activer l'option Surveillance des traps SNMP pour prendre en charge les alertes SNMP pour OpenManage Management Pack for vRealize Operations Manager. Cela permet à l'utilisateur de surveiller l'état d'intégrité du serveur ou du châssis en temps réel.

1. Accédez à https://<ApplianceIP/hostname/>.
2. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
3. Sur la page **Gestion de l'appliance**, faites défiler l'affichage vers le bas jusqu'à **Surveillance étendue**.

4. Pour modifier les paramètres de surveillance étendue, cliquez sur **Modifier**.
5. En mode modifier, activez ou désactivez la surveillance étendue et la surveillance des traps SNMP, puis cliquez sur **Appliquer**.

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

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

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

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

Chargement d'un certificat HTTPS

Assurez-vous que le certificat utilise le format PEM.

Utilisez les certificats HTTPS pour sécuriser les communications avec l'appliance OMIVV et les systèmes hôtes ou vCenter. Pour configurer ce type de communications sécurisées, envoyez le certificat CSR à un signataire autorisé, puis téléchargez le certificat CSR résultant en utilisant la console d'administration. Il existe aussi un certificat par défaut qui est autosigné et qui peut être utilisé pour sécuriser les communications. Ce certificat est unique à chaque installation.

1. Sur la page **GESTION DE L'APPLIANCE**, cliquez sur **Charger le certificat** dans la zone **CERTIFICATS HTTPS**.
2. Cliquez sur **OK** dans la boîte de dialogue **CHARGER LE CERTIFICAT**.
3. Pour charger le certificat, cliquez sur **Parcourir**, puis sur **Charger**.
   Pour vérifier l'état, accédez à la **Console des événements** du client vSphere des vCenters enregistrés.

Lors du chargement du certificat, la Console Administration OMIVV cesse de répondre pendant une durée allant jusqu'à 3 minutes. Une fois que la tâche de téléchargement du certificat HTTPs est terminée, fermez la session de navigateur et accédez au portail d'administration dans une nouvelle session de navigateur.

Restauration du certificat HTTPS par défaut

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

Lors de la restauration du certificat, la Console Administration OMIVV cesse de répondre pendant une durée allant jusqu'à 3 minutes. Une fois la tâche de restauration de certificat HTTPs par défaut terminée, fermez la session du navigateur en cours et accédez au portail d'administration dans une nouvelle session.

Configuration des alertes globales

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

1. Accédez à https://<ApplianceIP/hostname/>.
2. Dans la boîte de dialogue **Connexion**, saisissez le mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DES ALERTES**. Pour entrer de nouveaux paramètres d'alertes vCenter, cliquez sur **Modifier**.
4. Saisissez les valeurs numériques dans les champs suivants :
   Par défaut, le nombre actuel d'alertes s'affiche.
   - **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**.

À propos de la console de machine virtuelle OMIVV

La console de machine virtuelle OMIVV se trouve dans le client vSphere sur une machine virtuelle. La console fonctionne en étroite association avec la console d'administration. Vous pouvez utiliser la console pour effectuer les tâches suivantes :

- Configurer les paramètres réseau
- Changer le mot de passe de l'appliance OMIVV
- Configurer le NTP et les paramètres du fuseau horaire local
- Redémarrer l'appliance OMIVV enregistrée.
- Réinitialiser l'appliance OMIVV aux paramètres d'usine
- Se connecter à l'aide d'un rôle en lecture seule
- Se déconnecter de la console

Ouverture d'une console de machine virtuelle OMIVV

Pour ouvrir la console de la machine virtuelle OMIVV, lancez la console Web ou à distance de l'appliance OMIVV.

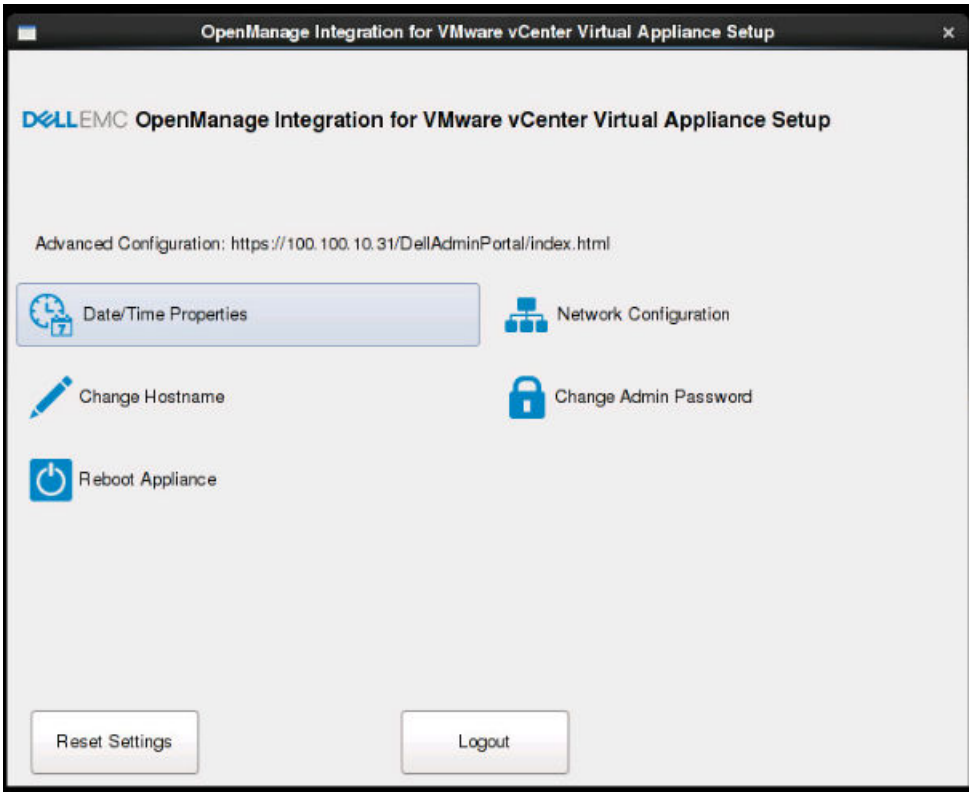
Après avoir ouvert la console de la machine virtuelle et saisi les informations d'identification (nom d'utilisateur : `admin` et mot de passe : mot de passe défini lors du déploiement de l'appliance), vous pouvez configurer la console.

Configuration de l'appliance OMIVV

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

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

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



REMARQUE : Lorsque l'appliance OMIVV n'est pas capable de récupérer une adresse IP du réseau (DHCP), `0.0.0.0` est l'adresse IP qui s'affiche. Pour résoudre ce problème, vous devez configurer manuellement l'IP statique.

a. Sous l'onglet **Date et heure**, cochez la case **Synchroniser la date et l'heure sur le réseau**. La case à cocher **Synchroniser la date et l'heure sur le réseau** n'est activée qu'après configuration réussie du NTP à l'aide du portail d'administration. Pour plus d'informations sur la configuration du NTP, voir Configuration des serveurs NTP (Network Time Protocol) , page 23.

b. Cliquez sur **Fuseau horaire** et sélectionnez le fuseau horaire applicable, puis cliquez sur **OK**.

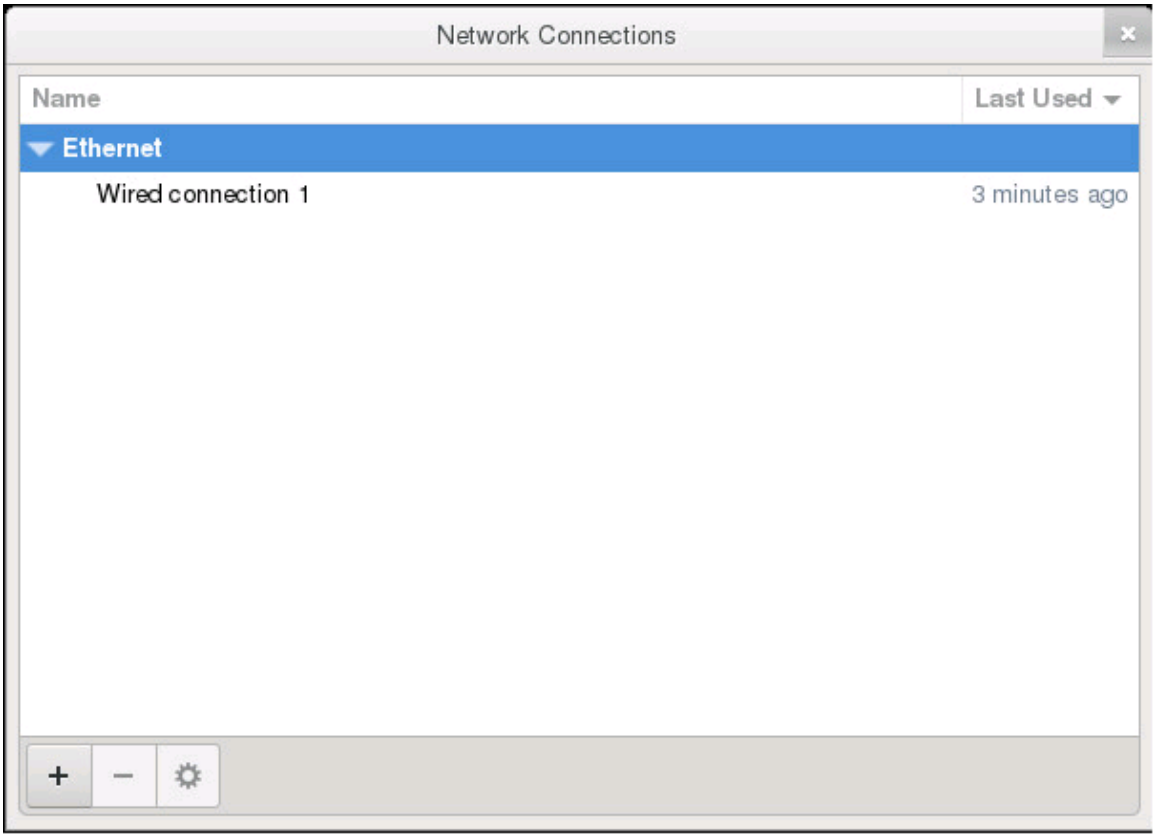
6. Pour configurer le réseau de l'appliance OMIVV, cliquez sur **Configuration réseau**.

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

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

   Si le réseau hors bande est accessible à l'aide du réseau vSphere, ne configurez pas deux adaptateurs réseau pour l'appliance OMIVV. Pour plus d'informations sur la configuration d'une deuxième carte réseau, voir Configuration de l'appliance OMIVV avec deux contrôleurs d'interface réseau (NIC) , page 29.

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



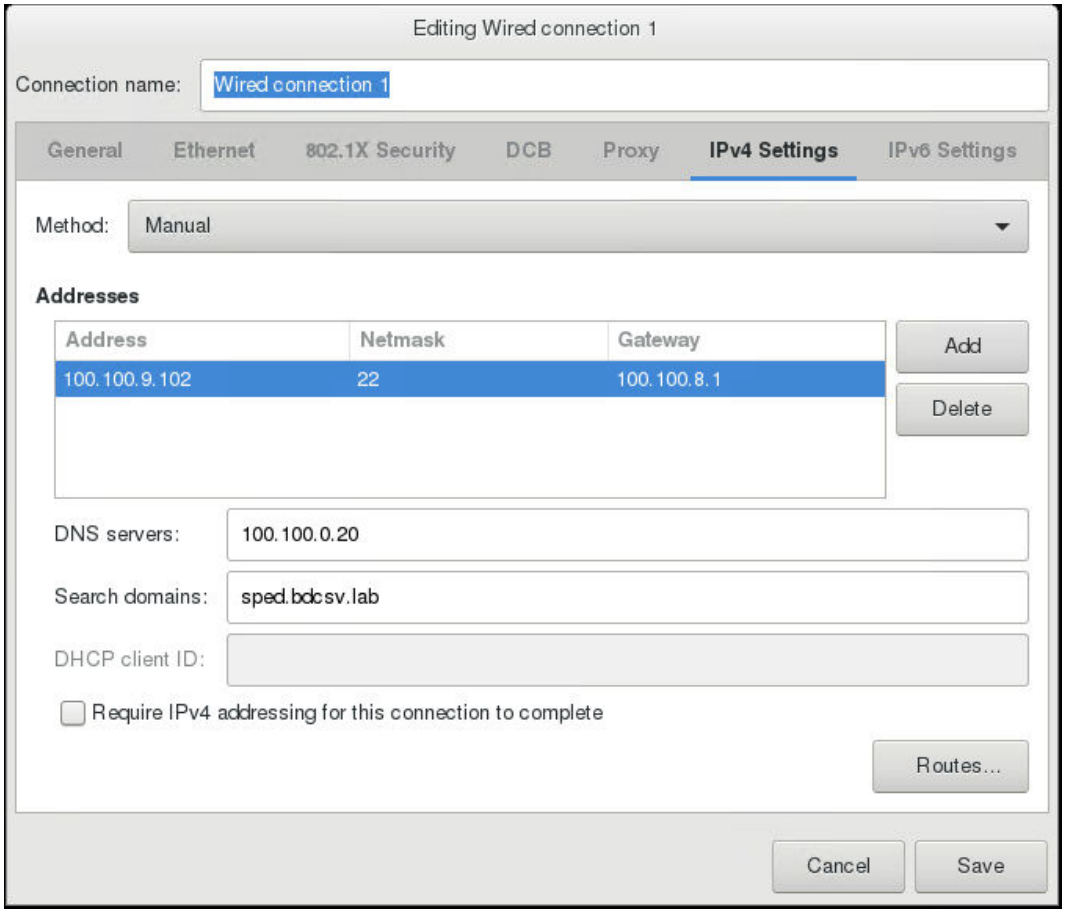
a. Cliquez sur l'onglet **Paramètres IPv4**, sélectionnez **Manuel** dans la liste déroulante **Méthode**, puis cliquez sur **Ajouter**.

   REMARQUE : Si vous sélectionnez Automatique (DHCP), ne saisissez aucune adresse IP car l'appliance OMIVV recevra automatiquement l'adresse IP via le serveur DHCP lors du prochain redémarrage.

b. Saisissez une adresse IP valide, un masque de réseau (au format CIDR (Classless Inter-Domain Routing)) et des informations de passerelle.
   Si vous saisissez une adresse IP dans le champ **Masque de réseau**, celle-ci est automatiquement convertie dans son format CIDR adapté.

c. Saisissez l'adresse IP du serveur DNS et les domaines à rechercher dans les champs **Serveurs DNS** et **Domaines de recherche** respectivement.

d. Cochez la case **Adressage IPv4 requis pour pouvoir établir cette connexion**, puis cliquez sur **Enregistrer**.



REMARQUE :

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

8. Pour modifier le nom d'hôte de l'appliance OMIVV, cliquez sur **Modifier le nom d'hôte**.
   a. Saisissez un nom d'hôte valide et cliquez sur **Mettre à jour le nom d'hôte**.

   REMARQUE : Si des serveurs vCenter sont déjà enregistrés avec l'appliance OMIVV, désenregistrez puis enregistrez de nouveau toutes les instances de vCenter. Pour plus d'informations, reportez-vous à la rubrique Gestion du désenregistrement et du réenregistrement dans le Guide d'installation.

9. Redémarrez l'appliance.

Configuration de l'appliance OMIVV avec deux contrôleurs d'interface réseau (NIC)

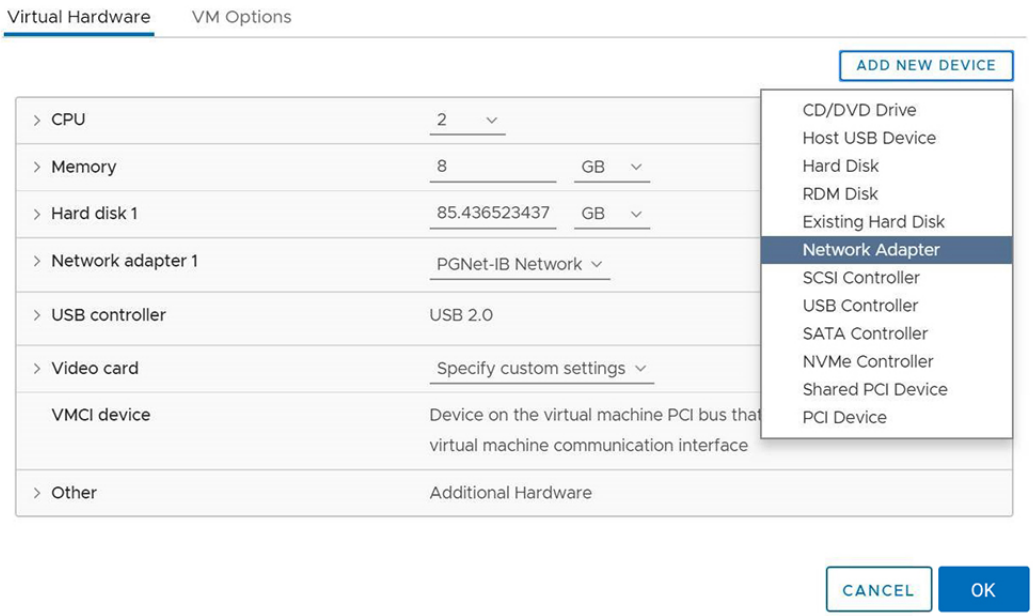
Pour gérer les serveurs Dell EMC dans votre environnement vSphere, OMIVV doit disposer d'un accès à la fois au réseau vSphere (vCenter et réseau de gestion ESXi), ainsi qu'au réseau hors bande (iDRAC, CMC et OME-Modular). Si le réseau vSphere et le réseau hors bande sont gérés comme des réseaux isolés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

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

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

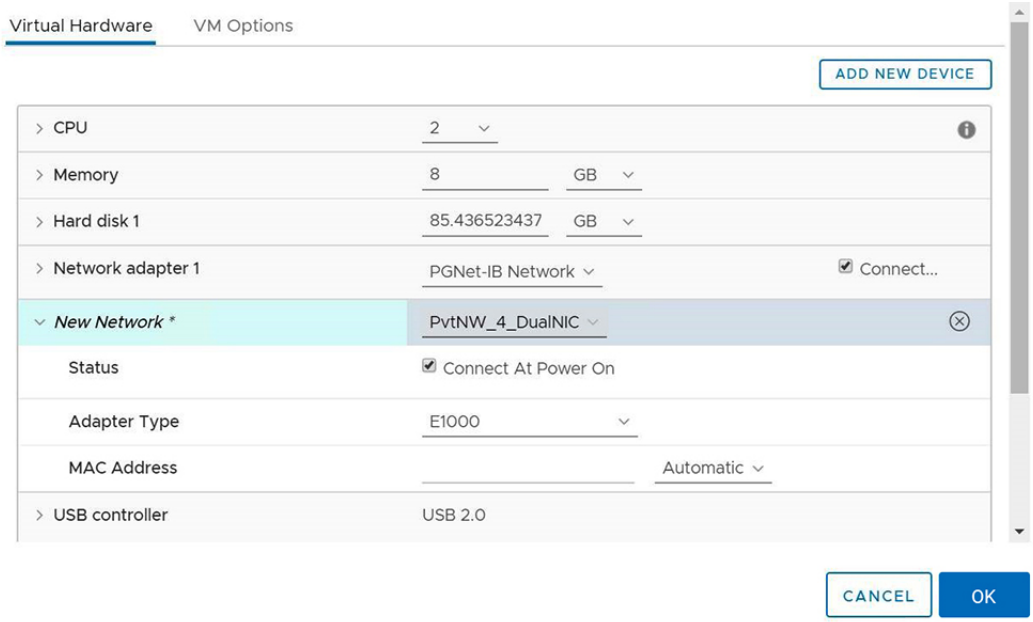
- Exigences DNS : OMIVV prend en charge la configuration DNS pour un seul réseau. Pour plus d'informations sur la configuration DNS, passez à l'étape 9 (b) de cette rubrique.

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



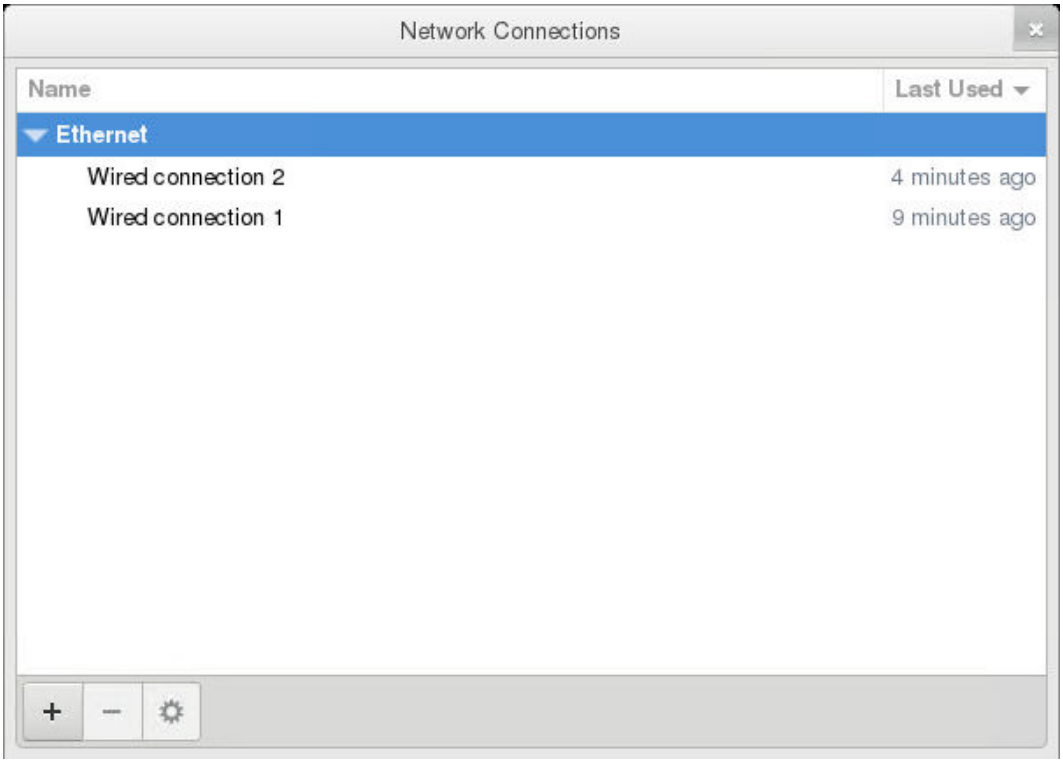
   a. Sélectionnez le réseau approprié pour la carte NIC, puis cochez la case **Connecter à la mise sous tension**.
   b. Sélectionnez l'adaptateur de type **VMXNET3** dans le menu déroulant.

   REMARQUE : OMIVV prend en charge les cartes NIC de type VMXNET3.



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

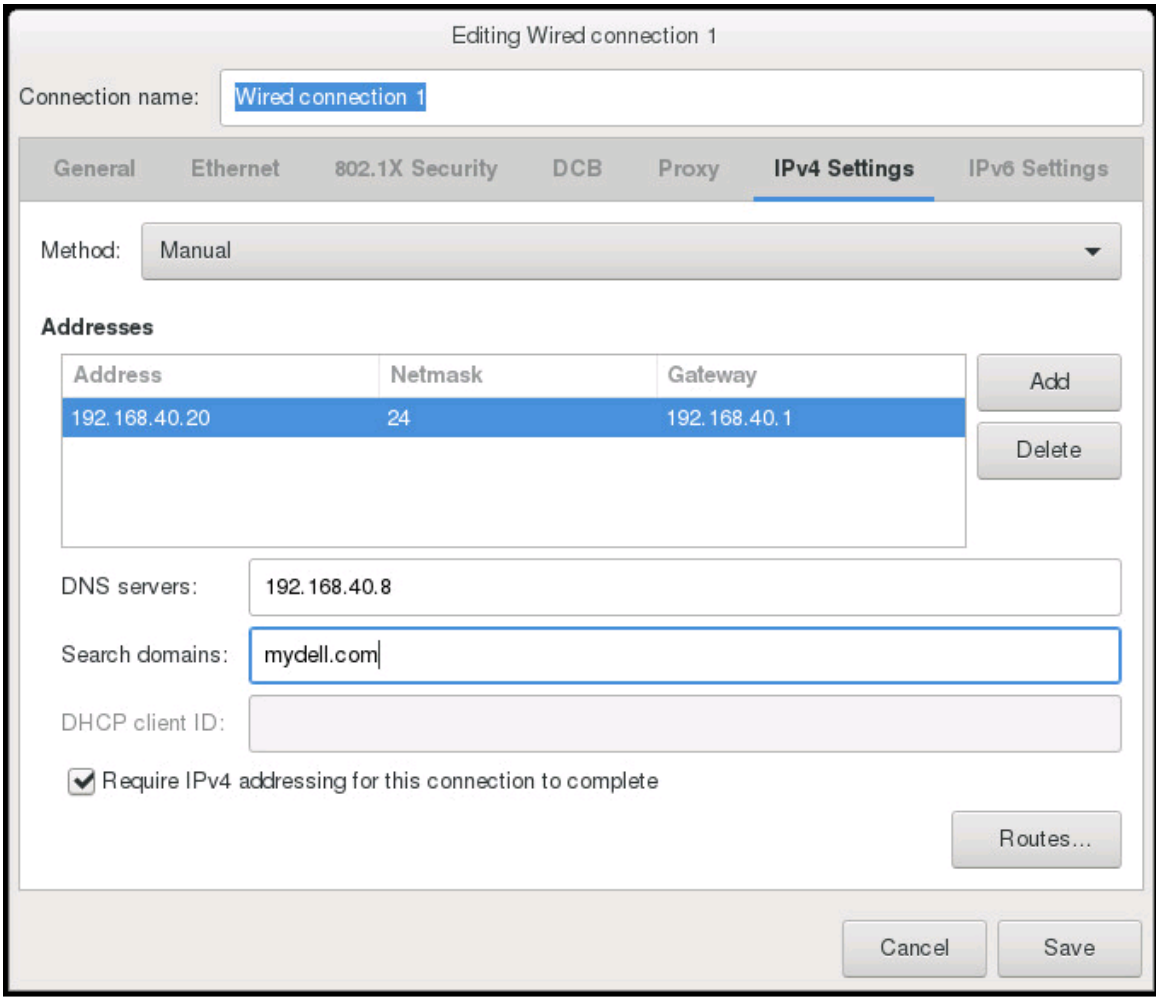
   La page **Connexions réseau** affiche deux cartes réseau.



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

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

   Assurez-vous de ne pas modifier l'adresse MAC par défaut qui est indiquée sous l'onglet **Ethernet**.
8. Cliquez sur l'onglet **Général**, puis cochez la case **Se connecter automatiquement à ce réseau lorsqu'il est disponible**.
9. Cliquez sur l'onglet **Paramètres IPv4** et procédez comme suit :



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

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

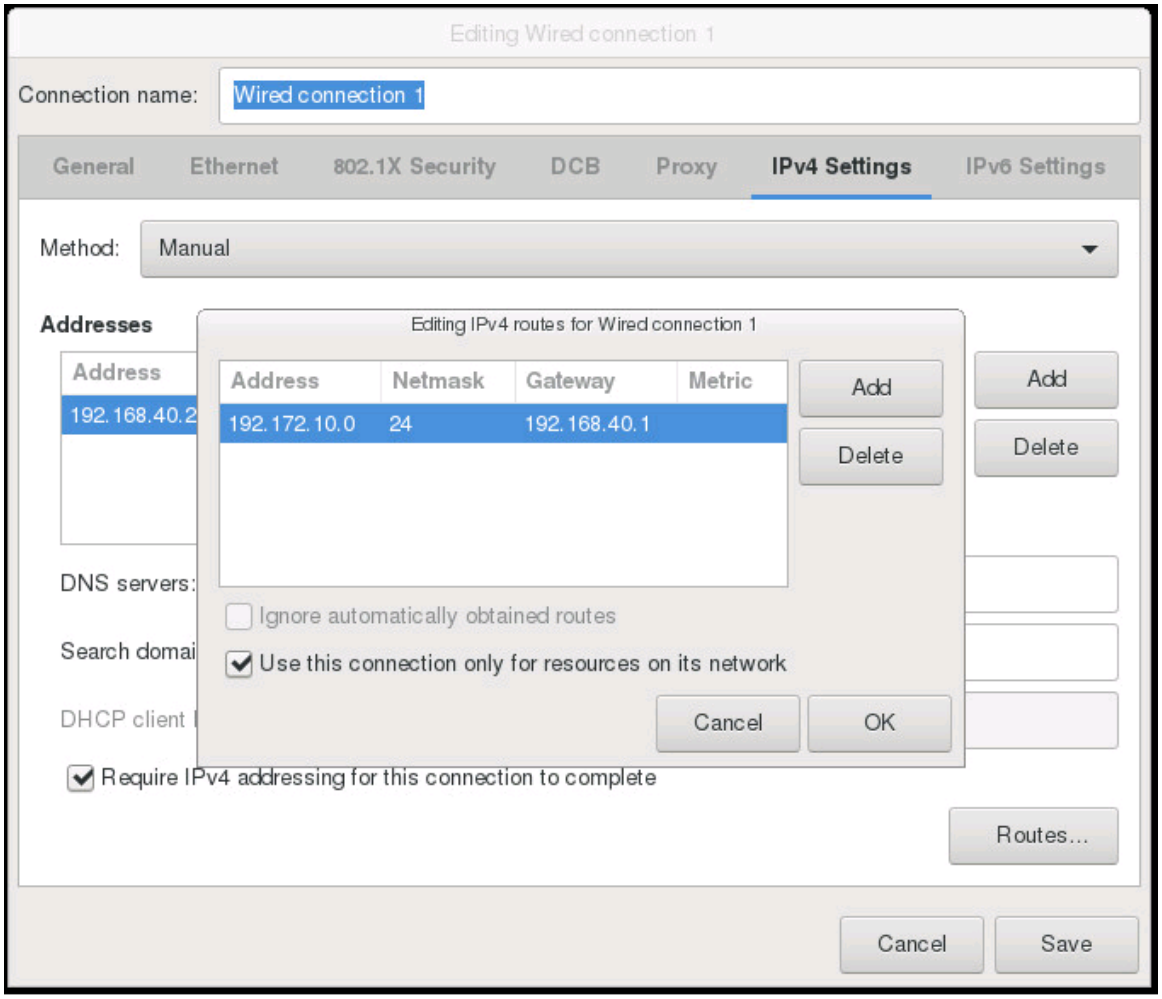
   Si le réseau vSphere et le réseau de gestion iDRAC sont gérés à l'aide du nom d'hôte ou du FQDN, le serveur DNS doit être configuré de manière à résoudre le nom d'hôte ou le FQDN des deux réseaux. Pour plus d'informations, consultez la documentation CentOS.

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

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

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

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



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

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

g. Cliquez sur **OK**.

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

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

Modification du mot de passe de l'appliance OMIVV

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

1. Ouvrez la console Web OMIVV.
2. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration pour VMware vCenter**, cliquez sur **Modifier le mot de passe Admin**.

   Suivez les instructions à l'écran pour définir le mot de passe.
3. Dans la zone de texte **Mot de passe actuel**, saisissez le mot de passe administrateur actuel.
4. Saisissez le nouveau mot de passe dans la zone de texte **Nouveau mot de passe**.

5. Saisissez une fois de plus le nouveau mot de passe dans la zone de texte **Confirmer le nouveau mot de passe**.
6. Cliquez sur **Modifier le mot de passe administrateur**.

Configuration du Network Time Protocol (NTP) et définition du fuseau horaire local

1. Ouvrez la console Web OMIVV.
2. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration pour VMware vCenter**, cliquez sur **Propriétés Date/Heure**.

   Assurez-vous de saisir les détails de NTP dans la console d'administration. Pour plus d'informations, voir Configuration des serveurs NTP (Network Time Protocol) , page 23.
3. Sous 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 un autre nom d'hôte ou une autre adresse IP du serveur NTP (si nécessaire), 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**.

Modification du nom d'hôte de l'appliance OMIVV

1. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration pour VMware vCenter**, cliquez sur **Modifier le nom d'hôte**.

   REMARQUE : Si des serveurs vCenter sont enregistrés avec l'appliance OMIVV, désenregistrez puis enregistrez de nouveau toutes les instances de vCenter.
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 la page du menu principal s'affiche.
4. Pour redémarrer l'appliance, cliquez sur **Redémarrer l'appliance**.

REMARQUE : Assurez-vous de mettre à jour manuellement toutes les références à l'appliance virtuelle sur son environnement, telles que le serveur de provisionnement dans l'iDRAC et Dell EMC Repository Manager (DRM).

Redémarrage de l'appliance OMIVV

1. Ouvrez la console Web OMIVV.
2. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration pour VMware vCenter**, cliquez sur **Redémarrer l'appliance**.
3. Pour redémarrer l'appliance, cliquez sur **Oui**.

Réinitialisation de l'appliance OMIVV sur les paramètres d'usine

1. Ouvrez la console Web OMIVV.
2. Dans l'utilitaire **Configuration de l'appliance virtuelle OpenManage Integration pour VMware vCenter**, cliquez sur **Réinitialiser les paramètres**.

   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 rétablir l'appliance, cliquez sur **Oui**.
   Si vous cliquez sur **Oui**, l'appliance OMIVV est rétablie sur les paramètres d'usine par défaut et tous les autres réglages et les données existantes sont supprimés.

   Une fois la réinitialisation des paramètres d'usine terminée, enregistrez de nouveau les vCenter sur l'appliance OMIVV.

REMARQUE : Lorsque les paramètres d'usine par défaut de l'appliance OMIVV sont rétablis, toutes les mises à jour que vous avez effectuées sur la configuration réseau sont conservées. Ces paramètres ne sont pas rétablis.

Rôle utilisateur en lecture seule

Il existe un rôle utilisateur non privilégié appelé « lecture seule » qui dispose d'un accès au shell à des fins de diagnostic. Cet utilisateur en lecture seule dispose de privilèges limités pour exécuter quelques commandes.

3

Suivi des hôtes et des châssis à l'aide du tableau de bord

Le tableau de bord affiche les éléments suivants :

- État de l'intégrité des hôtes et du châssis
- État de la garantie des hôtes et du châssis
- Informations de licence des hôtes et de vCenter
- État de conformité de la configuration des hôtes
- États des tâches planifiées à l'aide de OMIVV
- Serveurs sur matériel vierge disponibles pour le déploiement
- Références rapides aux fonctionnalités de OMIVV

Intégrité

La section **Intégrité** affiche l'intégrité de tous les châssis et hôtes gérés par OMIVV. Les hôtes qui s'affichent ici sont configurés à l'aide du même PSC (Platform Service Controller).

Le statut de chaque hôte et châssis est actualisé après l'achèvement d'une tâche de mesure d'intégrité périodique ou après un événement SNMP (déclenche la tâche de mesure d'intégrité pour l'hôte ou le châssis spécifique) de l'hôte et du châssis.

Par défaut, la tâche de mesure d'intégrité est exécutée toutes les heures. Les données affichées sont utilisées pour surveiller l'intégrité Proactive HA et la mise à jour de l'intégrité du serveur et du châssis sur le tableau de bord. Les détails de la tâche sont disponibles dans les journaux.

La liste suivante décrit les différents états des hôtes et des châssis :

- **Intègre** : affiche le nombre d'hôtes et de châssis qui fonctionnent normalement.
- **Avertissement** : affiche le nombre d'hôtes et de châssis qui nécessitent une action corrective, mais qui sont sans incidence immédiate sur le système.
- **Critique** : affiche le nombre d'hôtes et de châssis présentant des problèmes critiques sur un ou plusieurs composants. Ces problèmes doivent être résolus sans délai.
- **Inconnu** : affiche le nombre total d'hôtes et de châssis dont l'état est inconnu. L'hôte ou le châssis affiche un état inconnu lorsqu'il n'est pas accessible ou que son état d'intégrité est inconnu.

Pour afficher plus d'informations sur les hôtes, sur la page **Tableau de bord**, sous la section **Intégrité**, cliquez sur **AFFICHER L'HÔTE**.

Pour afficher plus d'informations sur le châssis, sur la page **Tableau de bord**, sous la section **Intégrité**, cliquez sur **AFFICHER LE CHÂSSIS**.

La garantie

Le nombre d'hôtes qui s'affichent dans cette catégorie de garantie indique les hôtes qui appartiennent aux serveurs vCenter configurés à l'aide du PSC (Platform Service Controller). Pour recevoir des informations sur la garantie de l'hôte et du châssis, assurez-vous d'avoir activé la notification d'expiration de la garantie sur la page **Paramètres**.

Pour un hôte disposant de plusieurs garanties ou de différentes garanties, par exemple, des garanties de type jour ouvré suivant (NBD) et pièces seulement (POW), OMIVV affiche le statut en fonction du type de garantie avec le plus petit nombre de jours encore couverts par la garantie.

La section **Garantie** fournit les informations suivantes sur les hôtes et les châssis :

- **Intègre** : affiche le nombre d'hôtes et de châssis pour lesquels le nombre de jours de garantie restants est supérieur au seuil d'avertissement.
- **Avertissement** : affiche le nombre d'hôtes et de châssis pour lesquels le nombre de jours de garantie restants est inférieur au seuil d'avertissement.

- **Critique** : affiche le nombre d'hôtes et de châssis pour lesquels le nombre de jours de garantie restants est inférieur au seuil critique.
- **Inconnu** : affiche le nombre d'hôtes et de châssis dont la garantie n'est pas connue.

Pour identifier les hôtes dont les états sont **Intègre**, **Avertissement**, **Critique** et **Inconnu**, procédez comme suit :

1. Accédez à **Hôtes et clusters**.
2. Pour afficher l'état d'intégrité de l'hôte au niveau du cluster, sélectionnez un cluster, puis cliquez sur **Surveiller** > **Informations sur le cluster OMIVV** > **Garantie**.
3. Pour afficher l'état d'intégrité de l'hôte au niveau du datacenter, sélectionnez un datacenter, puis cliquez sur **Surveiller** > **Informations sur le cluster OMIVV** > **Garantie**.

Licences

La section **Licences** comprend les informations suivantes :

- Nombre total de licences d'hôte et de vCenter
- Nombre de licences d'hôte et de vCenter disponibles
- Nombre de licences d'hôte et de vCenter en cours d'utilisation.

Pour acheter une licence, sur la page **Tableau de bord**, sous la section **Licences**, cliquez sur **ACHETER UNE LICENCE**.

Prêt pour le déploiement

Cette section ne s'applique qu'aux serveurs sur matériel vierge conformes, détectés à l'aide d'OMIVV. Pour déployer les serveurs sur matériel vierge, cliquez sur **DÉPLOYER**.

Conformité de la configuration

Cette section indique les hôtes qui font partie d'un cluster (associé au profil de cluster). Les hôtes qui s'affichent ici sont configurés à l'aide du même PSC (Platform Service Controller).

Pour afficher l'état de conformité de la configuration des hôtes, cliquez sur **AFFICHER LA CONFORMITÉ**.

Tâches

Cette section indique les tâches planifiées à l'aide d'OMIVV. Vous pouvez afficher les détails de la tâche uniquement pour les 7 derniers jours.

Le graphique circulaire affiche le nombre total de tâches définies sur les états suivants : **Réussite**, **En cours**, **Échec**, **Planifiée** et **Annulée**. Cliquez sur l'état d'une tâche pour filtrer les états de tâches dans le graphique circulaire.

Vous pouvez afficher le nombre de tâches suivantes définies sur **Réussite**, **En cours**, **Échec**, **Planifiée**et **Annulée** :

- Tâches de déploiement

  Pour plus d'informations, voir Tâches de déploiement , page 76.
- Tâches de mise à jour de firmware de l'hôte

  Pour plus d'informations, voir Tâches de mise à jour du firmware de l'hôte , page 78.
- Tâches de mise à jour de firmware du châssis

  Pour plus d'informations, voir Tâches de mise à jour du firmware du châssis , page 77.
- Tâches System Lockdown

  Pour plus d'informations, voir Tâches du mode de verrouillage du système , page 78.

Pour afficher l'état de toutes les tâches, cliquez sur **AFFICHER TOUTES LES TÂCHES**.

Références rapides

Cette section fournit des références rapides aux fonctions suivantes :

- Lancement de l'assistant de configuration initiale.

  Pour en savoir plus, voir Configuration initiale , page 90
- Profil d'identification d'hôte

  Pour en savoir plus, voir Profil d'identification d'hôte , page 39
- Gestion de la conformité

  Pour en savoir plus, voir Gestion de la conformité , page 71
- Profil d'identification de châssis

  Pour en savoir plus, voir Profil d'identification de châssis , page 44
- Profil de cluster

  Pour en savoir plus, voir Profil de cluster , page 52
- Déploiement

  Pour en savoir plus, voir Check-list de déploiement , page 65

4

Gestion des hôtes à l'aide du profil d'identification d'hôte

Profil d'identification d'hôte

Un profil d'identification d'hôte stocke les informations d'identification du contrôleur iDRAC et de l'hôte utilisées par OMIVV pour communiquer avec les serveurs. L'OMIVV gère les hôtes associés au profil d'identification d'hôte. Vous pouvez associer plusieurs serveurs à un même profil d'identification d'hôte.

L'hôte de châssis PowerEdge MX peut être géré à l'aide d'une seule adresse IP de gestion de châssis unifiée. Les hôtes présents dans un châssis PowerEdge MX avec une adresse IP iDRAC désactivée doivent être gérés à l'aide du profil d'identification du châssis. Pour gérer le châssis MX PowerEdge à l'aide d'un profil d'identification de châssis, voir Création d'un profil d'identification de châssis , page 44. Il vous est recommandé de gérer les hôtes de châssis PowerEdge MX avec une adresse IP iDRAC à l'aide du profil d'informations d'identification d'hôte pour obtenir des fonctionnalités OMIVV complètes.

Création du profil d'identification d'hôte

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

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

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

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification d'hôte**.
2. Sur la page **Profil d'identification d'hôte**, cliquez sur **CRÉER UN NOUVEAU PROFIL**.
3. Sur la page **Profil d'identification d'hôte** de l'Assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
4. Sur la page **Nom et informations d'identification**, effectuez les opérations suivantes :
   a. Saisissez le nom et la description du profil. Il n'est pas obligatoire de renseigner le champ de description.
   b. Dans la liste **Nom du vCenter**, sélectionnez une instance de vCenter sur laquelle vous souhaitez créer le profil d'identification d'hôte.
   c. Dans le champ **Informations d'identification**, saisissez les informations d'identification locales d'iDRAC ou AD.
      - Pour saisir les informations d'identification locales d'iDRAC, exécutez les tâches suivantes :
        - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur**. Le nom d'utilisateur est limité à 16 caractères.

          Pour plus d'informations sur la définition des noms d'utilisateur, consultez le *Guide de l'utilisateur de l'iDRAC* disponible sur le site **https://www.dell.com/support**.
        - Saisissez le mot de passe.

          Pour plus d'informations sur les caractères recommandés dans les noms d'utilisateur et mots de passe, reportez-vous au *Guide de l'utilisateur de l'iDRAC* disponible sur **https://www.dell.com/support**.
      - Pour télécharger et stocker le certificat iDRAC et le valider lors de toutes les connexions futures, cochez la case **Activer la vérification du certificat**.
      - Pour saisir les informations d'identification d'un iDRAC déjà configuré et activé pour AD, cochez la case **Utiliser Active Directory**.

        REMARQUE : Le compte iDRAC exige que l'utilisateur détienne des droits d'administration pour mettre à jour le firmware et déployer un système d'exploitation (SE).
        - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**.

Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur est limité à 256 caractères. Reportez-vous à la **documentation Microsoft Active Directory** pour connaître les conventions de nom d'utilisateur.

- Saisissez le mot de passe.

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

d. Dans le champ **Hôte racine**, saisissez les informations d'identification de l'hôte local ou AD.

Le nom d'utilisateur par défaut est root.

- Pour saisir les informations d'identification de l'hôte local, procédez comme suit :
  - Saisissez le mot de passe.

    Le mot de passe de l'hôte est requis uniquement pour les hôtes exécutant ESXi 6.5 U3 et les versions antérieures.

    Pour ignorer cette étape pour ESXi 6.7 et versions supérieures, assurez-vous que la case **Utiliser les informations d'identification de l'hôte** n'est pas cochée. Si un mot de passe est saisi pour l'hôte exécutant la version ESXi 6.7 et versions supérieures, le mot de passe est ignoré.

    Pour les hôtes exécutant la version ESXi 6.7 et versions supérieures, il est recommandé de ne pas saisir les informations d'identification ESXi. OMIVV peut associer l'iDRAC à son hôte ESXi, même si des informations d'identification d'hôte incorrectes ont été saisies.

- Pour saisir les informations d'identification des hôtes déjà configurés et activés pour AD, cochez la case **Utiliser Active Directory**.
  - Saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**. Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur est limité à 256 caractères. Reportez-vous à la **documentation Microsoft Active Directory** pour connaître les conventions de nom d'utilisateur.
  - Saisissez le mot de passe.

- Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, cochez la case **Activer la vérification du certificat**.

5. Cliquez sur **Suivant**.
   La page **Sélectionner les hôtes** s'affiche.
6. Sur la page **Sélectionner les hôtes**, développez l'arborescence et sélectionnez les hôtes, puis cliquez sur **OK**.
   - Pour ajouter ou supprimer des hôtes de la page **Hôtes associés**, cliquez sur **AJOUTER UN HÔTE**.

     REMARQUE : N'ajoutez pas un serveur PowerEdge MX avec un iDRAC IPv4 désactivé à un profil d'identification d'hôte. Ces serveurs sont gérés à l'aide d'un profil d'identification de châssis.

   Les hôtes sélectionnés sont affichés sur la page **Hôtes associés**.
7. Pour tester la connexion, sélectionnez un ou plusieurs hôtes, puis cliquez sur **DÉMARRER LE TEST**.
   Il est recommandé de tester la connexion pour tous les hôtes configurés.

   Lors du test de connexion, OMIVV active le service WBEM, puis le désactive après la récupération de l'adresse IP de l'iDRAC pour les hôtes exécutant ESXi 6.5 et versions supérieures.

   REMARQUE : Une fois que vous avez saisi des informations d'identification valides, l'opération de test de la connexion peut échouer pour l'hôte et un message s'affiche indiquant que des informations d'identification non valides ont été saisies. Ce problème survient si ESXi bloque l'accès. Plusieurs tentatives de connexion à ESXi à l'aide d'informations d'identification incorrectes vous empêchent d'accéder à ESXi pendant 15 minutes. Patientez 15 minutes, puis réessayez.

   - Pour arrêter le processus de test de connexion, cliquez sur **ANNULER LE TEST**.

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

Modification du profil d'identification d'hôte

Vous pouvez modifier les informations d'identification de plusieurs profils d'identification d'hôte à la fois.

1. Sur la page **Nom et références**, effectuez les opérations suivantes :

a. Modifier le nom du profil et sa description.
b. Dans le champ **Informations d'identification**, modifiez les informations d'identification locales d'iDRAC ou AD.
   - Pour modifier les informations d'identification locales d'iDRAC, exécutez les tâches suivantes :
     - Modifiez un nom d'utilisateur dans la zone **Nom d'utilisateur**. Le nom d'utilisateur est limité à 16 caractères.

       Pour plus d'informations sur la définition des noms d'utilisateur, consultez le *Guide de l'utilisateur de l'iDRAC* disponible sur le site **dell.com/support**.
     - Modifiez le mot de passe.
     - Pour télécharger et stocker le certificat iDRAC et le valider lors de connexions futures, cochez la case **Activer la vérification du certificat**.
   - Pour modifier les informations d'identification d'un iDRAC déjà configuré et activé pour AD, cochez la case **Utiliser Active Directory**.

     REMARQUE : Le compte iDRAC exige que l'utilisateur détienne des droits d'administration pour mettre à jour le firmware et déployer un système d'exploitation (SE).
     - Modifiez le nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**.

       Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur est limité à 256 caractères. Pour plus d'informations sur la définition du nom d'utilisateur, voir la *documentation Microsoft Active Directory*.
     - Saisissez le mot de passe.
     - Pour télécharger et stocker le certificat iDRAC et le valider lors de toutes les connexions futures, cochez la case **Activer la vérification du certificat**.

c. Dans le champ **Hôte racine**, modifiez les informations d'identification de l'hôte local ou AD.
   - Pour saisir les informations d'identification de l'hôte local, procédez comme suit :

     Le nom d'utilisateur par défaut est root.
     - Saisissez le mot de passe.

       Le mot de passe de l'hôte est requis uniquement pour les hôtes exécutant ESXi 6.5 U3 et les versions antérieures.

       Pour ignorer cette étape pour ESXi 6.7 et versions supérieures, assurez-vous que la case **Utiliser les informations d'identification de l'hôte** n'est pas cochée. Si un mot de passe est saisi pour l'hôte exécutant la version ESXi 6.7 et versions supérieures, le mot de passe est ignoré.

       Pour les hôtes exécutant la version ESXi 6.7 et les versions supérieures, il est recommandé de ne pas saisir les informations d'identification ESXi. OMIVV peut associer l'iDRAC à son hôte ESXi, même si des informations d'identification d'hôte incorrectes ont été saisies.
   - Pour modifier les informations d'identification des hôtes déjà configurés et activés pour AD, cochez la case **Utiliser Active Directory**.
     - Modifiez le nom d'utilisateur dans la zone **Nom d'utilisateur Active Directory**.

       Saisissez le nom d'utilisateur dans l'un des formats suivants : `domain\username` ou `username@domain`. Le nom d'utilisateur est limité à 256 caractères. Reportez-vous à la section *Documentation Microsoft Active Directory* pour connaître les conventions de nom d'utilisateur.
     - Modifiez le mot de passe.
   - Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, cochez la case **Activer la vérification du certificat**.

2. Cliquez sur **Suivant**.
   La page **Hôtes associés** s'affiche.
3. Pour ajouter ou supprimer les hôtes de la liste d'hôtes associés, sur la page **Hôtes associés**, cliquez sur **AJOUTER UN HÔTE**.

   REMARQUE : N'ajoutez pas un serveur PowerEdge MX avec un iDRAC IPv4 désactivé à un profil d'identification d'hôte. Ces serveurs sont gérés à l'aide d'un profil d'identification de châssis.

   Les hôtes sélectionnés sont affichés sur la page **Hôtes associés**.
4. Pour tester la connexion, sélectionnez un ou plusieurs hôtes, puis cliquez sur **DÉMARRER LE TEST**. Il est recommandé de tester la connexion pour tous les hôtes configurés.

   REMARQUE : Une fois que vous avez saisi des informations d'identification valides, l'opération de test de la connexion peut échouer pour l'hôte et un message s'affiche indiquant que des informations d'identification non valides ont été saisies. Ce

problème survient si ESXi bloque l'accès. Plusieurs tentatives de connexion à ESXi à l'aide d'informations d'identification incorrectes vous empêchent d'accéder à ESXi pendant 15 minutes. Patientez 15 minutes, puis réessayez.

- Pour arrêter les tests de connexion, cliquez sur **ANNULER LE TEST**.

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

Lors du test de connexion, OMIVV active le service WBEM, puis le désactive après la récupération de l'adresse IP de l'iDRAC pour les hôtes exécutant ESXi 6.5 et versions ultérieures.

5. Cliquez sur **Terminer**.

REMARQUE : Les champs Date de modification et Dernière modification par comprennent les modifications que vous effectuez via l'interface vSphere Client pour un profil d'identification de l'hôte. Toute modification apportée par l'appliance OMIVV aux profils d'identification d'hôte respectifs n'affecte pas ces deux champs.

Affichage du profil d'identification d'hôte

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification d'hôte**.
   Un tableau affiche tous les profils d'identification d'hôte ainsi que les informations suivantes :
   - **Nom du profil** : nom du profil d'identification d'hôte
   - **Description** : description du profil, le cas échéant
   - **vCenter** : FQDN ou nom d'hôte, ou adresse IP du serveur vCenter associé
   - **Hôtes associés** : hôtes associés au profil d'identification d'hôte. Si plusieurs hôtes sont associés, utilisez l'icône Développer pour tous les afficher.
   - **Vérification du certificat iDRAC** : indique si le certificat iDRAC est vérifié lors de la création d'un profil d'identification d'hôte.
   - **Vérification du certificat racine de l'hôte** : indique si le certificat racine de l'hôte est vérifié lors de la création d'un profil d'identification d'hôte.
   - **Date de création** : date à laquelle le profil d'identification d'hôte est créé.
   - **Date de modification** : date à laquelle le profil d'identification d'hôte est modifié.
   - **Dernière modification par** : détails sur l'utilisateur qui a modifié le profil d'identification d'hôte.

   REMARQUE : Si l'hôte PowerEdge MX est géré à l'aide du profil d'identification du châssis, OMIVV indique qu'il est associé à un profil d'identification de châssis. Pour plus d'informations, voir Affichage du profil d'identification de châssis , page 46.
2. Si vous souhaitez supprimer ou ajouter les noms de colonnes dans l'Assistant, cliquez sur .
   Par défaut, les colonnes **Date de modification** et **Dernière modification** ne sont pas sélectionnées. Pour sélectionner ces colonnes, cliquez sur .
3. Pour exporter les informations du profil d'identification d'hôte, cliquez sur .

Test du profil d'identification d'hôte

À l'aide de la fonction de test du profil d'identification, vous pouvez tester les informations d'identification de l'hôte et de l'iDRAC. Il vous est recommandé de sélectionner tous les hôtes.

1. Sur la page d'accueil d'OMIVV, sélectionnez un profil d'identification d'hôte ayant associé les hôtes, puis cliquez sur **TEST**.
   La page **Tester le profil d'identification d'hôte** s'affiche.
2. Sélectionnez tous les hôtes associés et cliquez sur **DÉMARRER LE TEST**.
   a. Pour arrêter les tests de connexion, cliquez sur **ANNULER LE TEST**.

   Les résultats du test de connexion pour les identifiants de l'iDRAC et de l'hôte s'affichent.

Suppression d'un profil d'identification d'hôte

Veillez à ne pas supprimer de profil d'identification d'hôte associé à un hôte lorsqu'une tâche d'inventaire, de garantie ou de déploiement est en cours d'exécution.

OMIVV ne gère pas les hôtes qui font partie du profil d'identification d'hôte que vous avez supprimé, tant que ces hôtes ne sont pas ajoutés à un autre profil d'identification d'hôte.

1. Sur la page **Profil d'identification d'hôte**, sélectionnez un profil et cliquez sur **SUPPRIMER**.
2. Lorsque le programme vous invite à confirmer, cliquez sur **SUPPRIMER**.
   Le profil sélectionné est supprimé de la liste Profil d'identification d'hôte.

5

Gestion des châssis à l'aide d'un profil d'identification de châssis

Profil d'identification de châssis

Un profil d'identification de châssis stocke les informations d'identification du châssis utilisées par OMIVV pour communiquer avec le châssis. OMIVV gère et surveille les châssis qui sont associés à un profil d'identification de châssis. Vous pouvez affecter plusieurs châssis à un même profil d'identification de châssis.

L'hôte de châssis PowerEdge MX peut être géré à l'aide d'une seule adresse IP de gestion de châssis unifiée. Les hôtes présents dans un châssis PowerEdge MX avec une adresse IP iDRAC désactivée doivent être gérés à l'aide du profil d'identification du châssis. Il vous est recommandé de gérer les hôtes de châssis PowerEdge MX avec une adresse IP iDRAC à l'aide du profil d'informations d'identification d'hôte pour obtenir des fonctionnalités OMIVV complètes. Pour plus d'informations sur la gestion des châssis MX, voir Gestion d'un châssis MX PowerEdge , page 117.

Création d'un profil d'identification de châssis

- Pour créer un profil d'identification de châssis, vous devez disposer des privilèges suivants :
  - Châssis M1000e, VRTX et FX2 : lecture et définition d'une destination d'interruption SNMP
  - Châssis MX PowerEdge : administrateur
- Avant d'utiliser les informations d'identification Active Directory (AD) pour un profil d'identification d'hôte, assurez-vous que :
  - Le compte d'utilisateur existe dans AD.
  - CMC ou OME-Modular est configuré pour l'authentification basée sur Active Directory.
- Pour les châssis PowerEdge MX, assurez-vous que vous disposez d'au moins un hôte MX dans le vCenter enregistré pour que le test de connexion réussisse.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification de châssis** > **CRÉER UN NOUVEAU PROFIL**.
2. Sur la page **Profil d'identification de châssis** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Sur la page **Nom et références**, effectuez les opérations suivantes :
   a. Saisissez le nom et la description du profil. La description est facultative.
   b. 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) ou à OpenManage Enterprise-Modular (OME-Modular).
   c. Dans la zone de texte **Mot de passe**, entrez le mot de passe.
   d. Dans la zone de texte **Vérifier le mot de passe**, saisissez le même mot de passe que vous avez saisi dans la zone de texte **Mot de passe**. Les mots de passe doivent correspondre.
4. Sur la page **Sélectionner le châssis**, sélectionnez un seul châssis ou plusieurs châssis à l'aide des cases à cocher situées en regard de la colonne **IP/nom de l'hôte**, puis cliquez sur **OK**.
   Le châssis sélectionné est affiché sur la page **Châssis associés**. Pour ajouter ou retirer le châssis de la liste des châssis associés, cliquez sur **Ajouter un châssis**.

   Si le châssis sélectionné est déjà associé à un profil d'identification de châssis, le message suivant s'affiche :

   Si vous sélectionnez un châssis actuellement associé à un autre profil, le châssis du profil d'identification du châssis sera supprimé. Un profil d'identification de châssis sans châssis associé sera supprimé.

   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.

   Le test de connexion s'exécute automatiquement pour le châssis sélectionné.

Le test de connexion s'exécute automatiquement :

- La première fois qu'un châssis est sélectionné.
- Lorsque vous modifiez les informations d'identification
- Si le châssis est de nouveau sélectionné

Le résultat du test (**Réussite** ou **Échec**) s'affiche dans la section **Résultats du test**. Pour tester la connectivité du châssis manuellement, sélectionnez le châssis, puis cliquez sur **DÉMARRER LE TEST**.

Pour un châssis PowerEdge MX configuré avec un groupe MCM, il vous est recommandé de gérer tous les châssis maîtres et membres à l'aide du châssis maître. L'opération de test de la connexion du châssis membre échoue et le résultat du test est défini sur **Échec**. La liaison IP du châssis principal s'affiche. Cliquez sur le lien IP du châssis principal pour découvrir le groupe MCM complet.

5. Cliquez sur **TERMINER**.

   Assurez-vous que vous disposez d'au moins un châssis validé pour terminer les tâches de l'Assistant. Seul un châssis validé correctement peut être associé à un profil d'identification de châssis.

   Pour ajouter le châssis PowerEdge MX, voir Ajout d'un châssis PowerEdge MX , page 118.

Modification d'un profil d'identification de châssis

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification de châssis**.
2. Sur la page **Profil d'identification de châssis**, cliquez sur **MODIFIER**.
3. Sur la page **Nom et références**, effectuez les opérations suivantes :
   a. Modifier le nom du profil et sa description. La description est facultative.
   b. Dans la zone de texte **Nom d'utilisateur**, modifiez le nom d'utilisateur doté des droits d'administrateur, généralement utilisé pour se connecter au contrôleur CMC (Chassis Management Controller) ou à OpenManage Enterprise-Modular (OME-Modular).
   c. Dans la zone de texte **Mot de passe**, entrez le mot de passe.

      Si vous ne renseignez pas le champ du mot de passe, OMIVV utilise le mot de passe saisi lors de la création du flux de travail.
   d. Dans la zone de texte **Vérifier le mot de passe**, saisissez le même mot de passe que vous avez saisi dans la zone de texte **Mot de passe**. Les mots de passe doivent correspondre.
4. Sur la page **Sélectionner le châssis**, sélectionnez ou supprimez le châssis à l'aide des cases à cocher situées en regard de la colonne **IP/nom de l'hôte**, puis cliquez sur **OK**.
   Le châssis sélectionné est affiché sur la page **Châssis associés**. Pour ajouter ou retirer le châssis de la liste des châssis associés, cliquez sur **Ajouter un châssis**.

   Si le châssis sélectionné est déjà associé à un profil d'identification de l'hôte, le message suivant s'affiche :

   Si vous sélectionnez un châssis actuellement associé à un autre profil, le châssis du profil d'identification du châssis sera supprimé. Un profil d'identification de châssis sans châssis associé sera supprimé.

   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.

   Le test de connexion s'exécute automatiquement pour le châssis sélectionné.

   Le test de connexion s'exécute automatiquement :

   - La première fois qu'un châssis est sélectionné.
   - Lorsque vous modifiez les informations d'identification
   - Si le châssis est de nouveau sélectionné

   Le résultat du test (**Réussite** ou **Échec**) s'affiche dans la section **Résultats du test**. Pour tester la connectivité du châssis manuellement, sélectionnez le châssis, puis cliquez sur **DÉMARRER LE TEST**.

   Pour un châssis PowerEdge MX configuré avec un groupe MCM, Dell EMC recommande de gérer le châssis maître et tous les châssis membres à l'aide du châssis maître. L'opération de test de la connexion du châssis membre échoue et le résultat du test indique l'état Échec. La liaison IP du châssis principal s'affiche. Cliquez sur le lien IP du châssis principal pour découvrir le groupe MCM complet.

   REMARQUE : Si les hôtes ne se trouvent pas dans les vCenters enregistrés associés au châssis PowerEdge MX ajouté, le test de connexion échoue pour le châssis.
5. Cliquez sur **TERMINER**.

   Assurez-vous que vous disposez d'au moins un châssis validé pour terminer les tâches de l'Assistant. Seul un châssis validé correctement peut être associé à un profil d'identification de châssis.

Pour ajouter un châssis PowerEdge MX, voir Ajout d'un châssis PowerEdge MX , page 118.

Affichage du profil d'identification de châssis

Après avoir créé un ou plusieurs profils d'identification de châssis, vous pouvez afficher le châssis et le châssis associé sur la page Profil d'identification de châssis.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification de châssis**.

   Un tableau affiche tous les profils d'identification de châssis et comprend les informations suivantes :

   - **Nom du profil** : nom du profil d'identification de châssis
   - **Description** : description du profil
   - **Adresse IP/Nom de l'hôte du châssis** : adresse IP du châssis ou lien du nom de l'hôte.

     Pour un groupe MCM (Multi-chassis Management), le châssis maître () et le châssis membre () sont répertoriés dans la hiérarchie.

     REMARQUE : Dans le cas d'un châssis MX PowerEdge dans une configuration MCM, OMIVV gère tous les châssis maîtres et membres à l'aide du châssis maître uniquement. Tous les châssis maîtres et membres sont associés au même profil d'identification de châssis auquel le châssis maître est associé.

     Dans le cas d'un châssis membre dans un groupe MCM (IPv4 est désactivé), une adresse IPv4 du châssis maître s'affiche. Le numéro de série du châssis membre s'affiche également entre parenthèses.
   - **Numéro de série du châssis** : ID unique attribué à un châssis.
   - **Date de modification** : date à laquelle le profil d'identification le châssis a été modifié.
2. Les informations suivantes sur les hôtes associés sont affichées dans la partie inférieure de la grille :

   - **Nom du profil**
   - **Hôtes associés**
   - **Numéro de série**
   - **Adresse IP/Nom d'hôte du châssis**
   - **Numéro de série du châssis**
3. Pour exporter les informations du profil d'identification de châssis, cliquez sur  .

Test d'un profil d'identification de châssis

À l'aide de la fonctionnalité de test des profils d'identification de châssis, vous pouvez tester les informations d'identification d'un châssis associé au profil d'identification de châssis. Il vous est recommandé de sélectionner tous les châssis.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification de châssis**.
2. Sélectionnez un profil d'identification de châssis, puis cliquez sur **TESTER**.
3. Sur la page **Tester le profil d'identification de châssis**, sélectionnez le châssis associé, puis cliquez sur **COMMENCER LE TEST**.
   a. Pour arrêter les tests de connexion, cliquez sur **ANNULER LE TEST**.

   Le résultat du test s'affiche dans la colonne **Résultat du test**.

Suppression d'un profil d'identification de châssis

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

Si le profil d'identification du châssis est supprimé, OMIVV ne surveille pas les châssis présents dans le profil d'identification du châssis supprimé, tant que vous n'avez pas ajouté le châssis à un autre profil d'identification du châssis.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil d'identification de châssis** > **SUPPRIMER**.
2. Sélectionnez un profil d'identification de châssis que vous souhaitez supprimer.
3. Lorsque le programme vous invite à confirmer, cliquez sur **SUPPRIMER**.

Si tous les châssis associés à un profil d'identification de châssis sont supprimés ou déplacés vers d'autres profils, un message de confirmation de la suppression s'affiche. Le message indique que le profil d'identification de châssis n'est associé à aucun châssis et qu'il a été supprimé.

Pour supprimer le profil d'identification de châssis, cliquez sur **OK** dans le message de confirmation de suppression.

6

Gestion des logithèques de micrologiciels et de pilotes à l'aide du profil de logithèque

Profil de logithèque

Un profil de logithèque vous permet de créer et de gérer des logithèques de pilotes ou de firmwares.

Vous pouvez utiliser les profils de logithèque de firmwares et de pilotes pour :

- Mettre à jour le firmware des hôtes
- Mettre à jour le pilote pour les hôtes qui font partie des clusters vSAN.
- Créer un profil de cluster et une configuration de base des clusters.

Les catalogues de firmwares OMIVV par défaut sont les suivants :

- **Catalogue par défaut Dell EMC** : profil de logithèque de firmwares créé en usine qui utilise le catalogue Dell EMC Online pour obtenir les dernières informations sur le firmware. Si l'appliance n'a pas de connexion Internet, modifiez cette logithèque de sorte qu'elle pointe vers un partage local basé sur CIFS ou NFS ou HTTP ou HTTPS. Pour plus d'informations sur la modification de ce catalogue, voir Modification ou personnalisation du catalogue Dell par défaut , page 50.

  Vous pouvez sélectionner Catalogue par défaut Dell EMC comme catalogue par défaut pour mettre à jour le firmware des hôtes vSphere qui ne sont pas associés à un profil de cluster.
- **Catalogue de piles MX validées** : profil de logithèque de firmwares créé en usine qui utilise le catalogue Dell EMC en ligne pour obtenir les informations sur le firmware validées pour le châssis MX et ses traîneaux correspondants. Pour plus d'informations sur la modification de ce catalogue, voir Modification d'un catalogue de piles MX validé , page 50. Pour plus d'informations sur le catalogue de piles MX validé, reportez-vous au livre blanc technique disponible ici : mise à jour de firmware MX7000.

  REMARQUE : Vous ne pouvez pas utiliser le catalogue par défaut Dell EMC et les profils de logithèque du catalogue de piles MX validé pour effectuer la configuration de base des clusters vSAN.

Création d'un profil de logithèque

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de logithèque**.
2. Sur la page **Profil de logithèque** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Sur la page **Nom et description du profil**, saisissez le nom et la description du profil. Le champ de description est facultatif et limité à 255 caractères.
4. Cliquez sur **SUIVANT**.
   La page **Paramètres du profil** s'affiche.
5. Sur la page **Paramètres du profil**, sélectionnez **firmware** ou **Pilote**.

   Ce qui suit s'applique au profil de logithèque de pilotes :

   - Un profil de logithèque de pilotes peut posséder un maximum de 10 pilotes. Si vous avez plus de fichiers, la sélection du pilote est aléatoire.
   - Seuls les lots de pilotes hors ligne (fichiers .zip) sont utilisés.
   - Téléchargez et extrayez les lots de pilote hors ligne (fichiers .zip) et enregistrez-les à l'emplacement partagé en fournissant le chemin complet de l'emplacement partagé. OMIVV crée automatiquement le catalogue dans l'appliance OMIVV. Les lots de pilotes sont disponibles sur https://my.vmware.com/web/vmware/downloads
   - OMIVV nécessite un accès en écriture au système de fichiers CIFS ou au NFS.
   - Les fichiers contenus dans les sous-dossiers sont ignorés.
   - Les fichiers dont la taille dépasse 10 Mo sont ignorés.
   - La logithèque de pilotes ne s'applique qu'aux clusters vSAN.

6. Dans la zone **Emplacement de partage de logithèque**, exécutez les tâches suivantes :
   a. Saisissez l'emplacement du partage de logithèque (NFS ou CIFS).
   b. Pour CIFS, saisissez les informations d'identification.

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

      REMARQUE : Si le partage SMB 1.0 est utilisé pour la logithèque de pilotes, ajoutez le séparateur de fichiers à la fin du chemin du répertoire.

7. Pour valider le chemin du catalogue et les informations d'identification, cliquez sur **DÉMARRER LE TEST**.

   Pour continuer la création d'un profil de logithèque, vous devez compléter ce processus de validation.

   Les résultats du test de connexion s'affichent.
8. Cliquez sur **SUIVANT**.
   La page **Synchroniser avec l'emplacement de la logithèque** s'affiche.
9. Cliquez sur **SUIVANT**.
   La page **Récapitulatif** s'affiche. Elle contient les informations concernant le profil de logithèque.
10. Cliquez sur **TERMINER**.
    Après avoir créé le catalogue, le téléchargement et l'analyse du catalogue sont lancés, 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 de firmware.

Modification d'un profil de logithèque

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil de logithèque** > **MODIFIER**.
2. Sur la page **Nom et description du profil**, modifiez le nom et la description du profil, puis cliquez sur **SUIVANT**.
3. Sur la page **Paramètres du profil**, sélectionnez **firmware** ou **Pilote**.

   Ce qui suit s'applique au profil de logithèque de pilotes :

   - Un profil de logithèque de pilotes peut posséder un maximum de 10 pilotes. Si vous avez plus de fichiers, la sélection du pilote est aléatoire.
   - Seuls les lots de pilotes hors ligne (fichiers .zip) sont utilisés.
   - Téléchargez et extrayez les lots de pilote hors ligne (fichiers .zip) et enregistrez-les à l'emplacement partagé en fournissant le chemin complet de l'emplacement partagé. OMIVV crée automatiquement le catalogue dans l'appliance OMIVV. Les lots de pilotes sont disponibles sur https://my.vmware.com/web/vmware/downloads
   - OMIVV nécessite un accès en écriture au système de fichiers CIFS ou au NFS.
   - Les fichiers contenus dans les sous-dossiers sont ignorés.
   - Les fichiers dont la taille dépasse 10 Mo sont ignorés.
   - La logithèque de pilotes ne s'applique qu'aux clusters vSAN.

4. Dans la zone **Emplacement de partage de logithèque**, exécutez les tâches suivantes :
   a. Saisissez l'emplacement du partage de logithèque (NFS ou CIFS).
   b. Pour CIFS, saisissez les informations d'identification.

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

5. Pour valider le chemin du catalogue et les informations d'identification, cliquez sur **DÉMARRER LE TEST**.

   Cette validation est obligatoire pour continuer.

   Les résultats du test de connexion s'affichent.
6. Cliquez sur **SUIVANT**.
   La page **Synchroniser avec l'emplacement de la logithèque** s'affiche.
7. Sur la page **Synchroniser avec l'emplacement de la logithèque**, cochez la case **Synchroniser avec l'emplacement de la logithèque**, puis cliquez sur **SUIVANT**.
   Pour mettre à jour le nom du profil uniquement ou revoir les informations, décochez la case **Synchroniser avec l'emplacement de la logithèque** pour que le catalogue reste inchangé dans OMIVV. Pour plus d'informations sur la synchronisation avec l'emplacement de la logithèque, voir Synchronisation avec l'emplacement de la logithèque , page 50.
8. Sur la page **Résumé**, vérifiez les informations du profil, puis cliquez sur **TERMINER**.

Modification ou personnalisation du catalogue Dell par défaut

1. Sur la page **Profil de logithèque**, sélectionnez **Catalogue Dell par défaut**.
2. Sur la page **Nom et description du profil**, modifiez la description du profil, puis cliquez sur **SUIVANT**.
3. Dans la section **Spécifier l'emplacement de la logithèque**, sélectionnez l'un des emplacements de logithèque suivants :
   - **Dell Default Online** : profil de logithèque défini sur **Dell Online** (`https://downloads.dell.com/catalog/Catalog.gz`). OMIVV utilise Dell EMC Online en tant que source pour le catalogue et les packages de mises à jour.
   - **Custom Online** : OMIVV utilise **Custom Online** (partage HTTP ou HTTPS) en tant que source pour le catalogue et les packages de mises à jour. Lorsque vous créez une logithèque personnalisée à l'aide de l'utilitaire de mise à jour des serveurs (SUU), assurez-vous que le fichier de signature du catalogue (`catalog.xml.gz.sign`) est bien dans le dossier du fichier de catalogue.
   - **Dossier de réseau partagé** : OMIVV utilise un dossier de réseau partagé (CIFS ou NFS) comme source pour le catalogue et les packages de mises à jour.

   a. Si vous sélectionnez **Custom Online**, saisissez le chemin d'accès au catalogue en ligne.
   b. Si vous sélectionnez **Dossier réseau partagé**, saisissez l'emplacement du fichier de catalogue (NFS ou CFIS).
4. Pour valider le chemin du catalogue et les informations d'identification, cliquez sur **DÉMARRER LE TEST**.
   Les résultats du test de connexion s'affichent.
5. Sur la page **Synchroniser avec l'emplacement de la logithèque**, cochez la case **Synchroniser avec l'emplacement de la logithèque**, puis cliquez sur **SUIVANT**.
   Pour mettre à jour le nom du profil uniquement ou revoir les informations, décochez la case **Synchroniser avec l'emplacement de la logithèque** pour que le catalogue reste inchangé dans OMIVV. Pour plus d'informations sur la synchronisation avec l'emplacement de la logithèque, voir Synchronisation avec l'emplacement de la logithèque , page 50.
6. Sur la page **Résumé**, vérifiez les informations du profil, puis cliquez sur **TERMINER**.

Modification d'un catalogue de piles MX validé

1. Sur la page **Profil de logithèque**, sélectionnez **Catalogue de piles MX validé**, puis cliquez sur **MODIFIER**.
2. Vous pouvez modifier uniquement les éléments suivants :
   a. La description du catalogue.
   b. La case à cocher **Synchroniser avec l'emplacement de la logithèque**.
      Pour mettre à jour le nom du profil uniquement ou revoir les informations, décochez la case **Synchroniser avec l'emplacement de la logithèque** pour que le catalogue reste inchangé dans OMIVV. Pour plus d'informations sur la synchronisation avec l'emplacement de la logithèque, voir Synchronisation avec l'emplacement de la logithèque , page 50.

Synchronisation avec l'emplacement de la logithèque

Le catalogue par défaut Dell et les profils de logithèque de piles MX validés vérifient automatiquement si des modifications ont été effectuées toutes les 24 heures ou à chaque redémarrage et se mettent à jour automatiquement.

Pour mettre à jour les catalogues hors ligne, effectuez les étapes suivantes :

1. Mettez à jour le catalogue du site hors ligne (CIFS ou NFS) à l'aide de Dell EMC Repository Manager (DRM) ou Server Update Utility (SUU). Si des pilotes sont présents, remplacez les lots de pilotes.
2. Modifiez le profil de logithèque et cochez la case **Synchroniser avec l'emplacement de la logithèque** pour capturer les modifications qu'OMIVV doit référencer. Ce processus prend quelques minutes.
3. Pour mettre à jour le firmware dans une base de conformité de configuration, veillez à modifier les profils de cluster respectifs et d'enregistrer.

Affichage d'un profil de logithèque

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil de logithèque**.
   Un tableau affiche tous les profils de logithèque ainsi que les informations suivantes :
   - **Nom du profil** : nom du profil de logithèque
   - **Description** : description du profil
   - **Type** : type de logithèque (firmware ou pilote)

- **Chemin de partage** : chemin NFS ou CIFS ou HTTP ou HTTPS
- **Heure de la dernière mise à jour réussie** : date et heure de la mise à jour du profil de logithèque.
- **État de la dernière actualisation** : état du téléchargement et de l'analyse du catalogue

2. Si vous souhaitez supprimer ou ajouter des noms de colonnes dans l'Assistant, cliquez sur .
3. Pour exporter les informations du profil de logithèque, cliquez sur l' .

Suppression d'un profil de logithèque

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

1. Sur la page **Profil de logithèque**, sélectionnez un profil et cliquez sur **SUPPRIMER**.
2. Dans la boîte de dialogue de confirmation de la suppression, cliquez sur **SUPPRIMER**.

7

Capture de la configuration de base à l'aide d'un profil de cluster

Profil de cluster

Un profil de cluster vous permet de capturer la configuration de base (configuration matérielle, firmware ou versions de pilotes), puis de maintenir l'état requis pour les clusters en identifiant toute dérive par rapport à la configuration de base.

Pour créer un profil de cluster, assurez-vous que vous disposez de l'un de ces profils : profil système, profil de logithèque de firmwares, profil de logithèque de pilotes ou une combinaison des trois. Il vous est recommandé d'utiliser des serveurs homogènes (même modèle, même configuration matérielle et même niveau de firmware) pour les clusters en cours de configuration de base.

- Une fois le profil de cluster créé, les profils de logithèque de firmwares et de pilotes doivent être analysés avant de pouvoir être utilisés pour la création d'un profil de cluster.
- Après la création du profil de cluster, un instantané actuel de la logithèque de firmwares et de pilotes associée est créé pour la ligne de base. Si les logithèques d'origine changent, le profil de cluster doit être remis à jour pour tenir compte des changements. Sinon, toutes les mises à jour effectuées sur les logithèques d'origine ne sont pas mises à jour sur les instantanés de 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.
- Si plusieurs vCenters autonomes sont enregistrés auprès d'OMIVV, nous vous recommandons de créer différents profils de cluster pour chaque vCenter.
- La configuration de base des pilotes est prise en charge uniquement sur les clusters vSAN.

  REMARQUE : Les pilotes qui sont installés en dehors d'OMIVV ne sont pas pris en compte pour la configuration de base.

Création d'un profil de cluster

Vérifiez que :

- vous disposez de l'un de ces profils : profil système, profil de logithèque de firmwares, profil de logithèque de pilotes ou une combinaison des deux.
- Le cluster est présent dans le vCenter.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de cluster** > **CRÉER UN NOUVEAU PROFIL**.
2. Sur la page **Profil de cluster** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Sur la page **Nom et description du profil**, saisissez le nom et la description du profil, puis cliquez sur **SUIVANT**.
   Le nom du profil peut comporter jusqu'à 200 caractères et la description jusqu'à 400 caractères.
4. Sur la page **Associer le ou les profils**, sélectionnez l'un des profils suivants ou ses combinaisons :
   - Profil système : la sélection d'un profil système définit la ligne de base de configuration pour les hôtes du cluster. Pour les types de profil système de base et avancé, le nom du profil système s'affiche au format suivant : Basic_<nom du profil système>, Advanced_<nom du profil système>
   - Profil de logithèque de firmwares : la sélection d'une logithèque de firmwares crée le firmware ou la ligne de base du BIOS de base pour les hôtes du cluster. Les logithèques en ligne ne sont pas prises en charge pour les clusters vSAN de base.
   - Profil de logithèque de pilotes : la sélection d'une logithèque de pilotes crée la ligne de base du pilote pour les hôtes du cluster. Vous pouvez associer un maximum de 10 pilotes à la fois à une ligne de base. La configuration de base des pilotes est prise en charge uniquement sur les clusters vSAN.
5. Cliquez sur **SUIVANT**.
   La page **Associer le ou les clusters** s'affiche.
6. Sur la page **Associer le ou les clusters**, exécutez les opérations suivantes :
   a. Sélectionnez une instance d'un serveur vCenter enregistrés.

b. Pour associer les clusters, cliquez sur **PARCOURIR**.
c. Sélectionnez le cluster que vous souhaitez référencer.
d. Cliquez sur **OK**.
Le cluster sélectionné s'affiche sur la page **Associer le ou les clusters**.
e. Cliquez sur **SUIVANT**.

7. Sur la page **Planifier la détection de dérive**, sélectionnez la date et l'heure, puis cliquez sur **SUIVANT**.
La page **Récapitulatif** s'affiche. Elle contient les informations concernant le profil de cluster.
8. Cliquez sur **TERMINER**.
La tâche de détection de dérive s'exécute immédiatement après que le profil de cluster est enregistré et s'exécute pendant la période planifiée. Affichez l'état d'achèvement de la tâche sur la page des tâches.

REMARQUE : Si le nombre de nœuds (gérés par OMIVV) est modifié après la création du profil du cluster pour celui-ci, la taille de la collecte est automatiquement mise à jour au cours des tâches de détection de dérive ultérieures.

Modification d'un profil de cluster

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

Si la logithèque de pilotes/firmwares associée ou le profil système ont été modifiés et si vous souhaitez utiliser les dernières modifications du profil de cluster, sélectionnez un profil de cluster, cliquez sur **MODIFIER**, cliquez sur **SUIVANT** dans l'assistant, puis cliquez sur **Terminer**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de cluster**.
2. Sélectionnez un profil de cluster, puis cliquez sur **MODIFIER**.
3. Sur la page **Nom et description du profil**, modifiez la description, puis cliquez sur **SUIVANT**.
4. Sur la page **Associer le ou les profils**, vous pouvez modifier les combinaisons de profils.
5. Sur la page **Associer le ou les clusters**, vous pouvez modifier l'instance vCenter et les clusters associés.
6. Sur la page **Planifier la détection de dérive**, vous pouvez modifier le planning de détection de dérive.
7. Passez en revue les informations mises à jour sur la page **Résumé**, puis cliquez sur **TERMINER**.
La tâche de détection de dérive s'exécute immédiatement après que le profil de cluster est enregistré et s'exécute pendant la période planifiée.

Affichage d'un profil de cluster

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de cluster**.
Un tableau affiche tous les profils de cluster ainsi que les informations suivantes :

- **Nom du profil** : nom du profil de cluster
- **Description** : description du profil
- **Profil système associé** : le nom du profil système associé pour les types de profils système de base et avancés, le nom du profil du système s'affiche au format suivant : Basic_<nom du profil système>, Advanced_<nom du profil système>
- **Profil de logithèque de firmwares associé** : nom du profil de logithèque de firmwares associé
- **Profil de logithèque de pilotes associé** : nom du profil de logithèque de pilotes associé

  REMARQUE : Pour un hôte MX PowerEdge géré à l'aide d'un profil d'identification de châssis, la dérive de la configuration n'est pas calculée.
- **vCenter** : l'instance vCenter associée au profil de cluster
- **Heure de la dernière mise à jour réussie** : date et heure de la mise à jour du profil de cluster.

REMARQUE : Si le profil de logithèque (firmware ou pilote) ou le profil système associé est modifié, un symbole d'avertissement s'affiche avec le nom du profil. Le profil de cluster doit être mis à jour après la modification d'un profil de logithèque ou de système afin que les modifications soient mises à jour dans la base. Pour plus d'informations sur la mise à jour du profil de cluster, voir Mise à jour d'un profil de cluster , page 54.

2. Si vous souhaitez supprimer ou ajouter les noms de colonnes dans l'Assistant, cliquez sur .
3. Pour exporter les informations du profil de cluster, cliquez sur .

Mise à jour d'un profil de cluster

Si vous mettez à jour le profil de logithèque (firmware ou pilote) et le profil système, un symbole d'avertissement s'affiche par rapport au nom du profil sur la page profil de cluster. La mise à jour des profils peut avoir une incidence sur la conformité de la configuration des clusters associés dans le profil de cluster et l'état de conformité des firmwares dans vSphere Lifecycle Manager. Vous pouvez utiliser la fonctionnalité **Mettre à jour les profils** pour mettre à jour ou réinitialiser le profil de cluster.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de cluster**.
2. Sélectionnez un profil de cluster doté d'un symbole d'avertissement par rapport au nom du profil.
3. Cliquez sur **METTRE À JOUR LES PROFILS**.
4. Pour mettre à jour les profils associés à la dernière version, cliquez sur **OK**.

   Une fois que vous avez mis à jour les profils, la ligne de base ne peut pas être rétablie.

   Le symbole d'avertissement disparaît lorsque le profil de cluster est synchronisé avec les profils de logithèque ou le profil système mis à jour.

Suppression d'un profil de cluster

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil de cluster**.
2. Sélectionnez un profil de cluster, puis cliquez sur **SUPPRIMER**.
3. Dans la boîte de dialogue **Confirmation de la suppression**, cliquez sur **SUPPRIMER**.
   Si le profil de cluster est supprimé, la tâche de détection de dérive correspondante est également supprimée.

8

Gestion des serveurs sur matériel vierge

Affichage des serveurs sur matériel vierge

Sur la page **Serveurs sur matériel vierge**, vous pouvez effectuer les opérations suivantes :

- Afficher les serveurs sur matériel vierge découverts à l'aide de la découverte automatique et de la découverte manuelle.

  Les informations telles que le **numéro de série**, le **nom du modèle**, l'**adresse IP d'iDRAC**, l'**état du serveur**, le **mode System Lockdown**, l'**état de conformité** et l'**état de la licence iDRAC** sont affichées.

  Vous trouverez ci-dessous les différents états possibles des serveurs sur matériel vierge :

  - **Non configuré** : le serveur est ajouté à OMIVV et en attente de configuration.
  - **Configuré** : le serveur est configuré avec toutes les informations matérielles requises pour réussir le déploiement du système d'exploitation.
  - **En quarantaine** : les serveurs ne peuvent pas effectuer de tâches telles que le déploiement du système d'exploitation et la mise à jour des firmwares, car les serveurs sont exclus des actions OMIVV.
- Afficher l'état de conformité des serveurs sur matériel vierge.

  Un serveur sur matériel vierge 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.
  - Carte LOM ou NIC absente.
  - Le mode System Lockdown est activé.
- Pour afficher plus d'informations sur le problème de conformité, cliquez sur **DÉTAILS** dans le volet horizontal inférieur.

Vous pouvez effectuer les opérations suivantes sur la page **Serveurs sur matériel vierge** :

- Découverte manuelle des serveurs sur matériel vierge
- Suppression d'un serveur sur matériel vierge
- Déploiement de profil système et de profil ISO
- Actualisation des serveurs sur matériel vierge
- Achat ou renouvèlement de la licence d'iDRAC

Détection de périphériques

La détection est le processus d'ajout d'un serveur sans système d'exploitation pris en charge. Une fois le serveur détecté, vous pouvez l'utiliser à des fins de déploiement du profil système et du profil ISO. Pour plus d'informations sur la liste de serveurs pris en charge, voir le document *Matrice de compatibilité d'OpenManage Integration pour VMware vCenter*.

Conditions préalables :

- Cette opération nécessite également une connectivité réseau de l'iDRAC de serveur sans système d'exploitation à la machine virtuelle OMIVV.
- Les hôtes dotés de systèmes d'exploitation existants ne doivent pas être détectés dans OMIVV, mais ajoutés au vCenter. Ajoutez-les à un profil d'identification d'hôte.
- Pour déployer le système d'exploitation sur une carte SD et pour utiliser les fonctionnalités du profil système sur des serveurs PowerEdge de 12e et 13e génération, assurez-vous que l'iDRAC version 2.50.50.50 ou ultérieure est installé.

Découverte automatique

La détection automatique est le processus d'ajout d'un serveur sans système d'exploitation. Une fois le serveur détecté, utilisez-le pour le déploiement de système d'exploitation et de matériel. La découverte automatique est une fonctionnalité d'iDRAC qui supprime la tâche de détection manuelle d'un serveur sur matériel vierge qui utilise OMIVV.

Conditions préalables à la détection automatique

Avant toute tentative de découverte de serveurs PowerEdge sur matériel vierge, assurez-vous qu'OMIVV est 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 connectivité réseau entre le contrôleur iDRAC du serveur Dell EMC sur matériel vierge et l'appliance OMIVV.

REMARQUE : Les hôtes dotés de systèmes d'exploitation existants ne doivent pas être détectés à l'aide d'OMIVV. Ajoutez plutôt le système d'exploitation à un profil d'identification d'hôte.

Pour que la découverte automatique fonctionne, les conditions suivantes doivent être réunies :

- Alimentation : branchez le serveur à la prise secteur. Le serveur n'a pas besoin d'être mis sous tension.
- Connectivité réseau : vérifiez que l'iDRAC du serveur dispose d'une connectivité réseau et communique avec le serveur de provisionnement sur le port 4433. Vous pouvez obtenir l'adresse IP du serveur de provisionnement à l'aide du serveur DHCP ou la spécifier manuellement dans l'utilitaire de configuration de l'iDRAC.
- Paramètres réseau supplémentaires : pour résoudre les noms de DNS, activez l'option Obtenir l'adresse du serveur DNS dans les paramètres de DHCP.
- Emplacement du service de provisionnement : assurez-vous que le contrôleur iDRAC connaît l'adresse IP ou le nom de l'hôte du serveur du service de provisionnement. Voir Emplacement du service de provisionnement.
- Accès au compte désactivé : s'il existe des comptes iDRAC disposant de privilèges administrateur, vous devez d'abord les désactiver depuis la console Web iDRAC. Une fois la détection automatique terminée, le compte administrateur iDRAC est réactivé avec les informations d'identification de déploiement saisies sur la page **Paramètres**. Pour plus d'informations sur les informations d'identification de déploiement, voir Configuration des informations d'identification de déploiement , page 86.
- Découverte automatique activée : assurez-vous que la détection automatique est activée sur l'iDRAC du serveur afin que le processus de détection automatique puisse commencer. Pour plus d'informations, voir Activation ou désactivation de comptes administratifs dans iDRAC , page 56.

Emplacement du service de provisionnement

Utilisez les options suivantes pour obtenir l'emplacement du service dde provisionnement 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 provisionnement.
- 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 provisionnement n'est pas spécifiée manuellement dans l'utilitaire de configuration de l'iDRAC, l'iDRAC tente d'utiliser 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 du 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 sur https://www.dell.com/support.

Activation ou désactivation de comptes administratifs dans iDRAC

Avant de configurer la détection automatique, désactivez tous les comptes IDRAC sauf ceux qui ne disposent pas d'accès administrateur. Après la détection automatique, vous pouvez activer tous les comptes à l'exception du compte racine (root).

REMARQUE : Avant la désactivation des privilèges administrateur, il vous est recommandé de créer un compte d'utilisateur non administrateur dans iDRAC.

1. Dans un navigateur, saisissez l'**adresse IP d'iDRAC**.

2. Connectez-vous à l'**interface utilisateur graphique d'iDRAC**.
3. Effectuez l'une des opérations suivantes :
   - 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**.
   - Pour iDRAC9 : accédez à **Paramètres d'iDRAC** > **Utilisateurs** > **Utilisateurs locaux**.
4. Dans l'onglet **Utilisateurs locaux**, 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, mais cochez la case **Activer l'utilisateur**, puis cliquez sur **Appliquer**.

Configuration manuelle des serveurs PowerEdge en vue d'une découverte 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. Une fois que vous avez reçu les serveurs de Dell EMC, lorsque vous les mettez sous tension après avoir monté et branché le câble iDRAC, les serveurs sont découverts et répertoriés automatiquement sur la page **Serveurs sur matériel vierge**.

REMARQUE : Pour les serveurs découverts automatiquement, les informations d'identification fournies dans **Paramètres** > **Paramètres de l'appliance** > **Informations d'identification du déploiement** sont définies en tant qu'informations d'identification d'administrateur 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 du système d'exploitation réussie, les informations d'identification iDRAC fournies dans le profil d'identification d'hôte associé sont définies.

Pour activer manuellement la détection automatique sur l'ordinateur cible, procédez comme suit pour les serveurs PowerEdge de 12e génération et de générations ultérieures :

1. Sur le système cible, appuyez sur la touche F2 pendant le démarrage initial.
2. Accédez à **Paramètres iDRAC** > **Configuration de l'utilisateur**, puis désactivez l'utilisateur root. 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 est activé et l'indicateur **Activer la détection automatique** est désactivé automatiquement.

Découverte manuelle des serveurs sur matériel vierge

Assurez-vous qu'un utilisateur iDRAC disposant de privilèges d'administration est utilisé pour la détection.

OMIVV vous permet de découvrir manuellement les serveurs en fonction d'une plage d'IPv4. Vous pouvez découvrir une seule adresse IP ou un seul groupe d'adresses IP à l'aide de la méthode de détection de plages d'IPv4.

Lorsque vous avez ajouté le serveur sur matériel vierge, il s'affiche dans la liste des serveurs sur la page **Serveurs sur matériel vierge**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Déploiement** > **DÉCOUVRIR**.
   La page **Détecter un serveur sur matériel vierge** s'affiche.
2. Sur la page **Détecter un serveur sur matériel vierge**, exécutez les tâches suivantes :
   a. Dans le champ **Nom de la tâche de détection**, saisissez un nom de tâche.
   b. Saisissez la description de la tâche (facultatif).

c. Pour saisir des plages d'adresses IP, cliquez sur **AJOUTER UNE PLAGE DE DONNÉES**.

   Plusieurs plages peuvent être mentionnées dans chaque tâche de détection. 1 024 adresses IP maximum sont prises en charge. 256 adresses IP maximum peuvent être configurées dans une plage.

   Les adresses IP incluses sont prioritaires lorsque vous ajoutez un ensemble d'adresses IP spécifique dans la liste d'exclusion d'une plage, puis que vous ajoutez les mêmes adresses IP dans la liste d'inclusions d'une autre plage.

d. Saisissez l'**adresse IP de début**.

   L'adresse IP de début doit être au format d'adresse IPv4.

e. Saisissez l'**adresse IP de fin**.

   L'adresse IP de fin doit être le dernier octet de l'adresse IP et d'une valeur supérieure à l'adresse IP de début.

f. Saisissez la **liste d'exclusion**.

   La liste d'exclusion est la liste des adresses IP que vous souhaitez exclure de la liste.

   La valeur que vous saisissez dans la **Liste d'exclusion** doit se trouver dans les plages **Adresse IP de début** et **Adresse IP de fin**. Les valeurs doivent être séparées par des virgules. Chaque valeur peut être une valeur de dernier octet ou une plage de valeurs de dernier octet séparées par le symbole -.

   Par exemple :

   Pour découvrir toutes les adresses IP de 100.100.100.1 à 100.100.100.50, à l'exception des adresses IP de 100.100.100.25 à 100.100.100.30 et de 100.100.100.40 à 100.100.100.45, saisissez la commande suivante dans **Adresse IP de début**, **Adresse IP de fin**, et **Liste d'exclusion**.

   Adresse IP de début : 100.100.100.1

   Adresse IP de fin : 50

   Liste d'exclusion : 25-30, 40-45

g. Pour utiliser les informations d'identification iDRAC saisies sur la page **Informations d'identification du déploiement**, cochez la case **Utiliser les informations d'identification du déploiement**.

   Pour plus d'informations sur les informations d'identification de déploiement, voir Configuration des informations d'identification de déploiement , page 86.

h. Saisissez le nom d'utilisateur et le mot de passe si les informations d'identification de déploiement ne sont pas définies.

   Par défaut, les informations d'identification du déploiement sont définies. Saisissez le nom d'utilisateur et le mot de passe de l'iDRAC si vous souhaitez utiliser des informations d'identification, différentes de celles de déploiement. Vous pouvez disposer d'un ensemble d'informations d'identification distinct pour chaque plage.

   Le nom d'utilisateur doit contenir entre 1 et 16 caractères. Les caractères spéciaux /, \, ~ et ' ne sont pas pris en charge.

   Le mot de passe peut contenir 42 caractères maximum.

3. Sélectionnez l'une des options suivantes :

   - **Exécuter maintenant** : cette action détecte toutes les adresses IP mentionnées dans la plage donnée.
   - **Exécuter plus tard** : cette action détecte les adresses IP dans la plage donnée.

4. Cliquez sur **APPLIQUER**.
   L'état de la tâche de détection s'affiche sur la page **Tâches de détection**. Pour plus d'informations, voir Tâches de détection , page 77.

Suppression d'un serveur sur matériel vierge

Vous pouvez supprimer manuellement un serveur qui a été découvert automatiquement ou ajouté manuellement.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Déploiement** > **SUPPRIMER**.
2. Sélectionnez un serveur sur matériel vierge, puis cliquez sur **OK**.

Actualisation des serveurs sur matériel vierge

L'opération d'actualisation redécouvre les serveurs sur matériel vierge en se connectant à iDRAC et en collectant l'inventaire de base.

REMARQUE : Si vous exécutez l'opération d'actualisation sur les serveurs sur matériel vierge dont l'état est « Configuré », celui-ci passera à l'état « Non configuré », car l'opération d'actualisation redécouvre chaque serveur.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Déploiement** > **ACTUALISER**.
2. Sur la page **Actualiser les serveurs sur matériel vierge**, sélectionnez un serveur, puis cliquez sur **OK**.
   L'actualisation des données des serveurs sans système d'exploitation peut prendre quelques minutes. Lorsque l'opération est en cours, vous pouvez fermer la page **Actualiser les serveurs sur matériel vierge**, car le processus de redécouverte se poursuit en arrière-plan. Le serveur redécouvert s'affiche sur la page **Serveurs sur matériel vierge**.

Achat ou renouvèlement de la licence d'iDRAC

L'état des serveurs sur matériel vierge indique qu'ils ne sont pas conformes lorsqu'ils ne disposent pas d'une licence iDRAC compatible. Un tableau présente l'état de la licence iDRAC. Sélectionnez un serveur sur matériel vierge non conforme pour afficher plus d'informations sur la licence iDRAC.

1. Pour renouveler la licence iDRAC, accédez à la page d'accueil de l'OMIVV, puis cliquez sur **Conformité et déploiement** > **Déploiement**.
2. Sélectionnez un serveur sur matériel vierge pour lequel la licence iDRAC n'est pas conforme, puis cliquez sur **ACHETER/ RENOUVELER UNE LICENCE IDRAC**.
3. Connectez-vous à Dell Digital Locker et mettez à jour ou achetez une nouvelle licence iDRAC.
4. Après avoir installé une licence iDRAC, cliquez sur **ACTUALISER**.

9

Gestion des profils de déploiement

Profil système

Le profil système capture les paramètres et la configuration au niveau des composants : iDRAC, BIOS, RAID, filtres d'événements, FC et cartes réseau. Ces configurations peuvent être appliquées à d'autres serveurs identiques lors du déploiement d'un système d'exploitation sur des serveurs sur matériel vierge. Le profil système peut être utilisé dans le profil de cluster pour gérer la configuration de base.

Prérequis

Avant de créer ou de modifier le profil système, assurez-vous que :

- La fonctionnalité CSIOR est activée sur le serveur de référence. Le serveur de référence doit être redémarré après l'activation de la fonction CSIOR afin que les données renvoyées par iDRAC soient à jour.
- L'inventaire a réussi pour chaque hôte de référence géré par vCenter.
- Les serveurs sur matériel vierge disposent des versions minimales obligatoires du BIOS et du firmware. Pour plus d'informations, voir la *Matrice de compatibilité OMIVV* disponible sur le site de support.
- Le serveur de référence et les serveurs cibles sont homogènes (même modèle, même configuration matérielle et même niveau de firmware).
- Le matériel des serveurs cibles (par exemple, FC, carte réseau et contrôleur RAID) est monté dans les mêmes logements que sur le serveur de référence.
- Avant d'inclure ou d'exclure un attribut de la sélection par défaut, passez votre curseur sur le nom pour comprendre les détails de l'attribut.
- L'utilisateur iDRAC utilisé pour découvrir l'iDRAC est sélectionné lors de la configuration des utilisateurs iDRAC dans le profil système.

  REMARQUE : N'effacez pas les attributs liés à l'utilisateur iDRAC qui est utilisé pour la détection sans système d'exploitation, sinon la tâche de déploiement du profil système risque d'échouer.
- Ne modifiez pas le nom de l'utilisateur iDRAC utilisé pour découvrir l'iDRAC. Cela entraîne un problème de connectivité avec iDRAC, la tâche de déploiement du profil système échoue sans appliquer d'attributs.

Avant de créer le profil système, nous vous recommandons de configurer l'attribut et la valeur du serveur de référence selon vos besoins. Appliquez l'attribut et la valeur de référence à tous les hôtes cibles requis.

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 à d'autres serveurs modulaires dans le même châssis FX en raison de restrictions au niveau de la carte réseau. Dans ce cas, nous vous recommandons de disposer d'un profil de système de référence pour chaque logement du châssis. Appliquez ces profils système à l'ensemble du châssis pour les logements correspondants uniquement.

REMARQUE : Un profil système ne prend pas en charge l'activation et la désactivation des options d'amorçage.

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 entraîne un échec.
- 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.

Création d'un profil système

Il est recommandé d'utiliser Google Chrome pour créer ou modifier le profil système.

Les serveurs PowerEdge R6515, R7515, R65125, R7525 et C6515, qui ont HBA, BOSS et PERC connectés à l'aide d'un câble extra-plat. Le profil système créé dans OMIVV avec une version de l'iDRAC antérieure à la version 4.30.30.30 ne peut pas être utilisé pour

l'iDRAC 4.30.30.30 et les versions supérieures. Créez un nouveau profil système avec l'iDRAC 4.30.30.30 ou une version supérieure et utilisez-le lorsque vous en avez besoin.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil système** > **CRÉER UN NOUVEAU PROFIL**.
2. Sur la page **Créer un profil système** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Sur la page **Nom et description**, effectuez les opérations suivantes :
   a. Saisissez le nom et la description du profil. Le champ de description est facultatif.
   b. Sélectionnez l'un des types de profils système suivants :
      - **Basique** : affiche l'ensemble minimal d'attributs d'iDRAC, du BIOS, du RAID, de la carte NIC et du FC.
      - **Avancé** : affiche tous les attributs d'iDRAC, du BIOS, du RAID, de la carte NIC, du FC et d'EventFilters.
4. Sur la page **Serveur de référence**, cliquez sur **SÉLECTIONNER** pour sélectionner un serveur de référence qui peut être un hôte ou un serveur sur matériel vierge.

   La sélection du serveur peut être désactivée pour l'une des raisons suivantes :

   - Le serveur est un serveur hôte non conforme ou un serveur sur matériel vierge non conforme.
   - Une tâche de déploiement est planifiée ou en cours d'exécution sur le serveur.
   - Le serveur est géré à l'aide du profil d'identification de châssis.

   La boîte de dialogue **Confirmation d'extraction** s'affiche.
5. Pour extraire la configuration système du serveur de référence, cliquez sur **OK**.
   L'extraction de la configuration système du serveur de référence peut prendre quelques minutes.
6. Vérifiez les détails du serveur de référence, puis cliquez sur **SUIVANT**.
   - Pour changer de serveur de référence sur la page **Sélectionner le serveur de référence**, cliquez sur **PARCOURIR**.

     Si le serveur de référence est dépourvu de système d'exploitation, seule son adresse IP iDRAC est affichée. Si le serveur de référence lui-même est un serveur hôte, les adresses IP de l'iDRAC et de l'hôte (FQDN) sont affichées.

   La page **Paramètres du profil** s'affiche.
7. Sur la page **Paramètres du profil**, vous pouvez afficher et modifier les paramètres du profil des composants (iDRAC, BIOS, RAID, NIC, CNA, FCoE et EvenFilters) en fonction de la configuration du serveur de référence.

   Par défaut, les attributs propres à la plate-forme et les attributs en lecture seule ne sont pas répertoriés. Pour plus d'informations sur les attributs spécifiques à la plate-forme, voir Attributs spécifiques au système , page 174.

   Les attributs de pseudo ne sont pas affichés dans le profil système. Pour plus d'informations, reportez-vous au document Fichier XML de configuration de serveur.

   Avant de sélectionner des attributs autres que ceux sélectionnés par défaut, vérifiez la nature de l'attribut, de la dépendance ainsi que les autres détails.

   Si vous sélectionnez des attributs autres que ceux sélectionnés par défaut, le message suivant s'affiche :

   Ces attributs peuvent affecter d'autres attributs dépendants, être destructeurs par nature, supprimer l'identité du serveur ou affecter la sécurité des serveurs cibles.

   REMARQUE : Pour les serveurs PowerEdge de 12e et 13e génération, il se peut que certains des attributs ne mappent pas correctement les dépendances dans l'OMIVV. Par exemple, le composant de tension de fonctionnement de la mémoire du BIOS est en lecture seule, sauf si le profil système est défini sur **Personnalisé** dans les **Paramètres système du BIOS**.

   a. Développez chaque composant pour afficher les options de configuration (**Instance**, **Nom d'attribut**, **Valeur**, **Destructeur**, **Dépendance** et **Groupe**).

      Si le texte de dépendance n'est pas disponible, un champ vide s'affiche.

      REMARQUE : Vous pouvez utiliser le champ de **Recherche** pour filtrer des données spécifiques à toutes les colonnes, à l'exception de **Valeur**.

   b. Il est obligatoire de définir des valeurs pour les attributs marqués d'un point d'exclamation rouge. Cette option est uniquement disponible pour l'utilisateur iDRAC ayant un nom d'utilisateur valide.
8. Cliquez sur **SUIVANT**.
   La page **Récapitulatif** affiche 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 et le nombre total d'attributs destructeurs s'affichent sous les statistiques des attributs.
9. Cliquez sur **TERMINER**.

Le profil enregistré s'affiche sur la page **Profil système**.

Certains attributs du profil système sont remplacés pour que l'OMIVV puisse fonctionner. Pour plus d'informations sur la personnalisation des attributs, voir Attributs de personnalisation , page 179. Pour plus d'informations sur le modèle de configuration du Profil système, des attributs et des workflow, voir Informations supplémentaires , page 178.

Modification du profil système

Il est recommandé d'utiliser Google Chrome pour créer ou modifier le profil système.

1. Sur la page **Créer un profil système**, sélectionnez un profil système, puis cliquez sur **MODIFIER**.
2. Sur la page **Nom et description**, modifiez le nom et la description du profil. La description est facultative.

   REMARQUE : Après avoir créé le profil système de base ou avancé, vous ne pouvez pas modifier les profils.

3. Sur la page **Serveur de référence**, pour modifier le serveur de référence qui peut être un hôte ou un serveur sur matériel vierge, cliquez sur **SÉLECTIONNER**.

   La sélection du serveur peut être désactivée pour l'une des raisons suivantes :

   - Le serveur est un serveur hôte non conforme ou un serveur sans système d'exploitation.
   - Une tâche de déploiement est planifiée ou en cours d'exécution sur le serveur.
   - Le serveur est géré à l'aide du profil d'identification de châssis.

   La boîte de dialogue **Confirmation d'extraction** s'affiche.
4. Pour extraire la configuration système du serveur de référence, cliquez sur **OK**.
   L'extraction de la configuration système du serveur de référence peut prendre quelques minutes.
5. Vérifiez les détails du serveur de référence, puis cliquez sur **SUIVANT**.

   - Pour changer de serveur de référence sur la page **Sélectionner le serveur de référence**, cliquez sur **PARCOURIR**. Si le serveur de référence est dépourvu de système d'exploitation, seule son adresse IP iDRAC est affichée. Si le serveur de référence lui-même est un serveur hôte, les adresses IP de l'iDRAC et de l'hôte (FQDN) sont affichées.

   La page **Paramètres du profil** s'affiche.
6. Sur la page **Paramètres du profil**, vous pouvez afficher et modifier les paramètres du profil des composants (iDRAC, BIOS, RAID, NIC, CNA, FCoE et EvenFilters) en fonction de la configuration du serveur de référence.

   Par défaut, les attributs propres à la plate-forme et les attributs en lecture seule ne sont pas répertoriés. Pour plus d'informations sur les attributs spécifiques à la plate-forme, voir Attributs spécifiques au système , page 174.

   Si vous tentez de modifier certains attributs, le message d'avertissement suivant s'affiche :

   Ces attributs peuvent affecter d'autres attributs dépendants, être destructeurs par nature, supprimer l'identité du serveur ou affecter la sécurité des serveurs cibles.

   REMARQUE : Après avoir modifié le profil système, si le mot de passe des utilisateurs de l'iDRAC utilisé pour détecter le serveur sur matériel vierge est modifié et que le mot de passe mis à jour est ignoré, le mot de passe mis à jour est remplacé par le mot de passe utilisé pour détecter les serveurs sur matériel vierge.

   a. Développez chaque composant pour afficher les options de configuration (Instance, Nom d'attribut, Valeur, Destructeur, Dépendance et Groupe).

      Si le texte de dépendance n'est pas disponible, un champ vide s'affiche.
   b. Il est obligatoire de définir des valeurs pour les attributs marqués d'un point d'exclamation rouge. Cette option est uniquement disponible pour l'utilisateur iDRAC ayant un nom d'utilisateur valide.
7. Cliquez sur **SUIVANT**.
   La page **Récapitulatif** affiche 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 et le nombre total d'attributs destructeurs s'affichent sous les statistiques des attributs.
8. Cliquez sur **TERMINER**.
   Le profil enregistré s'affiche sur la page **Profil système**.

   Certains attributs du profil système sont remplacés pour que l'OMIVV puisse fonctionner. Pour plus d'informations sur la personnalisation des attributs, voir Attributs de personnalisation , page 179. Pour plus d'informations sur le modèle de configuration du Profil système, des attributs et des workflow, voir Informations supplémentaires , page 178.

Afficher un profil système

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil système**.
   Un tableau affiche tous les profils système ainsi que les informations suivantes :
   - **Nom du profil** : nom du profil système
   - **Description** : description du profil
   - **Serveur de référence** : adresse IP de l'iDRAC à partir de laquelle les détails de configuration du système sont extraits.
   - **Modèle de serveur** : nom du modèle du serveur de référence
2. Si vous souhaitez supprimer ou ajouter des noms de colonnes dans l'Assistant, cliquez sur .
3. Pour exporter les informations du profil système, cliquez sur .

Suppression d'un profil système

La suppression d'un profil système faisant partie d'une tâche de déploiement en cours d'exécution peut entraîner l'échec de la tâche de suppression.

1. Sur la page **Profil système**, sélectionnez un profil et cliquez sur **SUPPRIMER**.
2. Dans la boîte de dialogue de confirmation de la suppression, cliquez sur **SUPPRIMER**.

Profil ISO

Un profil ISO contient le chemin de dossier du fichier de l'image ISO personnalisée ESXi Dell EMC enregistré dans les dossiers NFS ou CIFS. Un profil ISO est utilisé dans l'assistant de déploiement.

Création d'un profil ISO

Un profil ISO nécessite un emplacement de fichier ISO personnalisé Dell EMC sur un système de fichiers NFS ou CIFS.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil ISO** > **CRÉER UN NOUVEAU PROFIL**.
2. Sur la page **Profil ISO** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Sur la page **Nom et description du profil**, saisissez le nom et la description du profil. La description est facultative.
4. Dans la zone **Source d'installation (ISO)**, saisissez l'emplacement du fichier ISO (NFS ou CIFS).
   OMIVV prend uniquement en charge les partages CIFS des versions 1.0 et 2.0 de Server Message Block (SMB).
   a. Si vous utilisez CIFS, saisissez les informations d'identification.
5. Dans la liste déroulante **Version ESXi**, sélectionnez une version ESXi.
   Sélectionnez la version d'ESXi appropriée pour que le script de démarrage de l'installation soit utilisé. Si vous sélectionnez une version incorrecte d'ESXi, le déploiement peut échouer.
6. Pour vérifier l'accessibilité au chemin du fichier ISO ainsi que les informations d'identification, cliquez sur **DÉMARRER LE TEST**.
   Les résultats du test s'affichent.
7. Cliquez sur **TERMINER**.

Modification d'un profil ISO

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil ISO**.
2. Sélectionnez un profil ISO, puis cliquez sur **MODIFIER**.
3. Sur la page **Nom et description du profil**, modifiez le nom et la description du profil. La description est facultative.
4. Dans la zone **Source d'installation (ISO)**, modifiez l'emplacement du fichier ISO (NFS ou CIFS).
   OMIVV prend uniquement en charge les partages CIFS des versions 1.0 et 2.0 de Server Message Block (SMB).
   a. Si vous utilisez CIFS, saisissez les informations d'identification.

5. Dans la liste déroulante **Version ESXi**, sélectionnez une version ESXi.

   Sélectionnez la version d'ESXi appropriée pour que le script de démarrage de l'installation soit utilisé. Si vous sélectionnez une version d'ESXi incorrecte, le déploiement peut échouer.
6. Pour vérifier le chemin du fichier ISO et l'authentification, cliquez sur **DÉMARRER LE TEST**.
   Les résultats du test s'affichent.
7. Cliquez sur **TERMINER**.

Affichage d'un profil ISO

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profil ISO**.
   Un tableau affiche tous les profils ISO ainsi que les informations suivantes :
   - **Nom du profil** : nom du profil
   - **Description** : description du profil
   - **Source d'installation** : emplacement du fichier ISO (NFS ou CIFS)
   - **Version de base ESXi** : version de base ESXi
2. Si vous souhaitez supprimer ou ajouter des noms de colonnes dans l'Assistant, cliquez sur .
3. Pour exporter les informations d'un profil ISO, cliquez sur l' .

Suppression d'un profil ISO

La suppression d'un profil ISO faisant partie d'une tâche de déploiement en cours d'exécution peut entraîner l'échec de la tâche.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Profils** > **Profil ISO**.
2. Sélectionnez un profil ISO, puis cliquez sur **SUPPRIMER**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **SUPPRIMER**.

Téléchargement des images ISO Dell EMC personnalisées

Les images ESXi personnalisées qui contiennent tous les pilotes Dell EMC sont requises pour le déploiement.

1. Ouvrez un navigateur et accédez à **support.dell.com**.
2. Cliquez sur **Parcourir tous les produits** > **Serveurs** > **PowerEdge**.
3. Cliquez sur un modèle de serveur PowerEdge.
4. Cliquez sur la page **Pilotes et téléchargements** du modèle de serveur.
5. Dans la liste déroulante **Système d'exploitation**, sélectionnez la version d'ESXi.
6. Dans le menu déroulant **Catégorie**, sélectionnez **Solutions d'entreprise**.
7. Dans la liste **Solutions d'entreprise**, sélectionnez la version d'ISO requise, puis cliquez sur **Télécharger**.

10

Déploiement de profil système et de profil ISO

Pour déployer le profil système et le profil ISO, assurez-vous que tous les serveurs répondent aux exigences suivantes dans votre environnement :

- Tous les serveurs s'affichent dans l'Assistant de **déploiement de profil système et de profil ISO**.
- Informations spécifiques à la prise en charge du matériel, mentionnées dans la *Matrice de compatibilité d'OpenManage Integration for VMware vCenter*.
- Disponibilité des versions minimales prises en charge pour le firmware de l'iDRAC et le BIOS.

  Concernant les informations spécifiques à la prise en charge du firmware, voir le document *Matrice de compatibilité d'OpenManage Integration for VMware vCenter*.
- Disponibilité des caractéristiques techniques du stockage de l'IDSDM.

  Pour en savoir plus sur les spécifications de stockage du module IDSDM, consultez la documentation VMware.
- Module IDSDM activé à partir du BIOS avant de déployer un système d'exploitation avec OMIVV.

  OMIVV permet un déploiement sur un module IDSDM, des disques durs locaux ou une carte BOSS.
- Il existe un itinéraire entre les réseaux vCenter, OMIVV et iDRAC si vCenter, OMIVV et iDRAC sont connectés à différents réseaux.

  Cette exigence s'applique uniquement si l'appliance OMIVV n'est pas configurée avec deux contrôleurs d'interface réseau.
- La fonctionnalité Collecter l'inventaire système au redémarrage (CSIOR) est activée.
- Les données récupérées sont à jour en effectuant un redémarrage matériel sur le serveur avant de lancer une détection automatique ou manuelle.
- Pour la détection automatique de serveurs sans système d'exploitation, commandez les serveurs Dell EMC avec les options de détection automatique ou 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 exigences suivantes sont respectées avant de déployer le système d'exploitation si OMIVV n'est pas utilisé pour la configuration matérielle :
  - Activez l'indicateur de technologie de virtualisation (VT) dans le BIOS.
  - Le lecteur virtuel, le IDSDM et le BOSS sont configurés pour le premier disque de démarrage.
- 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 système. Si un lecteur virtuel n'est pas configuré sur le système cible, la configuration RAID Express ou clone est obligatoire.
- Assurez-vous que les images ESXi personnalisées qui contiennent tous les pilotes Dell EMC sont disponibles pour le déploiement.

  Téléchargez les images adéquates à partir de la section **Pilotes et téléchargements**, disponible sur la page **support.dell.com**. Pour en savoir plus sur le téléchargement des images ISO Dell EMC personnalisées, voir Téléchargement des images ISO Dell EMC personnalisées , page 64.
- Enregistrez les images personnalisées à un emplacement de partage CIFS ou NFS auquel OMIVV peut accéder lors du processus de déploiement.

  Pour consulter la liste actualisée des versions ESXi prises en charge par cette version, voir *OpenManage Integration for VMware vCenter Compatibility Matrix* (Matrice de compatibilité d'OpenManage Integration for VMware vCenter).

  Les affirmations suivantes s'appliquent au déploiement d'un hôte à l'aide de plusieurs cartes réseau :
- L'hôte peut disposer d'une carte NIC de gestion d'iDRAC et de vCenter sur le même réseau ou sur les deux réseaux distincts.
- L'image ISO peut être enregistrée dans l'un ou l'autre des réseaux.
- Veillez à sélectionner le réseau vCenter et le réseau OMIVV appropriés pour l'environnement. L'assistant de déploiement du système d'exploitation affiche les deux réseaux OMIVV.

Check-list de déploiement

Avant de déployer le profil système et le profil ISO, assurez-vous que les éléments suivants sont disponibles :

- Profil d'identification d'hôte

  Pour créer un profil d'identification d'hôte, cliquez sur **CRÉER**. Pour en savoir plus sur la création d'un profil d'identification d'hôte, voir Création du profil d'identification d'hôte , page 39.

- Serveur sur matériel vierge

  Pour découvrir un serveur sur matériel vierge, cliquez sur **DÉCOUVRIR**. Pour en savoir plus sur la découverte de serveurs sur matériel vierge, voir Découverte manuelle des serveurs sur matériel vierge , page 57.

- Profil système

  Pour créer un profil système, cliquez sur **CRÉER**. Pour en savoir plus sur la création d'un profil système, voir Création d'un profil système , page 60.

- Profil ISO

  Pour créer un profil ISO, cliquez sur **CRÉER**. Pour en savoir plus sur la création d'un profil ISO, voir Création d'un profil ISO , page 63.

L'assistant **Déploiement du profil système et du profil ISO** vous permet d'exécuter les opérations suivantes :

- Un déploiement de profil système

  Pour plus d'informations, voir Déploiement d'un profil système (configuration du matériel) , page 66.

- Un déploiement de profil ISO

  Pour plus d'informations, voir Déploiement d'un profil ISO (installation ESXi) , page 67.

- Un déploiement de profil système et de profil ISO

  Pour plus d'informations, voir Déploiement du profil système et du profil ISO , page 68.

Déploiement d'un profil système (configuration du matériel)

1. Pour lancer l'assistant de déploiement, accédez à **Conformité et déploiement** > **Déploiement** > **DÉPLOYER**.
2. Sur la page **Check-list pour le déploiement de profil système et de profil ISO** de l'assistant de déploiement, vérifiez la liste de vérification du déploiement, puis cliquez sur **DÉMARRER**.

   Vous pouvez effectuer le déploiement uniquement sur les serveurs conformes sur matériel vierge. Pour plus d'informations, voir Affichage des serveurs sur matériel vierge , page 55.
3. Sur la page **Sélectionner le ou les serveurs**, sélectionnez un ou plusieurs serveurs.
   La page **Sélectionner les options de déploiement** s'affiche.
4. Sur la page **Sélectionner les options de déploiement**, sélectionnez **Profil système (configuration du matériel)**.
5. Dans le menu déroulant **Profil système** , sélectionnez un profil système approprié, puis cliquez sur **SUIVANT**.

   Pour les types de profils système de base et avancés, le nom du profil du système s'affiche au format suivant : Basic_<nom du profil système>, Advanced_<nom du profil système>.

   La tâche **Aperçu de la configuration** tente de comparer ou de vérifier la compatibilité du profil système sélectionné avec l'hôte sélectionné.
6. Pour créer une tâche d'aperçu sur iDRAC, accédez à la page **Aperçu de la configuration**, puis sélectionnez une adresse IP iDRAC et cliquez sur **APERÇU**. L'aperçu de la configuration est une tâche facultative.
   L'opération d'aperçu du profil système peut prendre quelques minutes. L'état de comparaison s'affiche dans la colonne **Résultat**.

   Les résultats de la comparaison sont les suivants :

   - **Terminé** : la tâche d'aperçu a été exécutée correctement. Pour plus d'informations sur les résultats de la comparaison, cliquez sur **Afficher les détails** dans la colonne **Détails**.
   - **Non terminé** : la tâche d'aperçu n'a pas été exécutée correctement sur l'iDRAC. Assurez-vous qu'iDRAC est accessible et effectuez une réinitialisation d'iDRAC, le cas échéant. Pour plus d'informations sur la tâche, reportez-vous aux journaux OMIVV et aux journaux sur la console d'iDRAC.
7. Sur la page **Tâche de planification du déploiement**, procédez comme suit :
   a. Saisissez le nom et la description de la tâche de déploiement. La description est facultative.
   b. Pour exécuter la tâche de déploiement immédiatement, cliquez sur **Exécuter maintenant**.
   c. Pour planifier l'exécution de la tâche ultérieurement, cliquez sur **Planifier pour plus tard**, puis sélectionnez la date et l'heure.

d. Cochez la case **Accéder à la page Tâches après la soumission de la tâche**.
Vous pouvez consulter l'état de la tâche sur la page **Tâches**. Pour plus d'informations, voir Tâches de déploiement , page 76.

8. Cliquez sur **TERMINER**.

Déploiement d'un profil ISO (installation ESXi)

Vous pouvez effectuer le déploiement uniquement sur les serveurs conformes sur matériel vierge. Pour plus d'informations, voir Affichage des serveurs sur matériel vierge , page 55.

1. Pour lancer l'assistant de déploiement, accédez à **Conformité et déploiement** > **Déploiement** > **DÉPLOYER**.
2. Sur la page **Check-list pour le déploiement de profil système et de profil ISO** de l'assistant de déploiement, vérifiez la check-list du déploiement, puis cliquez sur **DÉMARRER**.
3. Sur la page **Sélectionner le ou les serveurs**, sélectionnez un ou plusieurs serveurs.
La page **Sélectionner les options de déploiement** s'affiche.
4. Sur la page **Sélectionner les options de déploiement**, sélectionnez **Profil ISO (installation ESXi)**.
5. Dans le menu déroulant **Nom du vCenter**, sélectionnez une instance de vCenter.
6. Pour sélectionner le vCenter de destination, cliquez sur **PARCOURIR**, puis sélectionnez le datacenter ou le cluster approprié sur lequel vous souhaitez déployer le système d'exploitation.
7. Dans le menu déroulant **Profil ISO**, sélectionnez un profil ISO approprié.
8. Sous **Cible d'installation**, sélectionnez l'une des options suivantes :

- **Premier disque de démarrage** : déploie un système d'exploitation sur le disque dur, le disque SSD (Solid-State Drive) ou le lecteur virtuel créé par contrôleur RAID.
- **Double module SD interne (IDSDM)** : déploie un système d'exploitation sur le module IDSDM. 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 **Premier disque d'amorçage** est disponible.
  - Si l'un des serveurs sélectionnés ne prend pas en charge un module IDSDM ou BOSS, ou si ceux-ci ne sont pas installés sur les serveurs au cours du déploiement, l'opération de déploiement sur ces serveurs est ignorée.

    Pour déployer un système d'exploitation sur le premier disque d'amorçage des serveurs, cochez la case **Déployer l'hyperviseur sur le premier disque d'amorçage des serveurs qui ne disposent pas d'un double module SD interne**.

  REMARQUE : La cible d'installation du Premier disque de démarrage n'est pas équivalente à la première entrée de la Séquence de disque dur du BIOS ou de la Séquence de démarrage UEFI. Cette option déploie le système d'exploitation sur le premier disque identifié par l'environnement ESXi pre-OS. Assurez-vous que les options Basculement du disque dur ou Réessayer la séquence de démarrage sont activées lorsque l'option **Premier disque de démarrage** est sélectionnée.
- **BOSS** : déploie un système d'exploitation sur la carte BOSS. Si un module BOSS équipe au moins l'un des serveurs sélectionnés, l'option BOSS est activée. Si ce n'est pas le cas, seule l'option **Premier disque d'amorçage** est disponible.

  Si vous utilisez OMIVV pour déployer un système d'exploitation sur le contrôleur BOSS, assurez-vous que le profil système est capturé à partir du serveur de référence avec la configuration BOSS VD et que le serveur cible doit avoir une carte BOSS de configuration similaire. Pour en savoir plus sur la création du DV, voir le *Guide de l'utilisateur du stockage serveur optimisé-S1 pour le démarrage Dell EMC* sur www.dell.com/support.

9. Sur la page **Sélectionner un profil d'identification d'hôte**, exécutez les tâches suivantes :

a. Pour utiliser le même profil d'identification de l'hôte pour tous les hôtes, cliquez sur **OUI**, puis procédez comme suit :

i. Sélectionnez le profil d'identification de l'hôte dans le menu déroulant.
ii. Saisissez le mot de passe.

Les éléments suivants sont applicables à l'utilisateur root lors du déploiement :

- Pour ESXi 6.5 et les versions supérieures, le mot de passe saisi dans le profil d'identification de l'hôte est utilisé.
- Pour ESXi 6.7 et les versions supérieures, le mot de passe saisi dans l'assistant de déploiement est utilisé.
- Pour ESXi 6.5 et les versions antérieures, si le mot de passe n'est pas défini dans le profil d'identification de l'hôte, le mot de passe saisi dans l'Assistant de déploiement est utilisé. Mettez à jour les informations d'identification de l'ESXi dans le profil d'identification de l'hôte pour garantir l'exécution réussie de l'inventaire après le déploiement du système d'exploitation.

b. Pour sélectionner le profil d'identification de l'hôte individuel pour chaque serveur, cliquez sur **NON**, puis effectuez procédez comme suit :

i. Sélectionnez le profil d'identification de l'hôte dans le menu déroulant.
ii. Entrez le mot de passe racine. Pour afficher le mot de passe saisi, cliquez sur l'icône en forme d'œil.

Assurez-vous de saisir le bon mot de passe, car l'option Confirmer le mot de passe n'est pas disponible.

REMARQUE : Si les informations d'identification AD sont utilisées pour l'iDRAC ou l'ESXi dans le profil d'identification de l'hôte, ces profils ne sont pas pris en compte pour un déploiement de système d'exploitation.

REMARQUE : Dans le profil d'identification d'hôte, il vous est recommandé d'associer l'utilisateur qui est utilisé pour la détection sans système d'exploitation, sinon l'utilisateur détecté est désactivé dans l'iDRAC après le déploiement du système d'exploitation.

10. Dans la page **Configurer les paramètres réseau**, exécutez les tâches suivantes :
    a. Entrez le FQDN (Nom de l'hôte complètement qualifié) du serveur. Un nom de domaine complètement qualifié pour le nom de l'hôte est obligatoire. 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. Créez un enregistrement DNS qui résout l'adresse IP avec le FQDN. 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.

    REMARQUE : Si vCenter est inscrit avec OMIVV à l'aide du FQDN, assurez-vous que l'hôte ESXi peut résoudre le FQDN à l'aide de la résolution DNS.

    b. Sélectionnez la carte NIC qui est utilisée pour le réseau de gestion. Assurez-vous que la carte NIC est connectée.

    REMARQUE : Veillez à sélectionner les cartes réseau de gestion en fonction de la connectivité réseau à OMIVV. L'option **APPLIQUER LES PARAMÈTRES À TOUS LES SERVEURS** n'est pas applicable pour la sélection de la carte NIC de gestion.

    c. Sélectionnez l'instance réseau OMIVV qui a accès à vCenter. Pour plus d'informations, voir Déploiement de profil système et de profil ISO , page 65.
    d. Sélectionnez l'une des options réseau suivantes :
    - Dans le cas des paramètres statiques, saisissez le serveur DNS souhaité, le serveur de DNS auxiliaire, l'adresse IP, le masque de sous-réseau et la passerelle par défaut.
    - **Utiliser un VLAN** : lorsqu'un ID VLAN est fourni, il est appliqué à l'interface de gestion du système d'exploitation 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. Pour plus d'informations, voir Prise en charge de la technologie VLAN , page 69.
    - **Utiliser un DHCP** : l'adresse IP attribuée au DHCP est utilisée 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.

11. Sur la page **Tâche de planification du déploiement**, procédez comme suit :
    a. Saisissez le nom et la description de la tâche de déploiement.
    b. Pour exécuter la tâche de déploiement immédiatement, cliquez sur **Exécuter maintenant**.
    c. Pour planifier l'exécution de la tâche ultérieurement, cliquez sur **Planifier pour plus tard**, puis sélectionnez la date et l'heure.
    d. Cochez la case **Accéder à la page Tâches après la soumission de la tâche**.
    Vous pouvez consulter l'état de la tâche sur la page **Tâches**. Pour plus d'informations, voir Tâches de déploiement , page 76.
12. Cliquez sur **TERMINER**.

    REMARQUE : Après avoir effectué le déploiement d'un système d'exploitation sur des serveurs sur matériel vierge, OMIVV efface toutes les tâches iDRAC.

    La tâche de déploiement de profil ISO planifiée dans une version antérieure d'OMIVV n'est pas valide dans la dernière version d'OMIVV. Annulez la tâche planifiée et créez une tâche de déploiement selon vos besoins.

    La tâche de déploiement échoue si la tâche planifiée n'est pas annulée. Dans ce cas, découvrez le serveur en tant que matériel vierge et créez une tâche de déploiement de profil ISO.

Déploiement du profil système et du profil ISO

Vous pouvez effectuer le déploiement uniquement sur les serveurs conformes sur matériel vierge. Pour plus d'informations, voir Affichage des serveurs sur matériel vierge , page 55.

1. Pour lancer l'assistant de déploiement, accédez à **Conformité et déploiement** > **Déploiement** > **DÉPLOYER**.

2. Sur la page **Check-list pour le déploiement de profil système et de profil ISO** de l'assistant de déploiement, vérifiez la liste de vérification du déploiement, puis cliquez sur **DÉMARRER**.
3. Sur la page **Sélectionner le ou les serveurs**, sélectionnez un ou plusieurs serveurs.
   La page **Sélectionner les options de déploiement** s'affiche.
4. Sur la page **Sélectionner les options de déploiement**, sélectionnez **Profil système (configuration du matériel)** et **Profil ISO (Installation ESXi)**.
5. Dans le menu déroulant **Nom du vCenter**, sélectionnez une instance de vCenter.
6. Pour sélectionner le vCenter de destination, cliquez sur **PARCOURIR**, puis sélectionnez le datacenter ou le cluster approprié sur lequel vous souhaitez déployer le système d'exploitation.
7. Pour utiliser le profil système associé au profil de cluster sélectionné, cliquez sur **Confirmer**.
   - Pour sélectionner un autre profil système, cliquez sur **Sélectionner un autre profil**. Il vous est recommandé de sélectionner le profil système associé au cluster afin d'éviter une dérive de la conformité de la configuration.
8. Dans le menu déroulant **Profil ISO**, sélectionnez un profil ISO approprié, puis cliquez sur **Suivant**.
9. Pour créer une tâche d'aperçu sur iDRAC, accédez à la page **Aperçu de la configuration**, puis sélectionnez une adresse IP iDRAC et cliquez sur **APERÇU**. L'aperçu de la configuration est une tâche facultative.
   L'opération d'aperçu du profil système peut prendre quelques minutes. L'état de comparaison s'affiche dans la colonne **Résultat**.

   Les résultats de la comparaison sont les suivants :
   - **Terminé** : la tâche d'aperçu a été exécutée correctement. Pour plus d'informations sur les résultats de la comparaison, cliquez sur **Afficher les détails** dans la colonne **Détails**.
   - **Non terminé** : la tâche d'aperçu n'a pas été exécutée correctement sur l'iDRAC. Assurez-vous qu'iDRAC est accessible et effectuez une réinitialisation d'iDRAC, le cas échéant. Pour plus d'informations sur la tâche, reportez-vous aux journaux OMIVV et aux journaux sur la console d'iDRAC.
10. Suivez les étapes 7 à 10 répertoriées dans la rubrique Déploiement d'un profil ISO (installation ESXi) , page 67.

Prise en charge de la technologie VLAN

OMIVV prend en charge le déploiement du système d'exploitation vers un VLAN routable. Vous pouvez configurer la prise en charge du VLAN dans l'assistant de déploiement. Dans cette partie de l'assistant de déploiement, il existe une option permettant de spécifier les VLAN à l'aide d'un ID VLAN. Lorsqu'un ID VLAN est fourni, il est appliqué à l'interface de gestion du système d'exploitation lors du déploiement et marque l'ensemble du trafic doté de l'ID VLAN.

Assurez-vous que le VLAN fourni lors du déploiement communique avec l'appliance OMIVV et le serveur vCenter. Le déploiement d'un système d'exploitation vers un VLAN qui ne peut pas communiquer avec l'une ou l'autre de ces destinations provoque l'échec du déploiement.

Si vous avez sélectionné plusieurs serveurs sur matériel vierge dans une tâche de déploiement unique et si vous souhaitez appliquer le même ID VLAN à tous les serveurs, dans la section Identification du serveur de l'assistant de déploiement, utilisez l'option **APPLIQUER LES PARAMÈTRES À TOUS LES SERVEURS SÉLECTIONNÉS**. 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 : Veillez à sélectionner les cartes réseau de gestion en fonction de la connectivité réseau à OMIVV. L'option **APPLIQUER LES PARAMÈTRES À TOUS LES SERVEURS** n'est pas applicable pour la sélection de la carte NIC de gestion.

Synchronisation de la tâche de déploiement

Le déploiement de profils système et de profils ISO peut 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 déploiement du profil système et du profil ISO varie en fonction du type de déploiement, de la complexité et du nombre de tâches de déploiement exécutées simultanément. Les tâches de déploiement sont exécutées par lots d'un maximum de cinq serveurs simultanés afin d'améliorer la durée de la tâche de déploiement globale. Le nombre exact de tâches simultanées dépend des ressources disponibles.

Le tableau suivant affiche la valeur moyenne et peut varier en fonction de facteurs tels que la configuration du serveur, la génération du serveur et le nombre de serveurs sur matériel vierge dont le déploiement est prévu :

Tableau 3. Durée approximative du déploiement d'un seul serveur

Type de déploiement	Durée approximative par déploiement
Profil ISO uniquement	De 30 à 130 minutes
Profil système uniquement	De 5 à 6 minutes
Profil système et profil ISO	30-130 minutes

État du serveur dans la séquence de déploiement

Les serveurs détectés lors de la découverte automatique ou manuelle 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 ces états pour vérifier l'état de la configuration matérielle.

Tableau 4. États du serveur dans la séquence de déploiement

État du serveur	Description
Non configuré	Le serveur a été ajouté à OMIVV et attend d'être configuré.
Configuré	Le serveur est configuré avec toutes les informations matérielles requises pour réussir le déploiement du système d'exploitation.

11

Conformité

Gestion de la conformité

Pour afficher et gérer les hôtes dans OMIVV, chaque hôte doit répondre à certains critères. Si les hôtes ne sont pas conformes aux critères de conformité, OMIVV ne les gérera pas et ne les surveillera pas. OMIVV affiche les détails de la non-conformité d'un serveur ou d'un hôte, et vous permet de remédier à cette non-conformité, le cas échéant.

L'hôte est non conforme si :

- L'hôte n'est pas associé à un profil d'identification d'hôte.
- 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.

  REMARQUE : L'état CSIOR n'est pas déterminé lorsque les hôtes sont gérés à l'aide d'un châssis.
- 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 peut se produire lorsque l'iDRAC ou les informations d'identification de l'hôte fournies par le profil d'identification d'hôte ne sont pas valides. Ou, aucun logement n'est libre dans l'iDRAC, ou le mode de verrouillage de l'iDRAC est activé uniquement sur les serveurs basés sur l'iDRAC9. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.
- OMIVV n'a pas activé le service WBEM sur les hôtes exécutant ESXi 6.5 ou versions ultérieures.
- La version du firmware de l'iDRAC est antérieure à la version 2.50.50.50. La version 2.50.50.50 ou ultérieure de l'iDRAC est uniquement requise pour utiliser la fonctionnalité de profil du système.
- La licence iDRAC n'est pas compatible (iDRAC Express est la configuration minimale requise). Les serveurs ne disposant pas d'une licence iDRAC compatible ne peuvent pas être utilisés pour la surveillance et la mise à jour de firmware.

PRÉCAUTION : Même s'ils ne sont pas conformes, les hôtes en mode Verrouillage ne sont pas affichés dans les tests de conformité. Assurez-vous de vérifier manuellement le niveau de conformité. Un message s'affiche lors d'une vérification manuelle. Ignorez le message. 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.

Sur la page **Gestion de la conformité**, vous pouvez effectuer les tâches suivantes :

- Corriger la conformité. Pour plus d'informations, voir Résolution d'un hôte non conforme , page 72.
- Exécuter l'inventaire. Le lien Exécuter une tâche d'inventaire est actif si l'état de l'iDRAC est défini sur **Non conforme** ou **Inconnu** pour l'un des hôtes associés à un profil d'identification de l'hôte.
- Renouveler la licence iDRAC. Pour plus d'informations, voir Résolution de la conformité à la licence iDRAC , page 73.
- Ajouter des hôtes OEM. Pour plus d'informations sur l'ajout d'hôtes OEM, voir Ajout d'hôtes OEM , page 73.

Affichage des hôtes non conformes

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Gestion de la conformité**.

Un tableau affiche tous les hôtes non conformes ainsi que les informations suivantes :

- **Hôte** : FQDN ou adresse IP de l'hôte
- **Modèle** : nom de modèle du serveur
- **Profil d'identification** : nom du profil d'identification de l'hôte
- **État CSIOR** : indique l'état CSIOR (**ACTIVÉ** ou **DÉSACTIVÉ**). L'état CSIOR indique **Non déterminé** pour les hôtes qui sont gérés à l'aide du châssis.
- **État des trap SNMP** : indique l'état des trap SNMP (**Configuré** ou **Non configuré**).
- **Hyperviseur** : nom et version de l'hyperviseur
- **État WBEM** : indique l'état WBEM (**Conforme** ou **Non conforme**). L'état CSIOR indique **Non applicable** pour les hôtes qui sont gérés à l'aide du châssis.

- **Version du firmware iDRAC** : version de firmware de l'iDRAC
- **État de la licence iDRAC** : indique l'état de la licence iDRAC (**Conforme** ou **Non Conforme**).

  REMARQUE : Lorsqu'un hôte PowerEdge MX est géré à l'aide d'un profil d'identification de châssis, la version du firmware iDRAC s'affiche comme **Non applicable** sur la page **Gestion de la conformité**. Cela est dû au fait que la conformité du firmware de l'iDRAC ne s'applique pas aux serveurs basés sur l'iDRAC9. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.

Résolution d'un hôte non conforme

L'hôte est non conforme si :

- L'hôte n'est pas associé à un profil d'identification d'hôte.
- 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.

  REMARQUE : L'état CSIOR n'est pas déterminé lorsque les hôtes sont gérés à l'aide d'un châssis.
- 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 peut se produire lorsque l'iDRAC ou les informations d'identification de l'hôte fournies par le profil d'identification d'hôte ne sont pas valides. Ou, aucun logement n'est libre dans l'iDRAC, ou le mode de verrouillage de l'iDRAC est activé uniquement sur les serveurs basés sur l'iDRAC9. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.
- OMIVV n'a pas activé le service WBEM sur les hôtes exécutant ESXi 6.5 ou versions ultérieures.
- La version du firmware de l'iDRAC est antérieure à la version 2.50.50.50. La version 2.50.50.50 ou ultérieure de l'iDRAC est uniquement requise pour utiliser la fonctionnalité de profil du système.
- La licence iDRAC n'est pas compatible (iDRAC Express est la configuration minimale requise). Les serveurs ne disposant pas d'une licence iDRAC compatible ne peuvent pas être utilisés pour la surveillance et la mise à jour de firmware.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Gestion de la conformité**.
2. Sélectionnez un hôte non conforme, puis cliquez sur **Corriger la conformité**.
3. Sur la page d'accueil de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
4. Sur la page **Sélectionner les hôtes**, sélectionnez un ou plusieurs hôtes non conformes et cliquez sur **SUIVANT**.
   - Si les hôtes ne sont pas associés à un profil d'identification d'hôte, le message d'avertissement suivant s'affiche :

     Certains des hôtes sélectionnés ne sont pas affectés à un profil d'identification d'hôte. Pour permettre à OMIVV d'exécuter une vérification de la conformité, vous devez ajouter ces hôtes à un profil d'identification d'hôte

     Pour exclure les hôtes qui ne sont pas affectés à un profil d'identification d'hôte, cliquez sur **CONTINUER**.

     Pour ajouter les hôtes à la page Profil d'identification d'hôte, cliquez sur **Annuler** et accédez à la page Profil d'identification d'hôte. Pour en savoir plus sur la création d'un profil d'identification d'hôte, voir Création du profil d'identification d'hôte , page 39.

     Les hôtes présents dans un châssis MX avec une IPv4 iDRAC désactivée doivent être gérés à l'aide du profil d'identification de châssis. Pour associer ces hôtes au profil d'identification de châssis, vous devez ajouter le châssis en utilisant Ajouter un châssis MX sur la page **Châssis Dell EMC**, puis en associant le châssis à un profil de châssis.

   Pour mettre à jour le firmware iDRAC et la version du BIOS, procédez comme suit :

   a. Sur la page **Mettre à jour le firmware iDRAC et la version du BIOS**, sélectionnez un ou plusieurs hôtes sur lesquels vous souhaitez mettre à jour la version du firmware.
   b. Cliquez sur **SUIVANT**.
   c. Sur la page **Redémarrer les hôtes**, visualisez les hôtes ESXi devant être redémarrés.
   d. Si vous souhaitez mettre automatiquement les hôtes en mode de maintenance et les redémarrer si nécessaire, cochez la case, puis cliquez sur **SUIVANT**.
   e. Sur la page **Résumé**, vérifiez le résumé des actions, puis cliquez sur **TERMINER**.

   Pour activer la fonction CSIOR, procédez comme suit :

   a. Sur la page **Sélectionner les hôtes**, sélectionnez un ou plusieurs hôtes non conformes et cliquez sur **SUIVANT**.
   b. Sur la page **Activer CSIOR**, sélectionnez un ou plusieurs hôtes pour lesquels vous souhaitez activer CSIOR, puis cliquez sur **SUIVANT**.
   c. Sur la page **Résumé**, vérifiez le résumé des actions, puis 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 des informations valides dans le profil d'identification de l'hôte et libéré l'un des quatre premiers logements disponibles dans la destination d'interruption de l'iDRAC ou si vous avez désactivé le mode System Lockdown dans l'iDRAC.

REMARQUE : Le mode System Lockdown s'applique uniquement aux serveurs basés sur l'iDRAC9.

S'il existe des hôtes non conformes WBEM, corrigez manuellement les conditions de ces hôtes qui provoquent l'échec de l'activation du service WBEM. Vous pouvez corriger les conditions d'erreurs en les affichant dans les journaux utilisateur. Activez OMIVV pour activer le service WBEM pour ces hôtes lors de l'inventaire.

Résolution de la conformité à la licence iDRAC

La licence iDRAC compatible est l'un des critères de conformité pour les hôtes. Si les hôtes n'ont pas de licence iDRAC compatible, ces hôtes sont répertoriés en tant qu'hôtes non conformes sur la page **Gestion de la conformité**.

Vous pouvez cliquer sur un hôte non conforme pour afficher des informations telles que la date d'expiration, le type de licence et la description de la licence iDRAC. Le lien de la tâche **EXÉCUTER L'INVENTAIRE** est actif si l'état de conformité de l'iDRAC est défini sur **Non conforme** ou **Inconnu** pour l'un des hôtes associés à un profil d'identification de l'hôte.

1. Pour corriger la conformité de la licence iDRAC, accédez à la page d'accueil d'OMIVV, puis cliquez sur **Conformité et déploiement** > **Conformité** > **Gestion de la conformité**.
2. Sélectionnez un hôte pour lequel la licence iDRAC n'est pas conforme, puis cliquez sur **RENOUVELER LA LICENCE iDRAC**.
3. Connectez-vous à Dell Digital Locker et mettez à jour ou achetez une nouvelle licence iDRAC.
   Après avoir installé une licence iDRAC, exécutez une tâche d'inventaire pour l'hôte et revenez sur cette page à la fin de celle-ci.

Prise en charge des serveurs OEM

Les serveurs OEM sont fournis par les partenaires Dell EMC, qui proposent des fonctionnalités ou des portefeuilles similaires aux serveurs PowerEdge.

- À partir d'OMIVV 4.3, les serveurs OEM de type Rack sont pris en charge.
- Ajoutez des serveurs OEM à l'aide de l'assistant **Ajouter des hôtes OEM**. Pour plus d'informations sur l'ajout d'hôtes OEM, voir Ajout d'hôtes OEM , page 73.

  REMARQUE : Si le service WBEM est déjà activé sur les hôtes OEM et qu'il est ajouté à vCenter, par défaut, OMIVV ajoute ces serveurs OEM à la liste gérée par OMIVV. Associez les hôtes au profil d'identification d'hôte pour gérer ces serveurs. Pour plus d'informations sur la création d'un profil d'identification d'hôte, voir Création du profil d'identification d'hôte , page 39.
- Après l'ajout des serveurs OEM, tous les processus de gestion de l'hôte seront identiques à ceux des serveurs Dell EMC PowerEdge.
- Les fonctionnalités de serveurs sur matériel vierge et de déploiement sont également pris en charge sur les serveurs OEM à l'aide d'iDRAC.

Ajout d'hôtes OEM

Outre les serveurs Dell EMC PowerEdge, OMIVV prend également en charge les serveurs démarqués ou renommés. Pour en savoir plus sur l'OEM, rendez-vous sur https://www.dellemc.com.

Si le service WBEM est déjà activé, OMIVV détermine la connectivité iDRAC de l'hôte. Si la connexion est disponible, OMIVV ajoute l'hôte à la liste gérée.

Si OMIVV ne parvient pas à déterminer la connectivité iDRAC de l'hôte, vous devez sélectionner manuellement l'hôte depuis l'assistant **Ajouter des hôtes OEM** afin que l'hôte soit ajouté à la liste gérée par OMIVV.

Si le service WBEM est désactivé ou si l'iDRAC n'est pas accessible, utilisez l'Assistant **Ajout d'hôtes OEM** pour que l'hôte soit ajouté à la liste gérée par OMIVV.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Conformité** > **Gestion de la conformité** > **Ajouter des hôtes OEM**.
2. Dans la fenêtre **Ajouter des hôtes OEM**, sélectionnez une instance vCenter dans la liste déroulante **Instance vCenter**.
3. Dans la liste déroulante **Profil d'identification d'hôte**, sélectionnez le profil d'identification d'hôte approprié.
4. Pour ajouter ou supprimer l'hôte associé, cliquez sur **AJOUTER UN HÔTE**.
   La fenêtre **Sélectionner des hôtes** s'affiche.

5. Dans la fenêtre **Sélectionner des hôtes**, sélectionnez les hôtes et cliquez sur **OUI**.

   REMARQUE : Seuls les hôtes qui ne sont pas gérés par OMIVV s'affichent dans la fenêtre **Sélectionner des hôtes**.

   OMIVV teste la connexion automatiquement et les résultats de ce test sont affichés dans la fenêtre **Ajouter des hôtes OEM**.

   Les colonnes **Test d'iDRAC** et **Test de l'hôte** affichent les résultats des tests de connexion pour les **Informations d'identification d'iDRAC** et les **Informations d'identification de l'hôte**.

   Pour arrêter tous les tests de connexion, cliquez sur **ANNULER LE TEST**.
6. Cliquez sur **OK**.
   Les hôtes sélectionnés sont ajoutés au profil d'identification d'hôte sélectionné et l'inventaire est déclenché.

Conformité de la configuration

La page **Conformité de la configuration** affiche l'état de conformité définit en fonction de la détection de dérive de tous les clusters associés au profil de cluster. Dans un environnement PSC avec plusieurs serveurs vCenter, la page Conformité de la configuration répertorie tous les clusters de tous les vCenters qui appartiennent au même PSC, inscrits avec la même appliance.

- Conformité de la configuration matérielle : affiche la dérive des attributs entre le profil système utilisé dans le profil de cluster et les hôtes vSAN associés qui font partie du cluster.
- Conformité du firmware : affiche la dérive de la version du firmware entre le profil de logithèque du firmware utilisé dans le profil de cluster et les hôtes associés qui font partie du cluster.
- Conformité du pilote : affiche la dérive de la version du pilote entre le profil de logithèque de pilotes utilisé dans le profil de cluster et les hôtes vSAN associés qui font partie du profil de cluster.

Affichage de la conformité de configuration

1. Sur la page d'accueil d'OMIVV, cliquez sur **Conformité et déploiement** > **Conformité** > **Conformité de la configuration**.
   Un tableau affiche les clusters avec le profil de cluster, le profil système, le profil de logithèque de firmwares et le profil de logithèque de pilotes qui lui sont associés.

   Pour les types de profils système de base et avancés, le nom du profil du système s'affiche au format suivant : Basic_<nom du profil système>, Advanced_<nom du profil système>.
2. Sur la page **Conformité de la configuration**, sélectionnez un cluster.
   Les informations de conformité de la configuration et l'état de conformité s'affichent.

   Les informations suivantes s'affichent dans la section **Conformité de la configuration** :

   - **Nom du cluster** : nom du cluster
   - **État de conformité** : indique l'état de conformité (conforme ou non conforme). Si l'un des hôtes du cluster n'est pas conforme, l'état indique Non conforme.
   - **Nombre d'hôtes** : nombre total d'hôtes présents dans le cluster.
   - **Planification** : date et heure auxquelles la tâche de détection de dérive suivante est planifiée.
   - **Heure de la dernière détection de dérive** : date et heure auxquelles la dernière tâche de détection de dérive est terminée.

   La section **État de conformité** affiche l'état de conformité du matériel, du firmware et des composants du pilote. Les différents états de conformité sont les suivants :

   - **Conforme** : affiche le nombre d'hôtes qui sont conformes aux composants matériels, firmwares et pilotes associés.
   - **Non conforme** : affiche le nombre d'hôtes qui ne sont pas conformes aux composants matériels, firmwares et pilotes associés.
   - **Non applicable** : affiche le nombre d'hôtes non applicables.

     La dérive du matériel n'est pas applicable pour les hôtes qui sont gérés à l'aide d'un profil d'identification de châssis.

     La dérive du pilote n'est pas applicable pour les hôtes qui font partie du cluster vSphere.

     Si le profil de cluster est créé à l'aide du catalogue en ligne, la conformité du firmware n'est pas applicable pour les clusters vSAN.
3. Pour afficher les détails de dérive, cliquez sur **AFFICHER LE RAPPORT DE DÉRIVE**. Ce lien est activé uniquement pour les clusters non conformes. Pour plus d'informations sur l'affichage du rapport de dérive, voir Affichage du rapport de dérive , page 75.

Affichage du rapport de dérive

La page **Rapport de conformité de la configuration** affiche les informations de dérive du matériel, du firmware et du pilote.

L'état de la tâche de détection de dérive s'affiche dans la section **Résumé**.

Pour le matériel :

- Nom de l'hôte ou adresse IP : indique l'adresse IP ou le nom de l'hôte.
- Numéro de série : affiche le numéro de série de l'hôte.
- État de dérive : indique l'état de dérive (non conforme ou en échec).
- 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 actuelle de l'attribut dans l'hôte.
- Valeur de la ligne de base : indique la valeur de la ligne de base.
- Type/Erreur 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 , page 180.

REMARQUE : La tâche de détection de dérive échoue uniquement lorsque l'hôte ou iDRAC n'est pas accessible. Si l'hôte ou iDRAC est inventorié avec succès, la tâche de détection de dérive s'affiche correctement. Pour vérifier les autres motifs d'échec de la tâche de détection de dérive, reportez-vous à la colonne **Type/Erreur de dérive** dans le rapport de dérive.

Pour le firmware et le pilote :

- Nom de l'hôte ou adresse IP : indique l'adresse IP ou le nom de l'hôte.
- Numéro de série : affiche le numéro de série de l'hôte.
- État de dérive : indique l'état de la dérive.
- Nom du composant : affiche le nom du composant.
- Valeur actuelle : indique la valeur actuelle de l'attribut dans l'hôte.
- Valeur de la ligne de base : indique la valeur de la ligne de base.
- Type/Erreur 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 , page 180.
- Importance (pour le firmware) : indique le niveau d'importance de la mise à jour de la version d'un composant identifié.
- Recommandation (pour le pilote) : indique la recommandation de mise à jour d'un composant du pilote.

REMARQUE : Si plusieurs versions du firmware sont disponibles, la version la plus récente est toujours utilisée pour la comparaison de conformité.

Vous pouvez utiliser l'option de filtre pour afficher les informations de dérive en fonction de l'état de celle-ci.

REMARQUE : Le lot de firmwares 32 bits n'est pas pris en charge dans la version 5.x. Si le profil de cluster est associé à un lot de firmwares 32 bits dans la version 4.x, l'état de dérive indique un échec lorsque vous exécutez la sauvegarde et la restauration de la version 4.x à la version 5.x. Utilisez le lot de firmwares 64 bits avec le profil de cluster et exécutez à nouveau la tâche de détection de dérive.

REMARQUE : Il est possible que vous remarquiez une incohérence entre OMIVV et le rapport de dérive de vSphere Lifecycle Manager. Cela est dû au fait que le vSphere Lifecycle Manager affiche toujours le rapport de dérive en temps réel et OMIVV affiche le rapport de dérive basé sur la date et l'heure planifiées. En cas d'incohérence entre les rapports de dérive, exécutez la tâche de détection de dérive à la demande sur la page **Tâches de détection de dérive**.

12

Gestion des tâches OMIVV

La page **Tâches** affiche les tâches suivantes :

- Déploiement
- Découverte
- Mises à jour de firmware
- Mode System Lockdown
- Détection de dérive
- Inventaire
- La garantie

OMIVV efface les tâches les plus anciennes lorsque le nombre total de tâches atteint 500, en incluant les tâches créées par l'utilisateur (par exemple, les tâches de déploiement) et les tâches créées par OMIVV (par exemple, la tâche de collecte des mesures d'intégrité). Si le nombre de tâches dépasse 500, les plus anciennes tâches au-delà de 500 sont supprimées.

Tâches de déploiement

Une fois les tâches de déploiement terminées, vous pouvez en suivre l'état sur la page **Tâches de déploiement**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Tâches de déploiement**.
   Un tableau affiche toutes les tâches de déploiement ainsi que les informations suivantes :
   - **Nom** : nom de la tâche de déploiement
   - **Description** : description de la tâche
   - **Heure planifiée** : date et heure auxquelles la tâche est planifiée.
   - **État** : état de la tâche de déploiement
   - **Taille de la collecte** : nombre de serveurs dans la tâche de déploiement
   - **Récapitulatif de progression** : informations sur la progression de la tâche de déploiement
2. Pour afficher plus d'informations sur les serveurs de la tâche de déploiement, sélectionnez une tâche de déploiement.
   Les informations suivantes sont affichées dans le volet inférieur :
   - **Numéro de série**
   - **IP iDRAC**
   - **État**
   - **Avertissements**
   - **Détails**
   - **Date et heure de début**
   - **Date et heure de fin**
   - **Plus de détails**

   a. Pour afficher plus d'informations à propos d'une tâche de déploiement, sélectionnez une tâche et passez votre pointeur sur la colonne **Détails**.
   b. Pour afficher plus d'informations sur l'échec des tâches basées sur le profil système, cliquez sur **Plus de détails**.
   Les informations suivantes s'affichent :
   - 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 système lorsque vous cliquez sur **Plus de détails**.
3. Pour interrompre une tâche de déploiement, cliquez sur **INTERROMPRE**.

4. Pour purger les tâches de déploiement, cliquez sur **SUPPRIMER LES TÂCHES TERMINÉES**, **Plus anciennes que la date et l'état de la tâche**, puis sur **Appliquer**.
   Les tâches sélectionnées sont alors supprimées de la page **Tâches de déploiement**.

Tâches de détection

Une fois la tâche de détection créée, vous pouvez en suivre le statut sur la page **Tâches de détection**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Tâches de détection**.
   Un tableau affiche toutes les tâches de détection, ainsi que les informations suivantes :
   - **Nom** : nom de la tâche de détection
   - **Description** : description de la tâche
   - **Heure planifiée** : date et heure auxquelles la tâche est planifiée.
   - **État** : état de la tâche de détection.

     L'état de la tâche indique Réussite lorsque le serveur est détecté correctement.

     En cas d'échec d'une tâche, le motif de l'échec s'affiche.
   - **Taille de la collecte** : nombre de serveurs dans la tâche de détection.
   - **Récapitulatif de progression** : informations sur la progression de la tâche de détection.
2. Pour afficher plus d'informations, sélectionnez une tâche de détection.
   Les informations suivantes sont affichées dans le volet inférieur :
   - **IP iDRAC**
   - **État**
   - **Détails**
   - **Date et heure de début**
   - **Date et heure de fin**
3. Pour purger la file d'attente des tâches de détection, cliquez sur **EFFACER LES TÂCHES TERMINÉES**.
   a. Sélectionnez la date.
      La tâche antérieure à la date sélectionnée a été supprimée.
   b. Sélectionnez l'état de la tâche.
   c. Cliquez sur **Appliquer**.

Tâches de mise à jour du firmware du châssis

Une fois les tâches de mise à jour du firmware du châssis terminées, vous pouvez afficher l'état de celles-ci sur la page de tâches **Mise à jour du firmware du châssis**.

1. Sur la page d'accueil de l'OMIVV, cliquez sur **Tâches** > **Mise à jour du firmware** > **Mise à jour du firmware du châssis**.
2. Pour afficher les dernières informations du journal, cliquez sur l'icône Actualiser.
   Un tableau affiche toutes les tâches de mise à jour du firmware du châssis ainsi que les informations suivantes :
   - **État** : état de la tâche de mise à jour du firmware.
   - **Heure planifiée** : heure de la tâche de mise à jour du firmware planifiée.
   - **Nom** : nom de la tâche.
   - **Description** : description de la tâche de mise à jour du firmware.
   - **vCenter** : nom du vCenter.
   - **Taille de la collection** : nombre de châssis dans la tâche de mise à jour de firmware.

     Le nombre total de châssis comprend uniquement les châssis maîtres et autonomes. Les châssis membres ne sont pas pris en compte.
   - **Récapitulatif de progression** : informations sur la progression de la tâche de mise à jour du firmware.
3. Pour afficher plus d'informations sur une tâche particulière, sélectionnez la tâche concernée.
   Les informations suivantes sont affichées dans le tableau inférieur :
   - **Numéro de série du châssis** : numéro de série du châssis.
   - **État** : état de la tâche.

- **Heure de début** : heure de début de la tâche de mise à jour du firmware.
- **Heure de fin** : heure de fin de la tâche de mise à jour du firmware.

4. Pour arrêter une mise à jour de firmware planifiée mais non exécutée, sélectionnez la tâche à annuler, puis cliquez sur **ARRÊTER**.

   AVERTISSEMENT : Si vous arrêtez une tâche de mise à jour des firmwares déjà soumise au châssis MX , le firmware peut encore être mis à jour sur l'hôte. OMIVV signale la tâche comme étant annulée.

5. Pour purger des tâches de mise à jour de firmware antérieures ou planifiées, cliquez sur **EFFACER LES TÂCHES TERMINÉES**.
   La boîte de dialogue **Purger des tâches de mise à jour de micrologiciel** s'affiche. Vous pouvez uniquement purger les tâches annulées, réussies ou échouées et ne pouvez pas purger les tâches planifiées ou actives.
6. Dans la boîte de dialogue **Purger des tâches de mise à jour de firmware**, sélectionnez **Antérieure à la date et à l'état de la tâche**, puis cliquez sur **OK**.
   Les tâches sélectionnées sont supprimées de la liste des tâches **Mise à jour du firmware du châssis**.

Tâches de mise à jour du firmware de l'hôte

Une fois les tâches de mise à jour du firmware du châssis terminées, vous pouvez afficher l'état de ces tâches sur la page de tâches **Mise à jour du firmware de l'hôte**.

1. Sur la page d'accueil de l'OMIVV, cliquez sur **Tâches** > **Mise à jour du firmware** > **Mise à jour du firmware de l'hôte**.
2. Pour afficher les dernières informations du journal, cliquez sur l'icône Actualiser.
   Un tableau affiche toutes les tâches de mise à jour du firmware de l'hôte ainsi que les informations suivantes :
   - **État** : état de la tâche de mise à jour du firmware.
   - **Heure planifiée** : heure de la tâche de mise à jour du firmware planifiée.
   - **Nom** : nom de la tâche.
   - **Description** : description de la tâche de mise à jour du firmware.
   - **vCenter** : nom du vCenter.
   - **Taille de la collection** : nombre de serveurs dans la tâche de mise à jour du firmware.
   - **Récapitulatif de progression** : informations sur la progression de la tâche de mise à jour du firmware.
3. Pour afficher plus d'informations sur une tâche particulière, sélectionnez la tâche concernée.
   Les informations suivantes sont affichées dans le tableau inférieur :
   - **Nom de l'hôte** : affiche le numéro de série de l'hôte
   - **État** : état de la tâche.
   - **Heure de début** : heure de début de la tâche de mise à jour du firmware.
   - **Heure de fin** : heure de fin de la tâche de mise à jour du firmware.

   REMARQUE : Si la tâche de mise à jour des firmwares est planifiée avec plusieurs DUP (Dell Update Packages) et que OMIVV ne parvient pas à télécharger certains des packages sélectionnés, OMIVV poursuit la mise à jour des packages téléchargés. La page des tâches affiche l'état des packages correctement téléchargés.
4. Pour arrêter une mise à jour de firmware planifiée mais non exécutée, sélectionnez la tâche à annuler, puis cliquez sur **ARRÊTER**.

   AVERTISSEMENT : Si vous arrêtez une tâche de mise à jour des firmwares déjà soumise au contrôleur iDRAC, le firmware peut encore être mis à jour sur l'hôte. OMIVV signale la tâche comme étant annulée.

5. Pour purger des tâches de mise à jour de firmware antérieures ou planifiées, cliquez sur **EFFACER LES TÂCHES TERMINÉES**.
   La boîte de dialogue **Purger des tâches de mise à jour de micrologiciel** s'affiche. Vous pouvez uniquement purger les tâches annulées, réussies ou échouées et ne pouvez pas purger les tâches planifiées ou actives.
6. Dans la boîte de dialogue **Purger des tâches de mise à jour de firmware**, sélectionnez **Antérieure à la date et à l'état de la tâche**, puis cliquez sur **OK**.
   Les tâches sélectionnées sont supprimées de la liste des tâches **Mise à jour du firmware de l'hôte**.

Tâches du mode de verrouillage du système

Le paramètre du mode de verrouillage du système est pris en charge uniquement pour les serveurs basés sur l'iDRAC9. 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. De plus, iDRAC doit posséder une licence d'entreprise pour activer le mode de verrouillage.

REMARQUE : Vous ne pouvez pas modifier le mode de verrouillage du système des hôtes qui sont gérés par un profil d'identification de châssis.

Une fois la configuration du verrouillage du système terminée, vous pouvez afficher l'état mis à jour du mode de verrouillage sur la page **Tâches du mode de verrouillage du système**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Mode de verrouillage du système**.
   Un tableau affiche toutes les tâches du mode de verrouillage du système ainsi que les informations suivantes :
   - **Nom** : nom de la tâche du mode de verrouillage du système
   - **Description** : description de la tâche
   - **Heure planifiée** : date et heure auxquelles la tâche du mode de verrouillage du système est planifiée.
   - **vCenter** : nom du vCenter.
   - **État** : état de la tâche du mode de verrouillage du système
   - **Taille de la collection** : nombre de serveurs dans la tâche du mode de verrouillage du système
   - **Récapitulatif de progression** : informations sur la progression de la tâche du mode de verrouillage du système
2. Pour afficher plus d'informations sur les serveurs inclus dans la tâche du mode de verrouillage du système, sélectionnez une tâche du mode de verrouillage du système.
   Les informations suivantes sont affichées dans le tableau inférieur :
   - **Numéro de service**
   - **IP iDRAC**
   - **Nom d'hôte**
   - **État**
   - **Détails**
   - **Date et heure de début**
   - **Date et heure de fin**

   Pour afficher plus d'informations à propos d'une tâche du mode de verrouillage du système, sélectionnez une tâche et passez votre curseur sur la colonne **Détails**.
3. Pour purger les tâches du mode de verrouillage du système, cliquez sur **EFFACER LES TÂCHES TERMINÉES**, **Antérieure à la date et à l'état de la tâche**, puis **APPLIQUER**.
   Les tâches sélectionnées sont alors supprimées de la page **Mode de verrouillage du système** .

Tâche 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.

REMARQUE : La tâche de détection de dérive échoue uniquement lorsque l'hôte ou iDRAC n'est pas accessible. Si l'hôte ou iDRAC est inventorié avec succès, la tâche de détection de dérive s'exécute correctement et vous pouvez afficher les informations pertinentes dans le rapport de dérive. Pour plus d'informations sur les rapports de dérive, voir Affichage du rapport de dérive , page 75.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Détection de dérive**.
   Un tableau affiche toutes les tâches de détection de dérive ainsi que les informations suivantes :
   - **Nom** : nom de la tâche de détection de dérive
   - **Dernière exécution** : date et heure d'exécution de la dernière tâche de détection de dérive.
   - **Prochaine exécution** : date et heure auxquelles la tâche de détection de dérive suivante est planifiée.
   - **État** : état de la tâche de détection de dérive
   - **Taille de la collection** : nombre de serveurs dans la tâche de détection de dérive
   - **Récapitulatif de progression** : informations sur la progression de la tâche de détection de dérive
2. Pour afficher les derniers détails de la tâche de détection de dérive, cliquez sur **Actualiser**.
3. Pour afficher plus d'informations sur les serveurs de la tâche de détection de dérive, sélectionnez une tâche de détection de dérive.
   Les informations suivantes s'affichent :
   - Numéro de service
   - IP iDRAC
   - Nom d'hôte
   - Cluster
   - vCenter

- État
- Date et heure de début
- Date et heure de fin

4. Pour exécuter la tâche **Détection des dérives** à la demande, cliquez sur **EXÉCUTER MAINTENANT**.

   Dans un cluster de base, après avoir ajouté un hôte au profil d'identification d'hôte ou au profil d'identification de châssis, la tâche de détection de dérive est automatiquement exécutée sur l'hôte nouvellement ajouté.

Affichage de la tâche d'inventaire de l'hôte

La page **Inventaire de l'hôte** affiche des informations sur la dernière tâche d'inventaire exécutée sur un hôte associé à un profil d'identification d'hôte.

1. Sur la page d'accueil de l'OMIVV, cliquez sur **Tâches** > **Inventaire** > **Inventaire de l'hôte**.
2. Sélectionnez un vCenter pour afficher toutes les informations sur les tâches d'inventaire des hôtes associés.

   - **vCenter** : FQDN ou adresse IP du serveur vCenter.
   - **Hôtes testés OK** : nombre d'hôtes pour lesquels l'inventaire a réussi
   - **Dernier inventaire** : date et heure d'exécution du dernier inventaire
   - **Prochain inventaire** : date et heure auxquelles le prochain inventaire est planifié

   Les détails des hôtes associés s'affichent dans le volet inférieur.

   - **Hôte** : FQDN ou adresse IP des hôtes.
   - **État** : affiche l'état de garantie de l'hôte. Options disponibles :
     - **Réussite**
     - **Échec**
     - **En cours**
   - **Durée (MM:SS)** : durée de la tâche d'inventaire, en minutes et secondes.
   - **Date et heure de début** : date et heure de début de la tâche d'inventaire
   - **Date et heure de fin** : date et heure de fin de la tâche d'inventaire.

Exécution de la tâche d'inventaire

Une fois la configuration initiale terminée, l'inventaire se déclenche automatiquement pour tous les hôtes ajoutés à un profil d'identification d'hôte.

1. Pour exécuter l'inventaire à la demande, cliquez sur **Tâches** > **Inventaire** > **Inventaire des hôtes**.
2. Cliquez sur **EXÉCUTER MAINTENANT**.
3. Pour afficher l'état de la tâche d'inventaire, cliquez sur **Actualiser**.
   Une fois la tâche d'inventaire terminée, vous pouvez consulter les informations de l'hôte sur la page **Informations sur l'hôte OMIVV**.
4. Pour afficher les informations de l'hôte OMIVV, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**
5. Dans le volet de gauche, sélectionnez un hôte.
6. Dans le volet de droite, sélectionnez **Surveiller**, puis cliquez sur **Informations sur l'hôte OMIVV**.
   Les informations suivantes s'affichent :

   - Inventaire du matériel
   - Stockage
   - Micrologiciel
   - Surveillance de l'alimentation
   - La garantie
   - Journal des événements système

   Lorsque les hôtes sont gérés à l'aide du profil d'identification de châssis, les données d'inventaire du firmware affichent quelques composants supplémentaires tels que Lifecycle Controller et le logiciel RAID.

   REMARQUE : Une tâche d'inventaire des hôtes excédant la limite de licences est ignorée et marquée comme Échouée.

7. Sur la page **Résumé**, dans la section **Informations sur l'hôte OMIVV**, vous pouvez également exécuter les opérations suivantes :

- Lancer la console Remote Access (iDRAC)
- Faire clignoter l'indicateur LED du serveur
- Configuration du mode de verrouillage du système

  Lorsque les hôtes sont gérés à l'aide du châssis, la fonction Configuration du mode de verrouillage du système n'est pas prise en charge.

- Exécutez l'assistant du firmware

Modification de la tâche d'inventaire des hôtes

Après avoir associé des hôtes à un profil d'identification d'hôte, vous devez planifier périodiquement un inventaire pour vous assurer que les informations d'inventaire des hôtes sont à jour. La fenêtre Tâches d'inventaire affiche l'état des tâches d'inventaire exécutées sur les hôtes.

Vous pouvez également modifier la planification de l'inventaire à partir de la page **Paramètres** > **Planification de la récupération des données** > **Récupération d'inventaire**.

1. Sur la page **Tâches**, sélectionnez une instance de vCenter, puis cliquez sur **MODIFIER LA PLANIFICATION**.
   La boîte de dialogue **Récupération des données d'inventaire** s'affiche.
2. Sous la section **Données d'inventaire**, procédez comme suit :
   a. Cochez la case **Activer la récupération des données d'inventaire (Recommandé)**.
   b. Sélectionnez le jour et l'heure d'extraction des données d'inventaire, puis cliquez sur **APPLIQUER**.
   c. Pour rétablir les paramètres, cliquez sur **EFFACER**.
   d. Pour exécuter une tâche d'inventaire maintenant, cliquez sur **EXÉCUTER MAINTENANT** sur la page **Tâches**.

   REMARQUE : Pour les serveurs qui n'ont pas de licence iDRAC Express ou Enterprise, l'inventaire échoue car la mise à niveau de la licence est nécessaire pour iDRAC.

   REMARQUE : Lorsque vous exécutez l'inventaire d'hôtes modulaires, les châssis correspondants sont automatiquement détectés. Si le châssis fait partie d'un profil d'identification de châssis, l'inventaire du châssis s'exécute automatiquement après l'inventaire de l'hôte.

Affichage de la tâche d'inventaire du châssis

La page **Inventaire du châssis** affiche des informations sur la dernière tâche d'inventaire exécutée sur un châssis associé à un profil d'identification de châssis.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Inventaire** > **Inventaire du châssis**.
2. Pour afficher des informations d'inventaire de châssis, sélectionnez un châssis.

   - **IP châssis/Nom de l'hôte** : adresse IP du châssis
   - **Numéro de série** : affiche le numéro de service du châssis. Le numéro de service est un identifiant unique fourni par le fabricant à des fins de support et de maintenance.
   - **État** : état du châssis
   - **Durée (MM:SS)** : durée de la tâche, en minutes et secondes.
   - **Date et heure de début** : date et heure de début de la tâche d'inventaire.
   - **Date et heure de fin** : date et heure de fin de la tâche d'inventaire.

   Dans un groupe MCM, l'inventaire s'exécute uniquement sur châssis maître. Les informations d'inventaire fournissent des données à la fois sur le châssis maître et le châssis membre.

   REMARQUE : La tâche d'inventaire du châssis n'est pas prise en charge sur les serveurs PowerEdge suivants : C6320P, C6320, C4130 et C6420.

   REMARQUE : Les serveurs lames de châssis MX ne sont pris en charge qu'avec les versions ESXi 6.5U2 et ultérieures. Si les versions ESXi précédentes sont déployées sur ces hôtes, le travail d'inventaire échoue dans OMIVV.

Exécution d'une tâche d'inventaire du châssis

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Inventaire du châssis**.
2. Sélectionnez un châssis, puis cliquez sur **EXÉCUTER MAINTENANT**.

   Une fois l'inventaire du châssis effectué, vous pouvez afficher les informations concernant le châssis sur la page **Hôtes et châssis** > **Châssis**.
3. Pour afficher les informations sur le châssis, sur la page **Châssis**, sélectionnez un châssis, puis cliquez sur **AFFICHER**.

   REMARQUE : Pendant l'inventaire, la destination d'interruption et les stratégies d'alerte sont configurées par OMIVV sur le châssis maître d'un groupe MCM.

   REMARQUE : Lorsque les hôtes sont gérés à l'aide d'un châssis, l'exécution de l'inventaire de châssis déclenche également l'inventaire des hôtes pour les hôtes. De plus, l'exécution de l'inventaire des hôtes déclenche l'inventaire des châssis.

Affichage de la garantie des hôtes

Une tâche de garantie est une tâche planifiée qui consiste à obtenir des informations de garantie depuis le site www.dell.com/support sur tous les systèmes. Assurez-vous que votre appliance OMIVV dispose d'une connectivité Internet pour extraire les informations de garantie. 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.

1. Sur la page d'accueil de l'OMIVV, cliquez sur **Tâches** > **Garantie** > **Garantie des hôtes**.
2. Sélectionnez un vCenter pour afficher les informations des hôtes associés.

   - **vCenters** : listes des vCenters.
   - **Hôtes testés OK** : nombre d'hôtes vCenter qui ont réussi le test.
   - **Dernière garantie** : date et heure d'exécution de la dernière tâche de garantie.
   - **Prochaine garantie** : date et heure d'exécution de la prochaine tâche de garantie.

   Les informations des hôtes associés s'affichent dans le volet inférieur.

   - **Hôte** : adresse IP de l'hôte.
   - **État** : affiche l'état de la tâche de garantie. Options disponibles :
     - Réussite
     - Échec
     - En cours
     - Planifié
   - **Durée (MM:SS)** : durée de la tâche de garantie, au format MM:SS.
   - **Date et heure de début** : date et heure de début de la tâche de garantie
   - **Date et heure de fin** : heure de fin de la tâche de garantie
3. Pour exécuter la garantie sur demande de l'hôte, cliquez sur **EXÉCUTER MAINTENANT**.

Modification de la tâche de garantie de l'hôte

Les tâches de garantie sont configurées à l'origine dans l'**Assistant de configuration initiale**. Vous pouvez également modifier des planifications de tâches de garantie sur la page **Paramètres** > **Planification de la récupération des données** > **Récupération de la garantie**.

1. Sur la page **Tâches**, développez la section **Garantie**, puis sélectionnez **Garantie des hôtes**.
2. Sélectionnez un vCenter, puis cliquez sur **MODIFIER LA PLANIFICATION**.
3. Sous la section **Données de garantie**, procédez comme suit :
   a. Cochez la case **Activer la récupération des données de garantie (Recommandé)**.
   b. Sélectionnez le jour et l'heure d'extraction des données de garantie, puis cliquez sur **APPLIQUER**.
   c. Pour rétablir les paramètres, cliquez sur **EFFACER**.

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. 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.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Tâches** > **Garantie** > **Garantie du châssis**.

   Un tableau affiche toutes les informations relatives à la tâche de garantie du châssis.

   - **IP du châssis/Nom de l'hôte** : adresse IP de l'hôte
   - **Numéro de série** : numéro de série du châssis
   - **État** : affiche l'état de la tâche de garantie. Options disponibles :
     - Réussite
     - Échec
     - En cours
     - Planifié
   - **Durée (MM:SS)** : durée de la tâche de garantie, au format MM:SS.
   - **Date et heure de début** : date et heure de début de la tâche de garantie.
   - **Date et heure de fin** : heure de fin de la tâche de garantie.

2. Pour exécuter la tâche de garantie sur demande du châssis, cliquez sur **EXÉCUTER MAINTENANT**.

13

Gestion des journaux

Afficher l'historique du journal

1. Sur la page **OpenManage Integration for VMware vCenter**, pour afficher tous les journaux, cliquez sur **Journaux**.
   Le processus de récupération du journal OMIVV récupère tous les journaux à partir de sa base de données. Le processus peut prendre quelques secondes en fonction de la taille du journal.
   - Pour exporter les données des journaux, cliquez sur  .
   - Pour trier les données de la grille, cliquez sur un en-tête de colonne.
   - Pour naviguer entre les pages, cliquez sur les icônes précédente et suivante.
   - Pour actualiser les journaux, cliquez sur l'icône d'actualisation dans le coin supérieur gauche.
2. Cliquez sur l'▼ pour filtrer les journaux en fonction des catégories et des plages de dates suivantes :
   Catégories :
   - **Toutes les catégories**
   - **Informations**
   - **Avertissement**
   - **Erreur**

   Date :
   - **La semaine dernière**
   - **Le mois dernier**
   - **L'année dernière**
   - **Plage personnalisée** : si vous sélectionnez cette option, indiquez les dates de début et de fin en cliquant sur l'icône du calendrier.
3. Après avoir sélectionné la catégorie et la date souhaitées, cliquez sur **APPLIQUER**.
   Vous pouvez afficher les journaux relatifs à la catégorie et à la plage de dates sélectionnées. La table de données des fichiers log affiche 100 journaux par page à la fois.
4. Pour effacer les données filtrées, cliquez sur **EFFACER LE FILTRE**.

14

Gestion des paramètres de l'appliance OMIVV

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

- Configurez les paramètres de notification d'expiration de la garantie. Pour plus d'informations, voir Configuration des notifications d'expiration de la garantie , page 85.
- Configurez les notifications de la dernière version de l'appliance. Pour plus d'informations, voir Configuration de la notification relative à la dernière version de l'appliance , page 86.
- Remplacez la gravité pour les alertes de Proactive HA. Pour plus d'informations, voir Remplacement de la gravité des notifications de mise à jour de l'intégrité , page 90.
- Configuration initiale. Pour en savoir plus, voir Configuration initiale , page 90
- Configurez et affichez les événements et alarmes. Pour plus d'informations, voir Configuration des événements et alarmes , page 96.
- Établissez ou modifiez les planifications de récupération des données pour l'inventaire et la garantie. Pour de plus amples informations, consultez Planification d'une tâche d'inventaire , page 109 et Planification des tâches de récupération de la garantie , page 109.

Gestion de plusieurs appliances

Si plusieurs vCenters partagent le même PSC et si ces vCenters sont inscrits auprès de plusieurs instances d'une appliance OMIVV, basculez entre les différentes instances d'OMIVV à l'aide de l'assistant Basculer entre les appliances.

Vous pouvez voir l'instance active d'OMIVVV sur la page d'accueil.

1. Sur la page d'accueil **OMIVV**, cliquez sur **MODIFIER**.
   - **Adresse IP/Nom** : FQDN ou adresse IP de l'appliance OMIVV.
   - **Version** : version actuelle de l'appliance OMIVV.
   - **État de conformité** : état (**Conforme** ou **Non conforme**) de l'appliance OMIVV en fonction de la version.
   - **État de la disponibilité** : état de la disponibilité de l'appliance OMIVV selon que les services OMIVV sont en cours d'exécution ou non. La mention **OK** ou **ERREUR** s'affiche pour indiquer l'état de fonctionnement des OMIVV.
   - **Serveurs vCenter enregistrés** : FQDN ou adresse IP du serveur vCenter enregistré.
   - **Actions** : nom de l'action (**SÉLECTIONNER** ou **SÉLECTIONNÉ**).
2. Sur la page **Basculer entre les appliances OMIVV**, cliquez sur **SÉLECTIONNER**.
3. Pour confirmer, cliquez sur **OUI**.
   Vous pouvez voir le changement de l'adresse IP de l'appliance sur la page d'accueil.

Configuration des notifications d'expiration de la garantie

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

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

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

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

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

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

Configuration des informations d'identification de déploiement

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

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

1. Sur la page d'accueil d'OMIVV, cliquez sur **Paramètres** > **Paramètres de l'appliance** > **Informations d'identification du déploiement**.
2. Saisissez les identifiants. Le nom d'utilisateur par défaut est **root** et le mot de passe est **calvin**.
   Assurez-vous de saisir le mot de passe en fonction de la stratégie de mot de passe utilisateur de l'iDRAC définie dans l'iDRAC. En outre, assurez-vous d'utiliser des caractères pris en charge par l'iDRAC.
3. Cliquez sur **APPLIQUER**.

Intégrité de la redondance des composants matériels - Proactive HA

Proactive HA est une fonctionnalité vCenter qui fonctionne avec OMIVV. Lorsque vous activez Proactive HA, la fonctionnalité protège vos charges applicatives proactivement en prenant des mesures basées sur la dégradation d'intégrité de la redondance des composants pris en charge dans un hôte.

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. Les états « modérément dégradé » sont représentés par *Avertissement* dans la colonne **Type** sur la page **Événements**.
- Critique (gravement dégradé) : le composant est affecté d'une panne critique.

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.

REMARQUE :

- Lors de la configuration des événements, il vous est recommandé de sélectionner l'option Publier tous les événements en tant que niveau de publication d'événement. Pour plus d'informations sur la configuration des événements, voir Configuration des événements et alarmes , page 96.
- Proactive HA est disponible uniquement sur les plateformes prenant en charge la redondance sur l'alimentation, le ventilateur et le module IDSDM.
- 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).

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 :

Tableau 5. 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
DellIDSDMRedundancy	Stockage	Événements de redondance de l'IDSDM **REMARQUE :** Lorsque les hôtes sont ajoutés à un cluster compatible Proactive HA en présence de composants IDSDM, assurez-vous que la redondance interne de la carte SD est configurée dans les paramètres iDRAC sur l'option **Miroir**.

Pour un hôte activé Proactive HA, les interruptions suivantes sont utilisées par OMIVV comme déclencheur pour déterminer l'intégrité redondante des composants :

Tableau 6. 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 du bloc d'alimentation	Le bloc d'alimentation détecte un avertissement	Avertissement

Tableau 6. Événements Proactive HA (suite)

Nom de l'événement	Description	Gravité
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
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 du 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

Configuration de Proactive HA pour les serveurs rack et tour

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

1. Créez un profil d'identification d'hôte et associez les hôtes à un profil d'identification d'hôte. Voir la section Création du profil d'identification d'hôte , page 39.
2. Vérifiez que l'inventaire des hôtes s'est terminé avec succès. Voir la section Affichage de la tâche d'inventaire de l'hôte , page 80.
3. Dans le contrôleur iDRAC, vérifiez que la destination d'interruption SNMP est définie sur l'adresse IP de l'appliance OMIVV.

REMARQUE : Veillez à confirmer la disponibilité d'un hôte pour un cluster Proactive HA à partir des données des journaux.

4. Activez Proactive HA sur un cluster. Voir Activation de Proactive HA sur un cluster.

Configuration de Proactive HA pour les serveurs modulaires

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 des composants du châssis (PSU et ventilateur) a une incidence sur tous les serveurs associés.

1. Créez un profil d'identification d'hôte et associez les hôtes à un profil d'identification d'hôte. Voir la section Création du profil d'identification d'hôte , page 39.
2. Vérifiez que l'inventaire des hôtes s'est terminé avec succès. Voir la section Affichage de la tâche d'inventaire de l'hôte , page 80.
   REMARQUE : Veillez à confirmer la disponibilité d'un hôte pour un cluster Proactive HA à partir des données des journaux.
3. Créez un profil d'identification de châssis pour le châssis associé. Voir la section Création d'un profil d'identification de châssis , page 44.
4. Vérifiez que l'inventaire du châssis s'est terminé avec succès. Voir la section Affichage de la tâche d'inventaire du châssis , page 81.
5. Lancez le contrôleur CMC ou OME-Modular et vérifiez que la destination d'interruption du châssis est définie sur l'adresse IP de l'appliance OMIVV. Pour plus d'informations sur la configuration des interruptions, voir le Guide de l'utilisateur du CMC et de OME-Modular disponible sur **dell.com/support**.
6. 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 d'identification d'hôte et être correctement répertoriés.
- Dans le cas d'un serveur modulaire, le châssis correspondant doit être ajouté au profil d'identification du châssis et correctement répertorié.

1. Dans le vSphere Client, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
   Tous les hôtes et clusters s'affichent dans le volet de gauche.
2. Sélectionnez un cluster dans le volet de droite, puis cliquez sur **vSphere DRS** > **MODIFIER**.
3. Sélectionnez l'option **vSphere DRS**, si elle n'est pas déjà sélectionnée.
4. Sélectionnez **Configurer** > **Disponibilité vSphere** > **Proactive HA** > **Modifier**.
   La page **Modifier les paramètres de cluster** s'affiche.
5. Sur la page **Modifier les paramètres de cluster**, sélectionnez **Proactive HA**.
6. Dans la section **Échecs et réponses** du menu déroulant, sélectionnez le niveau d'automatisation **Manuel** ou **Automatique**.
7. Pour la **Mesure corrective**, 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.
8. Cliquez sur **Fournisseurs**, puis sélectionnez **Dell Inc** pour le cluster.
9. Cliquez sur **ENREGISTRER**.

Après l'activation de Proactive HA sur un cluster, OMIVV initialise les états d'intégrité et de redondance Proactive HA et les envoie à vCenter. En fonction des notifications de mise à jour de l'intégrité envoyées par OMIVV, le serveur vCenter exécute l'action manuelle ou automatique que vous avez sélectionnée pour la **Mesure corrective**.

Pour remplacer la gravité existant, voir Remplacement de la gravité des notifications de mise à jour de l'intégrité , page 90.

Toutes les personnalisations effectuées sur le fournisseur de mise à jour d'intégrité Dell enregistré pour le cluster PHA sont restaurées sur les valeurs par défaut après la mise à niveau du RPM et les opérations de sauvegarde et de restauration.

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

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

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

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

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

1. Dans OpenManage Integration for Vmware vCenter, cliquez sur **Paramètres** > **Remplacer la gravité pour les alertes de Proactive HA**.
   La grille de données affiche tous les événements Proactive HA pris en charge. La grille de données comprend des colonnes pour les identifiants d'événements, la description de l'événement, le type du composant, la gravité par défaut et le remplacement de la gravité pour personnaliser la gravité de l'hôte et de ses composants.
2. Pour modifier la gravité d'un hôte ou d'un de ses composants, sélectionnez l'état souhaité dans la liste déroulante sous la colonne **Remplacer la gravité**.
   Cette stratégie s'applique à tous les hôtes Proactive HA sur tous les serveurs vCenter qui sont enregistrés avec OMIVV.
3. Répétez l'étape 2 pour tous les événements devant être personnalisés.
4. Effectuez l'une des actions suivantes :
   a. Pour enregistrer la personnalisation, cliquez sur **APPLIQUER**.
   b. Pour annuler le remplacement des paramètres de gravité, cliquez sur **ANNULER**.

   Pour réinitialiser les paramètres de gravité par défaut, cliquez sur **RÉTABLIR LES VALEURS PAR DÉFAUT**.

Configuration initiale

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

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

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

1. Sur la page **Bienvenue**, lisez les instructions, puis cliquez sur **DÉMARRER**.
2. Sur la page **Sélectionner un vCenter**, dans le menu déroulant **vCenters**, sélectionnez un vCenter spécifique ou **Tous les vCenters enregistrés**, puis cliquez sur **SUIVANT**.
   REMARQUE : Si vous disposez de plusieurs serveurs vCenter faisant partie du même PSC et enregistrés avec la même appliance OMIVV, et si vous choisissez de configurer un seul serveur vCenter, l'étape 2 doit être répétée jusqu'à ce que chaque vCenter soit configuré.
3. Sur la page **Créer un profil d'identification d'hôte**, cliquez sur **CRÉER UN PROFIL D'IDENTIFICATION D'HÔTE**.
   Pour plus d'informations sur la création d'un profil d'identification d'hôte, voir Création du profil d'identification d'hôte , page 39.

   Une fois les hôtes ajoutés au profil d'informations d'identification d'hôte, l'adresse IP d'OMIVV est automatiquement définie en tant que destination trap SNMP pour l'iDRAC de l'hôte. OMIVV active le service WBEM, puis le désactive après la récupération de l'adresse IP de l'iDRAC pour les hôtes exécutant ESXi 6.5 et versions supérieures.

   OMIVV utilise le service WBEM pour synchroniser correctement les relations de l'hôte ESXi et du contrôleur iDRAC. Si la configuration de la destination de trap SNMP échoue et/ou l'activation du service WBEM échoue pour certains hôtes, ceux-ci sont répertoriés comme non conformes. Pour afficher et corriger la non-conformité, voir Résolution d'un hôte non conforme , page 72 .
4. Sur la page **Configurer des paramètres supplémentaires**, procédez comme suit :
   a. Planification des tâches d'inventaire. Pour plus d'informations sur la planification de la tâche d'inventaire, voir Planification d'une tâche d'inventaire , page 109.
   b. Planification des tâches de récupération de la garantie. Pour plus d'informations sur la planification de la tâche de récupération de la garantie, voir Planification des tâches de récupération de la garantie , page 109.

      Si vous souhaitez modifier la planification de la tâche d'inventaire, accédez à **Paramètres** > **Paramètres vCenter** > **Planification de récupération des données** > **Récupération d'inventaire** ou **Tâches** > **Inventaire** > **Inventaire des hôtes**.

Si vous souhaitez modifier la planification de la tâche de récupération de la garantie, accédez à **Paramètres** > **Paramètres vCenter** > **Planification de récupération des données** > **Récupération de la garantie** ou **Tâches** > **Garantie**.

c. Configuration des événements et alarmes. Pour plus d'informations sur la configuration des événements et alarmes, voir Configuration des événements et alarmes , page 96.

d. Pour appliquer des paramètres individuels, cliquez sur le bouton **Appliquer** séparément, puis cliquez sur **SUIVANT**.

Il est vivement recommandé d'activer tous les paramètres supplémentaires. Si l'un des paramètres supplémentaires n'est pas appliqué, un message s'affiche pour indiquer que tous les paramètres supplémentaires sont obligatoires.

5. Sur la page **Étapes suivantes**, lisez les instructions, puis cliquez sur **TERMINER**.

Nous vous recommandons d'associer vos hôtes OMIVV à une ligne de base de configuration, car cela vous permet de surveiller étroitement les modifications de configuration qui se produisent dans les hôtes et les clusters associés. Une configuration de base peut être créée pour n'importe quel cluster une fois que les hôtes sont gérés avec succès par OMIVV. Pour créer une ligne de base de configuration, procédez comme suit :

- Créez un profil de logithèque de firmware et de pilote : cela vous aide à définir des versions de firmware et de pilote sur ligne de base.
- Créez un profil système : cela vous permet de définir des configurations matérielles sur ligne de base pour les hôtes.
- Créez un profil de cluster : pour créer une ligne de base réussie, sélectionnez des clusters, puis associez le firmware, les pilotes et les configurations matérielles.
- Les hôtes présents dans un châssis PowerEdge MX équipé d'un iDRAC IPv4 désactivé doivent être gérés à l'aide d'un profil d'identification de châssis.

Afficher l'état de la configuration initiale

Sur la page de l'assistant de configuration initiale, vous pouvez exécuter les tâches suivantes :

- Afficher l'état de la configuration initiale

  L'état de la configuration initiale indique Terminé uniquement lorsque tous les vCenters sont configurés avec le profil d'identification d'hôte, les événements et les alarmes, les tâches d'inventaire et de garantie.

- Lancer l'assistant de configuration initiale

Paramètres de mise à jour de firmware

Si vous cochez la case **Effacer les tâches et réinitialiser l'iDRAC**, toutes les tâches de l'iDRAC présentes dans la **file d'attente** sont effacées, puis l'iDRAC est réinitialisé avant la mise à jour de firmware sur l'hôte.

Le paramètre **Effacer les tâches et réinitialiser l'iDRAC** est utilisé lors de l'exécution des opérations suivantes :

- Mise à jour des firmwares à l'aide de OMIVV

  Ce paramètre peut être remplacé lors de la mise à jour des firmwares à l'aide de OMIVV. Toutefois, le remplacement du paramètre n'aura aucun impact sur les paramètres qui s'effectuent sur la page **Paramètres de mise à jour des firmwares**.

- Mesure corrective des firmwares à l'aide de vSphere Lifecycle Manager

  Ce paramètre ne peut pas être remplacé lors de la mesure corrective du firmware.

1. Cochez la case **Effacer les tâches et réinitialiser l'iDRAC**.
2. Cliquez sur **APPLIQUER**.

Affichage des informations de licence

Lorsque vous téléchargez une licence OMIVV, le nombre d'hôtes et de serveurs vCenter pris en charge s'affiche dans cet onglet.

Pour acheter une licence logicielle, cliquez sur **Acheter une licence** en regard de **Licence logicielle**. Pour plus d'informations, voir Achat d'une licence logicielle , page 93.

Les informations suivantes apparaissent sur la page **Licence** :

Type de licence	Description
Licences hôtes	• Licences disponibles Affiche le nombre de licences disponibles • Licences utilisées Affiche le nombre de licences en cours d'utilisation
Licences vCenter	• Licences disponibles Affiche le nombre de licences disponibles • Licences utilisées Affiche le nombre de licences en cours d'utilisation

La section **Gestion des licences** affiche les liens vers les éléments suivants :

- Portail des licences de produit (Digital Locker)
- Console d'administration

Gestion des licences d'OpenManage Integration pour VMware vCenter (OMIVV)

OMIVV possède deux types de licences :

- Licence d'évaluation : lorsque l'appliance OMIVV est mise sous tension pour la première fois, une licence d'évaluation est installée automatiquement. La version d'essai contient une licence d'évaluation pour cinq hôtes (serveurs) gérés par OMIVV. Cette version d'évaluation de 90 jours est la licence par défaut fournie lors de l'expédition.
- Licence standard : vous pouvez acheter n'importe quel nombre de licences hôtes gérées par OMIVV. Cette licence inclut un support produit et des mises à jour de l'appliance OMIVV. La licence standard est disponible pour une période de trois ou cinq ans. Toute licence supplémentaire achetée prolonge la période de la licence existante.

La durée de la licence pour une clé XML unique est calculée à partir de la date de vente indiquée sur la commande d'origine. Toutes les nouvelles licences téléchargées seront incluses dans le nombre après la fin de la période de grâce de 90 jours pour toute licence antérieure ou expirée.

OMIVV prend en charge jusqu'à 15 instances vCenters. Lorsque vous effectuez la mise à niveau de la licence d'évaluation vers une licence standard complète, vous recevez un e-mail de confirmation de 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**.

Lorsque vous achetez une licence, le fichier .XML (clé de licence) est téléchargeable sur Dell Digital Locker à l'adresse **https://www.dell.com/support**. Si vous ne parvenez pas à télécharger vos clés de licence, contactez le service de support Dell en vous rendant sur **Contacter le support Commandes** à l'adresse **https://www.dell.com/support** pour trouver le numéro de téléphone du service du support Dell de votre zone géographique pour votre produit.

Les licences présentent les informations suivantes dans la console Administration OMIVV :

- Licences de connexions vCenter maximales : jusqu'à 15 connexions vCenter enregistrées et utilisées sont autorisées.
- Nombre maximum de licences de connexions hôte : nombre de connexions hôte achetées (avec un maximum de 2000 hôtes pris en charge pour une seule instance OMIVV).
- En cours d'utilisation : le nombre de connexions vCenter ou connexions hôte utilisées. Pour les connexions hôte, ce nombre représente le nombre d'hôtes (ou de serveurs) répertoriés.
- Disponibles : nombre de licences de connexions vCenter ou de connexions hôte disponibles pour un usage ultérieur.

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

REMARQUE : Vous pouvez utiliser n'importe quelle licence active pour les versions OMIVV 5.x. Les licences sauvegardées à partir d'instances précédentes d'OMIVV ou téléchargées à partir de Digital Locker peuvent être utilisées pour les instances actuelles d'OMIVV.

Achat d'une licence logicielle

1. Accédez à **Paramètres** > **Licences** > **Acheter une licence**, ou **Tableau de bord** > **Acheter une licence**, ou **Portail administrateur** > **Inscription vCenter** > **Licence** > **ACHETER MAINTENANT**.
   La page de support DellEMC s'affiche.
2. Téléchargez et enregistrez le fichier de licence à un emplacement connu.
   Le fichier de licence peut être compressé dans un fichier zip. Assurez-vous de décompresser le fichier zip et de charger uniquement le fichier .xml de licence. Le nom du fichier de la licence peut correspondre à votre numéro de commande (par exemple : 123456789.xml).

Accès aux informations de support

Tableau 7. Informations sur la page du support

Nom	Description
Documentation de support	Fournit les liens vers la documentation suivants : • Serveurs PowerEdge • Manuels OMIVV • iDRAC avec Lifecycle Controller
Console d'administration	Fournit un lien vers la Console Administration.
Aide générale	Fournit un lien vers le site de support Dell EMC.
Réinitialisation de l'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. Pour de plus amples informations concernant la réinitialisation de l'iDRAC, voir Réinitialisation de l'iDRAC , page 93.
Avant de contacter le support technique	Offre des conseils sur la façon de contacter le support de Dell EMC 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 Création et téléchargement d'un lot de dépannage , page 93.
Recommandations de Dell EMC	Fournit un lien vers la page de support de Dell EMC Repository Manager (DRM). Le DRM est utilisé pour créer un catalogue personnalisé, qui peut être utilisé pour mettre à jour la détection du firmware et de la dérive.

Création et téléchargement d'un lot de dépannage

Pour générer le lot de dépannage, assurez-vous que vous vous connectez au portail Administration.

Le lot de dépannage contient des informations de connexion à l'appliance virtuelle OpenManage Integration qui peuvent être utilisées pour vous aider à résoudre des problèmes ou être envoyées au support technique. OMIVV ne consigne pas les données sensibles de l'utilisateur.

1. Sur la page **Support**, cliquez sur **Créer et télécharger un lot de dépannage**.
   La boîte de dialogue **Lot de dépannage** s'affiche.
2. Dans la boîte de dialogue **Lot de dépannage**, cliquez sur **CRÉER**.
   En fonction de la taille des journaux, la création du lot peut parfois être longue.
3. Pour enregistrer le fichier, cliquez sur **TÉLÉCHARGER**.

Réinitialisation de l'iDRAC

La réinitialisation du contrôleur iDRAC entraîne un redémarrage normal de celui-ci. Après la réinitialisation d'iDRAC, iDRAC est normalement redémarré, mais pas l'hôte. Après la réinitialisation, iDRAC ne peut être utilisé qu'au bout de quelques minutes. Procédez à la réinitialisation uniquement si iDRAC ne répond pas sur une appliance OMIVV.

- Vous pouvez effectuer cette réinitialisation seulement sur un hôte qui fait partie d'un profil d'identification d'hôte et qui a été inventorié au moins une fois.
- Dell EMC vous recommande de basculer l'hôte en mode maintenance, puis de réinitialiser iDRAC.
- Une fois iDRAC réinitialisé, si iDRAC devient inutilisable ou cesse de répondre, réinitialisez-le. Pour plus d'informations sur la réinitialisation matérielle, reportez-vous au Guide de l'utilisateur d'iDRAC, disponible sur https://www.dell.com/support/.

Lors de la réinitialisation de l'iDRAC, vous verrez peut-être :

- Retard de communication alors que l'OMIVV récupère l'état d'intégrité de l'hôte.
- Toutes les sessions actuellement ouvertes dans iDRAC sont terminées.
- Modification de l'adresse DHCP de l'iDRAC. Si iDRAC utilise le protocole DHCP pour générer son adresse IP, l'adresse IP d'iDRAC peut être modifiée. Dans ce cas-là, réexécutez la tâche d'inventaire des hôtes pour obtenir la nouvelle adresse IP d'iDRAC dans les données d'inventaire.

1. Sur la page **Support**, cliquez sur **RÉINITIALISER iDRAC**.
2. Sur la page **RÉINITIALISER iDRAC**, saisissez le nom de l'hôte ou l'adresse IP.
3. Pour confirmer que vous comprenez bien le processus de réinitialisation d'iDRAC, sélectionnez l'option **Je comprends les conséquences de la réinitialisation d'iDRAC.** Case à cocher **Continuer à réinitialiser iDRAC sur l'hôte sélectionné**.
4. Cliquez sur **Réinitialiser iDRAC**.

15

Gestion des paramètres de vCenter

À propos des événements et des alarmes

Sur la page **Paramètres**, vous pouvez activer les événements et les alarmes pour les hôtes et châssis, mais aussi sélectionner le niveau de publication d'événement et restaurer les alarmes par défaut. Vous pouvez configurer des événements et alarmes pour chaque vCenter ou pour tous les serveurs vCenter inscrits. Les événements et les alarmes correspondant à un châssis sont associés au vCenter.

Voici les quatre niveaux de publication d'événement :

Tableau 8. Niveau de publication d'événement

Événement	Description
Ne pas publier d'événement	Ne pas autoriser OMIVV à transférer les événements ou les alertes dans les vCenters qui lui sont associés.
Publier tous les événements	Publier tous les événements, notamment les événements non formels, qu'OMIVV reçoit des hôtes Dell EMC gérés dans les vCenters associés. Il est recommandé de sélectionner l'option **Publier tous les événements** comme niveau de publication d'événement.
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 les événements et les alarmes, 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. OMIVV transfère les événements reçus des hôtes gérés à vCenter 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 tombe en panne et qu'une alarme est créée, la machine passe en mode de 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. Dell EMC recommande d'activer l'option DRS avant d'activer les alarmes Dell. Pour en savoir plus, voir la documentation VMware.

L'option 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 souhaitez restaurer les paramètres d'alarme par défaut, sélectionnez l'option **Restaurer les alarmes**. Cette option vous permet de restaurer la configuration d'alarme par défaut sans désinstaller et réinstaller le produit. Si des configurations d'alarme Dell EMC ont été modifiées depuis l'installation, ces changements sont annulés lorsque vous utilisez l'option **Restaurer les alarmes**.

REMARQUE : Pour recevoir les événements de Dell, veillez à activer les événements requis dans iDRAC, CMC et le contrôleur de gestion.

REMARQUE : OMIVV 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.

Configuration des événements et alarmes

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

1. Sur la page d'accueil OMIVV, cliquez sur **Paramètres** > **Paramètres vCenter** > **Événements et alarmes**.
2. Pour activer les alarmes pour tous les hôtes et leur châssis, cliquez sur **Activer les alarmes pour tous les hôtes et leur châssis**. La page **Activation des avertissements d'alarmes Dell EMC** affiche les clusters et l'hôte non mis en cluster qui peuvent être affectés après l'activation des alarmes Dell EMC.

   REMARQUE : Les hôtes Dell EMC pour lesquels les alarmes sont activées répondent à certaines événements critiques en entrant en mode de maintenance. Vous pouvez modifier l'alarme, si nécessaire.

   REMARQUE : Dans vCenter 6.7 U1 et 6.7 U2, l'option de modification échoue. Pour modifier les définitions d'alarme, nous vous recommandons d'utiliser le client Web (FLEX).

   REMARQUE : Les interruptions BMC n'ont pas d'ID de message, de sorte que les alertes ne possèdent pas ces détails dans OMIVV.
3. Pour accepter la modification, cliquez sur **CONTINUER**.
   Les alarmes pour tous les hôtes et leurs châssis sont activées.
4. Sélectionnez un des niveaux de publication d'événement suivants :
   - **Ne pas publier d'événements** : ne pas transférer d'événements ou d'alertes dans ses vCenters associés.
   - **Publier tous les événements** : publier tous les événements, y compris les événements d'information et les événements reçus des hôtes et du châssis et gérés dans ses vCenters associés. Nous vous recommandons de sélectionner l'option Publier tous les événements comme niveau de publication d'événement.
   - **Publier uniquement les événements de type Critique et Avertissement** : publier uniquement les événements de niveau critique et d'avertissement dans ses vCenters associés.
   - **Publier uniquement les événements relatifs à la virtualisation** : publier les événements liés à la virtualisation reçus des hôtes dans ses vCenters associés. Les événements liés à la virtualisation sont ceux qui sont les plus critiques pour les hôtes exécutant des machines virtuelles.
5. Pour enregistrer les modifications, cliquez sur **APPLIQUER**.

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

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

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

Affichage des événements du châssis

1. Dans le vSphere Client, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
2. Dans le volet de gauche, sélectionnez une instance de vCenter.
3. Dans le volet de droite, cliquez sur **Surveillance** > **Tâches et événements** > **Événements**.
4. Pour afficher plus d'informations, sélectionnez un événement spécifique.

   REMARQUE : Pour un châssis PowerEdge MX avec une configuration MCM, la source de l'événement sera affichée en tant que châssis maître. Cependant, les détails du message auront le numéro de série du châssis membre pour identification.

Affichage des alarmes de châssis

1. Dans le vSphere Client, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
2. Dans le volet de gauche, sélectionnez une instance de vCenter.
3. Dans le volet de droite, cliquez sur **Surveiller** > **Problèmes et alarmes** > **Alarmes déclenchées**.

4. Dans **Alarmes déclenchées**, cliquez sur le nom de l'alarme pour afficher la définition de celle-ci.

Affichage des paramètres d'alarmes et d'événements

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. Sur la page d'accueil OMIVV, cliquez sur **Paramètres** > **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. Configuration des événements et alarmes. Voir la section Configuration des événements et alarmes , page 96.

Pour afficher les niveaux de publication d'événement, voir À propos des événements et des alarmes , page 95.

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:<Message description>, Chassis name:<name of the chassis>, Chassis Service Tag:<chassis Service Tag>, Chassis Location:<chassis location>

Tableau 9. Événements de virtualisation

Nom de l'événement	Description	Gravité	Action recommandée
Dell-alertHWCAuditWarning	Avertissement de configuration matérielle	Avertissement	Pas d'action
Dell-alertHWCAuditInformation	Informations sur la configuration matérielle	Informatif	Pas d'action
Dell-alertLiquidCoolingLeakInformational	Une petite fuite précédemment détectée sur le périphérique est maintenant résolue	Informatif	Pas d'action
Dell-alertLiquidCoolingLeakWarning	Une petite fuite a été détectée sur le périphérique.	Avertissement	Pas d'action
Dell-alertLiquidCoolingLeakFailure	Une fuite importante a été détectée sur le périphérique.	Critique	Débranchez l'alimentation d'entrée, puis contactez immédiatement votre prestataire de services.
Dell-alertStorageSoftwareDefinedSubSystemFailure	Défaillance du sous-système de stockage Software-Defined	Critique	Vérifiez l'état d'intégrité du disque dur identifié dans le message, puis relancez l'opération. Pour vérifier l'état d'intégrité de l'interface graphique de l'iDRAC, dans le tableau de bord de l'iDRAC, cliquez sur **Stockage** > **Disques physiques**. Exécutez la commande RACADM suivante à partir de l'interface de ligne de commande (CLI) : `racadm raid get pdisks -o -p status`

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
			Ajoutez des disques physiques au pool de stockage, puis relancez l'opération.
Dell-alertStorageSoftwareDefinedSubSystemWarning	Avertissement relatif au sous-système de stockage Software-Defined	Avertissement	Pas d'action
Dell-alertTemperatureProbeReadWarning	Impossible de lire les capteurs de température	Avertissement	Pas d'action
Dell-alertTemperatureProbeChangeFailure	Erreur d'augmentation de la température	Critique	Vérifiez le journal des événements du châssis pour voir s'il y a des problèmes de ventilation et résolvez tout problème existant. Si aucun problème de ventilateur n'est détecté, vérifiez la température ambiante du châssis et assurez-vous qu'elle est dans les limites de fonctionnement. Pour vérifier la température ambiante du châssis, exécutez la commande RACADM suivante : `racadm getsensorinfo`.
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	Erreur	Mettez le système en mode de maintenance

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	en panne ou n'est pas présent		
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
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

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
Dell - L'alimentation secteur a été restaurée	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Avertissement de perte d'alimentation secteur	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
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

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
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	Pas d'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	Erreur	Pas d'action

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	système ou le logement du lecteur au sein du système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer		
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	Pas d'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

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
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 du boîtier	Informations du matériel du boîtier	Informatif	Pas d'action
Dell - Stockage : avertissement du matériel du boîtier	Avertissement du matériel du boîtier	Avertissement	Pas d'action
Dell - Stockage : défaillance du matériel du boîtier	Erreur du matériel du boîtier	Erreur	Mettez le système en mode de maintenance
Dell - Stockage : panne d'un disque de baie	Panne d'un disque de baie	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
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 baie	Avertissement d'un disque de baie	Avertissement	Pas d'action
Dell - Stockage : informations de disque de baie	Informations d'un disque de baie	Informatif	Pas d'action
Dell - Stockage : avertissement du bloc d'alimentation	Avertissement du bloc d'alimentation	Avertissement	Pas d'action
Dell - Panne de disque Fluid Cache	Panne 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	Avertissement	Pas d'action

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	Controller a détecté un avertissement		
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
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

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
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 ou il y a eu une modification de la configuration, ce qui nécessite des	Informatif	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	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	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.

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	système peut s'arrêter.		
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 fonctionne(nt) pas correctement.	Critique	Replacez la carte SD défectueuse.
Dégradation de la redondance du double module SD interne	L'une des cartes SD, ou les deux, ne fonctionne(nt) pas correctement.	Avertissement	Replacez 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	Avertissement	Examinez le journal des événements pour détecter des pannes de blocs d'alimentation. Vérifiez la configuration du système et la consommation d'énergie

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	redondance de l'alimentation.		
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.
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	Critique	Enlevez et réinstallez les ventilateurs qui sont en panne ou installez des ventilateurs supplémentaires.

Tableau 9. Événements de virtualisation (suite)

Nom de l'événement	Description	Gravité	Action recommandée
	ventilateurs supplémentaires.		

Gestion de la planification de la récupération des données

Planification d'une tâche d'inventaire

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

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

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

1. Sur la page d'accueil de OMIVV, cliquez sur **Paramètres** > **Paramètres vCenter** > **Planification de récupération des données** > **Récupération de l'inventaire**.
2. Cochez la case **Activer la récupération des données d'inventaire (Recommandé)**.

   Dans un environnement PSC disposant de plusieurs serveurs de vCenter, si la planification de chaque vCenter est différente et si vous sélectionnez l'option **Tous les vCenters inscrits** pour mettre à jour la planification de l'inventaire, la page Paramètres de planification de l'inventaire affiche la planification par défaut.
3. Sélectionnez le jour et l'heure d'extraction des données d'inventaire, puis cliquez sur **APPLIQUER**.

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

Planification des tâches de récupération de la garantie

1. Pour mettre à jour la clé d'autorisation, assurez-vous que vous avez accès au catalogue d'index (`https://downloads.dell.com/catalog/CatalogIndex.gz`).
2. Pour obtenir un rapport sur la garantie, assurez-vous que vous avez accès à `https://apigtwb2c.us.dell.com`.
3. Assurez-vous que l'inventaire est exécuté avec succès sur les hôtes et les châssis.
4. Pour utiliser les fonctions de garantie d'OMIVV, vous devez disposer d'une connexion Internet. Si votre environnement requiert un proxy pour accéder à Internet, veillez à configurer les paramètres de proxy dans le portail d'administration.

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

Dans un environnement PSC avec plusieurs serveurs vCenter, la garantie du châssis s'exécute automatiquement pour chaque vCenter lorsque la garantie de n'importe lequel d'entre eux est exécutée. Toutefois, la garantie ne s'exécute pas automatiquement si elle n'est pas ajoutée au profil d'identification de châssis.

REMARQUE : Les paramètres de cette page sont réinitialisés sur les paramètres par défaut chaque fois que l'Assistant Configuration est appelé. Si vous avez déjà configuré une tâche de récupération de la garantie, veillez à répliquer la tâche de récupération de la garantie précédente dans cette page avant de suivre les fonctions de l'assistant afin que la tâche précédente ne soit pas remplacée par les paramètres par défaut.

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

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

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

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

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

16

Gestion de châssis

Affichage des informations sur les châssis Dell EMC

Vous pouvez afficher les informations sur les châssis découverts et inventoriés à l'aide d'OMIVV. La liste des châssis Dell EMC répertorie tous les châssis gérés par OMIVV.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   Les informations suivantes s'affichent :
   - **Nom** : affiche un lien d'adresse IP pour chaque châssis Dell EMC.
   - **Intégrité** : affiche les états d'intégrité du châssis.

     Pour filtrer en fonction de l'état d'intégrité de chaque châssis Dell EMC, cliquez sur l'icône de filtre en regard de la recherche.
   - **Adresse IP/FQDN** : affiche l'adresse IP ou le FQDN du vCenter.
   - **Numéro de série** : affiche le numéro de série du châssis.
   - **URL du châssis** : affiche l'URL du châssis.
   - **Modèle** : affiche le nom du modèle.
   - **Rôle** : applicable uniquement pour châssis MX. Affiche le rôle du châssis (maître ou membre).
   - **Dernier inventaire** : affiche les informations du dernier inventaire.
   - **Logements disponibles** : affiche les logements disponibles dans le châssis.
   - **Nom du profil** : affiche le nom du profil d'identification de châssis auquel le châssis est associé.
   - **Emplacement** : affiche l'emplacement du châssis.

   Si vous n'exécutez pas l'inventaire, le **Nom**, le **Dernier inventaire**, les **Logements disponibles**, le **Nom de profil**, l'**Emplacement** et les informations d'inventaire du châssis ne s'affichent pas.

   REMARQUE : Pour un châssis MX PowerEdge en configuration MCM, toute l'infrastructure MCM est gérée à l'aide du châssis maître. Si les adresses IP des châssis membres et les adresses IP iDRAC sont désactivées et/ou si le rôle du châssis est modifié, Dell EMC recommande de supprimer le châssis principal existant et d'ajouter à nouveau l'adresse IP du nouveau châssis maître, puis de l'associer au profil d'informations d'identification du châssis.
2. Sélectionnez un châssis pour afficher les informations concernant le firmware, le type de licence et la garantie.
   Si vous n'exécutez pas l'inventaire, le **nom**, le **firmware**, le **type de licence** et les informations sur la **garantie** ne s'affichent pas.

Affichage des informations sur l'inventaire du châssis

1. Sur la page **Châssis Dell EMC**, sélectionnez un châssis ou cliquez sur un numéro de série.
2. Dans la section **Informations sur le châssis**, cliquez sur **AFFICHER**.
   La page **Présentation** affiche l'intégrité du châssis, les erreurs actives, l'état d'intégrité du niveau des composants du châssis, la présentation du matériel et la relation entre les châssis (uniquement pour les châssis MX).

   REMARQUE : Pour les châssis M1000e version 4.3 et antérieures, les erreurs actives ne sont pas affichées.

   Le volet principal affiche l'intégrité générale d'un châssis. Les voyants d'intégrité valides sont :**Intègre**, **Avertissement**, **Critique** et **Inconnu**. Dans la vue de grille Intégrité du châssis, l'intégrité de chaque 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 du firmware M1000e inférieures à 4.3, seuls deux voyants d'intégrité sont affichés, à savoir Intègre et Avertissement ou Critique.

   L'intégrité globale indique l'intégrité basée sur le châssis doté du nombre de paramètres d'intégrité le plus bas. Par exemple, s'il existe cinq signes d'intégrité et un signe d'avertissement, le symbole d'intégrité globale correspond à Avertissement.

Affichage des informations d'inventaire matériel du châssis

Vous pouvez afficher les informations sur l'inventaire matériel du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Matériel**.

Tableau 10. Les informations sur l'inventaire matériel

Inventaire matériel : composant	Navigation dans OMIVV	Informations

Ventilateurs	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série.
	• Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**.
	• Dans le volet de droite, cliquez sur **Ventilateurs**.
	OU
	• Sur la page **Présentation**, cliquez sur **Ventilateurs**.
		Informations relatives aux ventilateurs :
		• Nom
		• Présent
		• ID (applicable uniquement pour les châssis MX)
		• État de l'alimentation
		• Mesure (RPM)
		• Seuil d'avertissement (non applicable pour les châssis MX)
		• Seuil critique (non applicable pour les châssis MX)
		  ○ Minimum
		  ○ Maximum
		• Modulation par largeur d'impulsions (uniquement pour châssis MX)
		REMARQUE : Dans un châssis PowerEdge MX, la mention « Oui » indique la présence d'un ventilateur, même lorsqu'un ventilateur est retiré du châssis. Toutefois, l'intégrité du ventilateur s'affiche comme **Critique** sur la page **Récapitulatif** de l'erreur active.

Blocs d'alimentation	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série. • Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**. • Dans le volet de droite, cliquez sur **Blocs d'alimentation**. **OU** • Sur la page **Présentation**, cliquez sur **Blocs d'alimentation**.	Informations relatives aux blocs d'alimentation : • Nom • Capacité • Présent • État de l'alimentation • Tension d'entrée (uniquement pour châssis PowerEdge MX).

Capteurs de température :	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série.
	• Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**.
	• Dans le volet de droite, cliquez sur **Capteurs de température**.
		Informations relatives aux capteurs de température :
		• Emplacement
		• Valeur
		• Seuil d'avertissement
		  ○ Maximum
		  ○ Minimum
		• Seuil critique

Tableau 10. Les informations sur l'inventaire matériel (suite)

Inventaire matériel : composant	Navigation dans OMIVV	Informations
	OU • Sur la page **Présentation**, cliquez sur **Capteurs de température**.	○ Maximum ○ Minimum **REMARQUE :** Des informations sur la température du châssis s'affichent s'il s'agit d'un PowerEdge M1000e. Pour les autres châssis, des informations sur les capteurs de température s'affichent pour le châssis et les serveurs modulaires associés.
Modules d'E/S	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série. • Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**. • Dans le volet de droite, cliquez sur **Modules d'E/S**. **OU** • Sur la page **Présentation**, cliquez sur **Modules d'E/S**.	Informations relatives aux modules d'E/S : • Logement/Emplacement • Présent • Nom • Structure • Numéro de série • État de l'alimentation • Rôle • Version du firmware • Version du matériel • Adresse IP • Masque de sous-réseau • Passerelle • Adresse MAC • DHCP activé
Structure (uniquement pour châssis PowerEdge MX)	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série. • Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**. • Dans le volet de droite, développez **Structure**. **OU** • Sur la page **Présentation**, cliquez sur **Structure**.	Informations sur les composants de la structure : • Intégrité • Structure • Description • Nombre de commutateurs • Nombre de calculs • Nombre de données sortantes Pour afficher les commutateurs qui sont associés à la structure, sélectionnez un composant de la structure. Les informations suivantes s'affichent sur la grille inférieure : • Commutateur • Châssis • Emplacement • Rôle de châssis • Modèle de commutateur
PCIe	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série. • Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**. • Dans le volet de droite, développez **PCIe**. **OU** • Sur la page **Présentation**, cliquez sur **PCIe**.	Informations relatives à PCIe : • Logement PCIe ○ Emplacement ○ Nom ○ État de l'alimentation ○ Structure • Logement du serveur ○ Nom ○ Numéro • Type de logement • Mappage des serveurs • État d'affectation

Tableau 10. Les informations sur l'inventaire matériel (suite)

Inventaire matériel : composant	Navigation dans OMIVV	Informations
		• Alimentation de logement allouée • ID de PCI • Numéro/ID fournisseur **REMARQUE :** Les informations sur le PCIe ne s'appliquent pas au châssis M1000e.
iKVM (uniquement pour PowerEdge M1000e)	• Sur la page **Châssis Dell EMC**, cliquez sur **Châssis** > **Liste des châssis**, puis sur le lien Numéro de série. • Sur la page **Présentation**, dans le volet de gauche, sélectionnez **Matériel**. Dans le volet de droite, développez **iKVM**. **OU** • Sur la page **Présentation**, cliquez sur **iKVM**.	Informations relatives au module iKVM : • Nom du module iKVM • Présent • Version du firmware • USB/Vidéo du panneau avant activés • Autoriser l'accès à l'interface de ligne de commande CMC. **REMARQUE :** L'onglet iKVM s'affiche uniquement si le châssis contient un module iKVM.

Affichage des informations sur l'inventaire du firmware

Vous pouvez afficher les informations relatives au firmware du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Firmware**.
   Les informations suivantes sur le firmware s'affichent :
   - Composant
   - Version actuelle

   Sur cette page, vous pouvez également lancer OpenManage Enterprise Modular et CMC.

Affichage des informations sur le contrôleur de gestion

Vous pouvez afficher les informations relatives au contrôleur de gestion du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Contrôleur de gestion**.
   Les informations suivantes sur le contrôleur de gestion s'affichent :
   - Général
     - Nom
     - Version du firmware
     - Heure de la dernière mise à jour
     - Emplacement du châssis
     - Version du matériel

- Réseau commun
  - Nom de domaine DNS
  - Utiliser DHCP pour DNS
  - Adresse MAC
  - Mode de redondance
  - Version du matériel
- Informations sur IPv4
  - IPv4 activé
  - DHCP activé
  - Adresse IP
  - Masque de sous-réseau
  - Passerelle
  - Serveur DNS préféré
  - Serveur DNS auxiliaire
- Informations IPv6
  - IPv6 activé
  - DHCP activé
  - Adresse IP
  - Adresse locale de liaison
  - Passerelle
  - Serveur DNS préféré
  - Serveur DNS auxiliaire
- Configuration de l'accès local
  - Matériel de Quick Sync présent
  - Écran LCD présent
  - LED présente
  - KVM activé

REMARQUE : Des attributs d'informations liées au réseau relatifs à un châssis membre qui fait partie de la configuration MCM ne s'affichent pas dans la section **Contrôleur de gestion**.

Affichage des informations sur l'inventaire de stockage

Vous pouvez afficher les informations relatives au stockage du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Stockage**.

   Les informations suivantes sur le stockage s'affichent :

   - Disques virtuels.
   - Disques physiques
   - Contrôleurs
   - Boîtiers
   - Disques de secours

   Pour les châssis MX, les informations suivantes s'affichent :

   - Numéro de logement
   - Nom du logement
   - Modèle
   - Numéro de série
   - Version du firmware
   - Numéro d'inventaire

- État de l'alimentation
- Mode d'attribution

Pour les châssis MX, si vous voulez voir des informations sur les disques, cliquez sur le traîneau de stockage. Les informations suivantes sur le lecteur sont affichées dans le volet inférieur :

- Intégrité
- État
- Emplacement
- Attribution du logement
- Nom du disque
- Capacité
- Protocole du bus
- Support

Si un disque du châssis MX PowerEdge n'est pas affecté, son attribution de logement est indiquée comme suit : **N/A**.

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 :

- Nom
- Modèle
- Numéro de série
- Adresse IP (lien au stockage)
- Structure
- Nom de groupe
- Adresse IP du groupe (lien au groupe de stockage).

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.

Afficher les informations sur la garantie

Vous pouvez afficher les informations relatives à la garantie du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Garantie**.

   Informations relatives à la garantie :

   - Fournisseur
   - Description
   - État
   - Type de droits
   - Date de début
   - Date de fin
   - Jours restants
   - Dernière mise à jour

   REMARQUE : Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Planification des tâches de récupération de la garantie , page 109.

Affichage de l'hôte associé à un châssis

Vous pouvez afficher les informations relatives à l'hôte du châssis sélectionné.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.
3. Sur la page **Présentation**, cliquez sur **Hôtes associés**.
   Les informations suivantes sur l'hôte associé s'affichent :
   - Nom d'hôte
   - Numéro de série
   - Modèle
   - IP iDRAC
   - Emplacement
   - Emplacement de logement
   - Dernier inventaire
4. Pour afficher plus d'informations sur un hôte, sélectionnez-le.

Affichage des informations sur le châssis lié

La section **Relations du châssis** montre la relation entre les châssis dans un châssis MX déployé en mode MCM.

REMARQUE : Les informations de châssis lié ne s'appliquent qu'aux châssis MX PowerEdge configurés dans un groupe MCM.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis**.
   La page **Châssis Dell EMC** s'affiche.
2. Sélectionnez un châssis, puis cliquez sur le lien Numéro de série.
   La page **Présentation** s'affiche.

   Sur la page **Présentation**, la section **Relations du châssis** affiche toutes les informations sur le châssis associé aux châssis maître et membre.

Gestion d'un châssis MX PowerEdge

La façon dont vous gérez un châssis MX7000X est différente de la gestion d'autres châssis Dell EMC tels que M1000e, VRTX et FX2.

Vous pouvez gérer un châssis MX en mode autonome avec des adresses IP publiques pour le module de gestion et des adresses IP iDRAC. De plus, vous pouvez configurer un châssis MX en mode Multi-Chassis Management (MCM) avec un maître et plusieurs membres.

Dell EMC OpenManage Enterprise-Modular prend en charge les groupes MCM câblés. Dans le type câblé, le châssis est connecté en guirlande ou câblé via un port redondant sur le module de gestion. Le châssis que vous sélectionnez pour créer le groupe doit être relié en guirlande à au moins un châssis. Pour plus d'informations sur la création du groupe de châssis, consultez le document *Guide de l'utilisateur de Dell EMC OpenManage Enterprise-Modular pour châssis MX7000 PowerEdge*, disponible sur dell.com/support.

Vous pouvez gérer les serveurs présents dans un châssis MX de deux façons :

1. **Gestion des serveurs à l'aide du profil d'identification d'hôte** : la façon standard et recommandée de gérer les serveurs où toutes les fonctions sont prises en charge. Dans ce cas, le châssis n'est découvert qu'une fois l'inventaire des hôtes MX terminé. Pour plus d'informations sur la création d'un profil d'identification d'hôte, voir Création du profil d'identification d'hôte , page 39.
2. **Gestion des serveurs à l'aide du profil d'identification de châssis** : si vous choisissez de gérer vos hôtes à l'aide du profil d'identification de châssis, les fonctions OMIVV telles que l'inventaire, la surveillance, la mise à jour de firmware et des pilotes sont prises en charge. Pour plus d'informations sur la gestion du châssis et de l'hôte à l'aide du profil d'identification de châssis, voir Création d'un profil d'identification de châssis , page 44.

REMARQUE : OMIVV ne prend pas en charge la gestion des châssis MX PowerEdge avec une configuration de châssis maître de sauvegarde.

REMARQUE : Si l'adresse IPv4 de l'iDRAC est désactivée, vous pouvez choisir de gérer le serveur en utilisant le profil d'identification de châssis. Si vous gérez le serveur à l'aide du profil d'identification de châssis, les fonctions OMIVV suivantes ne sont pas prises en charge :

- Mode de verrouillage iDRAC
- Possibilité d'utiliser ce serveur comme serveur de référence pour capturer le profil système

- Déploiement du SE
- Obtention ou mise à jour de l'état CSIOR
- Conformité de configuration de serveurs
- Quelques informations relatives à l'inventaire

REMARQUE : Les hôtes possédant une adresse IP IPv4 iDRAC publique peuvent également être gérés en utilisant le profil d'identification de châssis. Toutefois, cela n'est pas recommandé car les fonctions énumérées ci-dessus ne sont pas prises en charge.

Gestion du châssis et de l'hôte à l'aide de l'IP de gestion unifiée des châssis

Si une IPv4 iDRAC est désactivée pour un hôte géré à l'aide d'un profil d'identification d'hôte, l'inventaire des hôtes échoue et le châssis n'est pas détecté. Dans ce cas, le châssis doit être ajouté manuellement et doit être associé à un profil d'identification de châssis pour gérer le châssis et ses hôtes associés.

Si vous choisissez de gérer vos hôtes à l'aide de l'IP de gestion unifiée des châssis, les fonctions OMIVV telles que l'inventaire, la surveillance, le firmware et les mises à jour des pilotes sont prises en charge. Vous trouverez ci-dessous la description détaillée des tâches pour gérer le châssis et les hôtes à l'aide de l'IP de gestion unifiée des châssis :

1. Ajoutez un châssis MX.

   Pour plus d'informations sur l'ajout d'un châssis MX, voir Ajout d'un châssis PowerEdge MX , page 118.
2. Créez un profil d'identification de châssis et associez les hôtes.

   Pour plus d'informations sur la création d'un profil d'identification de châssis, voir Création d'un profil d'identification de châssis , page 44.
3. Affichez les tâches pour le châssis et pour l'hôte géré à l'aide du profil d'identification de châssis.
4. Affichez l'inventaire du châssis et de l'hôte.

   Pour plus d'informations sur l'inventaire des hôtes et des châssis, voir Affichage de la tâche d'inventaire de l'hôte , page 80 et Affichage de la tâche d'inventaire du châssis , page 81.
5. Effectuez la mise à jour de firmware sur les hôtes qui sont gérés à l'aide du châssis.

   Pour plus d'informations sur la mise à jour de firmware, voir Mise à jour du micrologiciel , page 134.

   REMARQUE : Le workflow sans système d'exploitation n'est pas pris en charge lorsque les hôtes sont gérés à l'aide d'un châssis.

Ajout d'un châssis PowerEdge MX

Un hôte comportant une adresse IP IPv4 iDRAC valide peut être ajouté au profil d'identification. Ainsi, pendant l'inventaire de l'hôte, le châssis MX associé est automatiquement découvert et affiché sur la page **Châssis Dell EMC**.

Si une IPv4 iDRAC est désactivée pour un hôte, l'inventaire de l'hôte échoue et le châssis n'est pas détecté. Dans ce cas, un châssis MX doit être ajouté manuellement et doit être associé à un profil d'identification de châssis pour gérer le châssis et ses hôtes associés.

Pour ajouter manuellement un châssis MX, effectuez les opérations suivantes :

1. Sur la page d'accueil d'**OMIVV**, cliquez sur **Hôtes et châssis** > **Châssis**.
2. Sur la page **Châssis Dell EMC**, cliquez sur **AJOUTER UN CHÂSSIS MX**.
3. Entrez un module de gestion IPv4, un FQDN ou un nom d'hôte, puis cliquez sur **OK**.

   Lorsque vous saisissez une adresse IP, elle est validée si l'IP est gérée par OMIVV.

   REMARQUE : Avant d'ajouter un châssis à l'aide d'un nom d'hôte ou d'un FQDN, assurez-vous que des entrées de recherche directes et inversées valides sont créées dans le DNS.

   REMARQUE : Si vous entrez FQDN, l'URL du châssis s'affiche avec le FQDN.

   Le châssis est ajouté à la page **Châssis Dell EMC**.
4. Associez les hôtes au profil d'identification du châssis en créant un profil d'identification de châssis. Pour plus d'informations sur la création d'un profil d'identification de châssis, voir Création d'un profil d'identification de châssis , page 44.

REMARQUE : Si vous entrez une adresse IP autre que l'adresse IP du châssis MX, la connexion de test échoue et l'entrée non valide reste sur la page **Châssis Dell EMC**. Seul un châssis validé avec succès est associé à un profil d'identification de châssis.

REMARQUE : La connexion de test échoue si les hôtes ne sont pas présents dans les vCenters enregistrés qui sont associés au châssis MX ajouté.

REMARQUE : Dans le cas d'un châssis MX PowerEdge configuré dans une configuration MCM, les châssis maître et membre doivent avoir les mêmes informations d'identification.

mise à jour de firmware d'un châssis MX

Avant de planifier la mise à jour de firmware, assurez-vous que les conditions suivantes sont réunies dans l'environnement :

- Assurez-vous que le châssis MX fait partie du profil d'identification du châssis et qu'il est correctement répertorié.
- Si l'un de ses hôtes subit des mises à jour de firmware, le firmware du châssis ne peut pas être mis à jour.

REMARQUE : À l'aide de la fonctionnalité de mise à jour de firmware du châssis MX, vous pouvez mettre à jour le firmware du module de gestion uniquement.

1. Sur la page d'accueil de OMIVV, cliquez sur **Hôtes et châssis** > **Châssis** > **Liste des châssis** > **MISE À JOUR DE FIRMWARE DU CHÂSSIS MX**.
2. Sur la page **mise à jour de firmware du châssis** de l'assistant, lisez les instructions, puis cliquez sur **DÉMARRER**.
3. Dans **Liste des châssis MX**, sélectionnez un ou plusieurs châssis MX, puis cliquez sur **SUIVANT**.
   Le châssis ne s'affiche pas si l'une des conditions suivantes n'est pas remplie dans l'environnement :
   - La mise à jour de firmware du châssis est en cours à partir d'OMIVV.
   - Le profil d'identification de châssis n'est pas créé pour le châssis.
   - L'inventaire n'a pas été correctement exécuté pour le châssis.

   Pour les châssis MX PowerEdge avec configuration MCM, vous pouvez sélectionner uniquement le châssis maître. Le châssis membre est sélectionné automatiquement.
4. Sur la page **Sélectionner une source de mise à jour**, procédez comme suit :
   a. Dans le menu déroulant, sélectionnez le profil de logithèque approprié.
   b. En fonction du profil de logithèque de firmwares et de châssis que vous avez sélectionné, sélectionnez les lots appropriés dans la catégorie système identifiée.
5. Sur la page **Sélectionner les composants du firmware**, sélectionnez les composants du firmware qui nécessitent une mise à jour, puis cliquez sur **SUIVANT**.
   Les composants dont la version est inférieure à la version disponible dans le catalogue ou qui sont dans le même niveau (à jour) ne peuvent pas être sélectionnés. Pour sélectionner les composants répertoriés à l'état rétrogradé, cliquez sur **Autoriser la rétrogradation du firmware**.

   Pour un châssis MX PowerEdge associé à une configuration MCM, la version du firmware peut être rétrogradée même si la case **Autoriser la rétrogradation du firmware** n'est pas cochée.

   Vous ne pouvez sélectionner que les châssis membres pour les mettre à jour ou les rétrograder. Sélectionner le châssis maître permet de sélectionner automatiquement le châssis membre.

   Pour sélectionner tous les composants du firmware sur toutes les pages, cliquez sur .

   Pour désélectionner tous les composants du firmware sur toutes les pages, cliquez sur .
6. Sur la page **Tâche de planification**, procédez comme suit :
   a. Saisissez le nom et la description de la tâche de mise à jour de firmware. La description est facultative.
      Le nom de la tâche de mise à jour de firmware est obligatoire et empêche l'utilisation d'un nom existant. Si vous supprimez le nom d'une tâche de mise à jour de firmware, vous pouvez le réutiliser.
   b. Sélectionnez une option de planification appropriée pour appliquer les mises à jour.
7. Sur la page **Aperçu du résumé**, vérifiez les informations de mise à jour de firmware, puis cliquez sur **TERMINER**.

Tableau 11. Nombre total de mises à jour simultanées du firmware de châssis MX pour chaque mode de déploiement.

Mode de déploiement	Nombre de mises à jour simultanées du firmware du châssis
Petit	1
Moyen	1
Important	2
Très grande	2

17

Gestion des hôtes

Affichage des hôtes OMIVV

Vous pouvez afficher tous les hôtes gérés par OMIVV sur la page **Hôtes d'OMIVV**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Hôtes et châssis** > **Hôtes**.
2. Sur l'onglet **Hôtes d'OMIVV**, consultez les informations suivantes :
   - **Nom de l'hôte** : affiche l'adresse IP de l'hôte. Pour afficher les informations sur l'hôte, sélectionnez-en un.
   - **Intégrité** : affiche les états d'intégrité des hôtes.

     Pour filtrer en fonction de l'état d'intégrité de chaque hôte Dell EMC, cliquez sur l'icône de filtre en regard de la recherche.
   - **vCenter** : affiche l'adresse IP du vCenter correspondant à l'hôte.
   - **Cluster** : affiche le nom du cluster, si l'hôte Dell EMC est dans un cluster.
   - **Profil d'identification d'hôte** : affiche le nom du profil d'identification d'hôte.

Surveillance d'un seul hôte

OMIVV vous permet d'afficher des informations détaillées sur un seul hôte. Vous pouvez afficher tous les hôtes OMIVV sur la page **Hôtes et clusters**. Pour afficher plus d'informations, sélectionnez un hôte géré par OMIVV, puis accédez à **SurveillerInformations sur l'hôte OMIVV**.

Affichage du résumé des informations de l'hôte

Vous pouvez afficher les détails de récapitulatif d'un hôte individuel sur la page **Résumé**, où divers portlets sont affichés. Deux des portlets sont applicables pour OMIVV. Les deux portlets sont les suivants :

- **Intégrité de l'hôte OMIVV**
- **Informations sur l'hôte OMIVV**

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. Sur la page d'accueil d'OMIVV, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
2. Dans le volet de gauche, sélectionnez l'hôte concerné.
3. Dans le volet de droite, cliquez sur **Résumé**.
4. Faites défiler l'affichage pour voir le portlet OMIVV Server Management.

   Vous pouvez afficher les informations suivantes dans la section **Informations sur l'hôte OMIVV** et **Intégrité de l'hôte OMIVV** :

Tableau 12. Informations sur l'hôte OMIVV

Informations	Description
Numéro de service	Affiche le numéro de service du serveur. 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

Tableau 12. Informations sur l'hôte OMIVV (suite)

Informations	Description
	mémoire. Ceci s'applique aux serveurs PowerEdge 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 : ● 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 iDRAC 8 et serveurs ultérieurs. 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 : ● Nom d'hôte : affiche le nom de l'hôte géré par OMIVV ● 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 d'identification d'hôte : affiche le nom du profil d'identification d'hôte pour 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	Affiche les éléments suivants : ● 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	Affiche un lien permettant de lancer la console d'accès à distance Remote Access (iDRAC).
Actions de l'hôte	Configurez le serveur physique pour qu'il clignote à différents intervalles de temps. Voir la section Configuration de l'indicateur de clignotement , page 151.

Tableau 13. Intégrité de l'hôte OMIVV

Informations	Description
Intégrité de l'hôte OMIVV	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 paramètres d'intégrité le plus bas. Les options possibles incluent : • 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 : Les informations de surveillance de l'alimentation ne sont pas disponibles pour les hôtes dotés d'une PSU câblée ou pour les serveurs modulaires.

Affichage des informations sur l'hôte OMIVV

Vous pouvez afficher les informations sur le matériel, le stockage, le firmware, la surveillance de l'alimentation, la garantie, les journaux des événements système sur tous les hôtes gérés par OMIVV sur la page **Informations sur l'hôte OMIVV**.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
2. Dans le volet de gauche, sélectionnez un hôte, puis cliquez sur **Surveiller** > **Informations sur l'hôte OMIVV**.

Affichage des informations sur le matériel d'un hôte

Tableau 14. Informations sur le matériel d'un seul hôte

Matériel : *Composant*	Informations
FRU	• **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.
Processeurs	• **Socket** : affiche le numéro de logement. • **Vitesse** : affiche la vitesse actuelle. • **Marque** : affiche la marque du processeur. • **Version** : affiche la version du processeur. • **Cœurs** : affiche le nombre de cœurs du processeur.
Blocs d'alimentation	• **Type** : affiche le type du bloc d'alimentation. Les types de blocs d'alimentation sont les suivants :

Tableau 14. Informations sur le matériel d'un seul hôte (suite)

Matériel : *Composant*	Informations
	○ 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.
Mémoire	• **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.
Cartes NIC	• **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.
Logements PCI	• **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 de l'appareil PCI. • **Type** : affiche le type de logement PCI. • **Largeur** : affiche la largeur du bus de données, si disponible.
Carte d'accès à distance	• **Adresse IP** : affiche l'adresse IP de la carte d'accès à distance. Si vous gérez des hôtes à l'aide d'une adresse IP unifiée, l'adresse IP de l'iDRAC ne s'affiche pas dans cette section. • **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 informations de stockage d'un hôte

Vous pouvez visualiser le nombre de disques virtuels, contrôleurs, boîtiers et disques physiques associés ainsi que la quantité de disques de secours globaux et dédiés. Pour afficher plus d'informations sur chacun des composants de stockage, sélectionnez le composant concerné dans le menu déroulant **Afficher**.

Dans le cas des hôtes gérés à l'aide du châssis, les informations de stockage intégrales (contrôleurs, boîtiers, disques de secours globaux, disque de secours dédié) ne s'affichent pas.

REMARQUE : Lorsque les hôtes sont gérés à l'aide du profil de châssis, si vous cliquez sur **Stockage**, puis sélectionnez les options suivantes dans le menu déroulant **Afficher** :

- **Boîtiers**- le numéro d'ID de contrôleur du boîtier de stockage s'affiche en tant que 0 au lieu du numéro d'ID de contrôleur correct.
- **Disques physiques**— Le type de support pour HDD s'affiche en tant que **disque magnétique** au lieu de **disque dur**.

Tableau 15. Détails de stockage d'un seul hôte

Informations	Description
Disques virtuels.	• **Nom** : affiche le nom du lecteur virtuel. • **FQDD de périphérique** : affiche le descripteur de périphérique complet. • **Disque physique** : indique le disque physique où se trouve le lecteur virtuel. • **Capacité** : affiche la capacité du lecteur virtuel. • **Disposition** : affiche le type de disposition du stockage virtuel, c'est-à-dire le type de RAID configuré pour ce lecteur virtuel. • **Type de support** : indique s'il s'agit d'un support SSD ou HDD. Pour afficher des informations telles que la taille de bande, le protocole de bus et la règle de cache, sélectionnez un disque virtuel. • **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 lecteur virtuel. Les valeurs possibles sont : ○ 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 : ○ 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 : ○ 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.
Disques physiques Lorsque vous sélectionnez cette option dans le menu déroulant **Afficher**, la liste déroulante **Filtre** s'affiche. Les options de filtre suivantes sont disponibles : • **Tous les disques physiques** • **Disques de secours globaux** • **Disques de secours dédiés** • La dernière option affiche les noms personnalisés des lecteurs virtuels.	• **Nom** : affiche le nom du disque physique. • **FQDD 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 : ○ EN LIGNE ○ PRÊT ○ DÉGRADÉ ○ EN ÉCHEC ○ HORS LIGNE ○ RECONSTRUCTION ○ INCOMPATIBLE ○ SUPPRIMÉ ○ EFFACÉ

Tableau 15. Détails de stockage d'un seul hôte (suite)

Informations	Description
	○ ALERTE SMART DÉTECTÉE ○ INCONNU ○ ÉTRANGER ○ NON PRIS EN CHARGE • **Configuré** : indique si le disque est configuré. • **Type de disque de secours** (non applicable pour PCIe) : affiche le type de disque de secours. Les options possibles incluent : ○ 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 lecteur virtuel. Lorsqu'un disque physique dans le lecteur virtuel tombe en panne, le disque de secours est activé pour remplacer le disque physique défaillant sans interrompre le système ni nécessiter votre intervention. • **Disque virtuel** : affiche le nom du lecteur virtuel. • **Protocole de bus** : affiche le protocole de bus. • **ID de contrôleur** : affiche l'ID du contrôleur. • **Type de support** : indique s'il s'agit d'un support SSD ou HDD. • **Endurance d'écriture nominale restante** : affiche l'endurance d'écriture SSD restante. • **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	• **ID de contrôleur** : affiche l'ID du contrôleur. • **Nom** : affiche le nom du contrôleur. • **FQDD de périphérique** : affiche le descripteur de périphérique complet. • **Version de firmware** : affiche la version du firmware. • **Micrologiciel minimum requis** : affiche la version minimale requise du micrologiciel. Cette colonne est renseignée si le firmware n'est pas à jour et si 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. **REMARQUE :** Cette section affiche les informations sur le contrôleur du jeu de puces. Cela ne s'affiche pas dans la section contrôleur de stockage de l'interface utilisateur iDRAC, mais vous pouvez afficher ces informations sur la page inventaire de iDRAC.
Enceintes	• **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. • **FQDD de périphérique** : affiche le descripteur de périphérique complet. • **Numéro de service** : affiche le numéro de service.

Affichage des informations de firmware d'un seul hôte

Les informations relatives au firmware suivantes sont affichées :

- **Nom** : affiche le nom de tous les firmwares sur cet hôte.
- **Type** : affiche le type de firmware.
- **Version** : affiche la version de tous les firmwares sur cet hôte.
- **Date d'installation** : affiche la date d'installation.

REMARQUE : Lorsque les hôtes sont gérés à l'aide du profil d'identification de châssis, les données d'inventaire du firmware affichent quelques composants supplémentaires tels que Lifecycle Controller et le logiciel RAID.

Vous pouvez lancer la mise à jour du firmware et configurer les assistants du mode de verrouillage du système à partir de cette page.

Affichage des informations de surveillance de l'alimentation d'un seul hôte

Vous pouvez afficher les informations telles que les informations générales, les seuils, la capacité d'alimentation de réserve et les statistiques énergétiques.

- **Informations générales** : affiche le bilan énergétique et le nom du profil actuel.
- **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.

Statistiques d'énergie

- **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.
- **REMARQUE :** L'heure de l'hôte, telle qu'utilisée ici, désigne l'heure locale de l'endroit où l'hôte se trouve.

  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.

REMARQUE : Les informations de surveillance de l'alimentation ne sont pas disponibles pour les hôtes dotés d'une PSU câblée ou pour les serveurs modulaires.

REMARQUE : Pour les hôtes gérés à l'aide du châssis, les informations de surveillance de l'alimentation ne s'affichent pas.

Affichage des informations sur la garantie d'un seul hôte

Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Planification des tâches de récupération de la garantie , page 109. 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.

- **Fournisseur** : affiche le nom du fournisseur de la garantie.
- **Description** : affiche une description.
- **État** : affiche l'état de la garantie de l'hôte. Les options d'état possibles incluent :
  - 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.
  - Critique : l'hôte est sous garantie, mais un seuil critique a été franchi
  - Expiré : la garantie de cet hôte est arrivée à expiration.
  - Inconnu : l'OMIVV 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.
- **Type de droits** : affiche les états suivants :
  - Initial
  - Étendu
  - Expirée
- **Date de début** : affiche la date de début de la garantie.
- **Date de fin** : affiche la date de fin de la garantie.
- **Jours avant expiration** : 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.

Affichage des informations du journal des événements système d'un seul hôte

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

- **État** : différents types d'icônes d'état sont disponibles comme Information (point d'exclamation bleu), Avertissement (triangle jaune avec point d'exclamation), Erreur (X rouge) et Inconnu (boîte contenant un point d'interrogation).

  Les niveaux de gravité sont définis de la manière suivante :

  - Informatif
  - Avertissement
  - Erreur

- **Heure (Heure du serveur)** : indique l'heure et la date de l'événement.

Pour effacer le Journal des événements système, cliquez sur **EFFACER LE JOURNAL**. Un message s'affiche, indiquant que les données du journal ne peuvent pas être récupérées une fois que le journal a été effacé.

Surveillance des hôtes sur des clusters et des datacenters

OMIVV vous permet d'afficher des informations détaillées sur tous les hôtes d'un datacenter ou d'un cluster.

Affichage des informations du datacenter et du cluster OMIVV

Affichage de la présentation du datacenter et du cluster

Vous pouvez afficher les informations du datacenter ou du cluster, du mode System Lockdown, des ressources matérielles et de la garantie. Pour afficher les informations sur cette page, assurez-vous que l'inventaire a été effectué avec succès. Les données du rapport sur les datacenters et les clusters OMIVV proviennent directement de l'iDRAC.

1. Sur la page d'accueil d'OMIVV, cliquez sur **Menu**, puis sélectionnez **Hôtes et clusters**.
2. Dans le volet de gauche, sélectionnez un datacenter ou un cluster, puis cliquez sur **Surveiller** > **Informations sur le datacenter ou le cluster OMIVV**.
3. Pour afficher plus d'informations, sélectionnez un hôte spécifique.

   Les informations telles que l'adresse IP de l'iDRAC, l'URL du châssis, les processeurs et la mémoire s'affichent dans le volet inférieur horizontal de la page.

Tableau 16. Aperçu des datacenters et clusters

Informations	Description
Informations Datacenter/Cluster	Affiche les éléments suivants : ● Nom de datacenter/cluster ● Nombre d'hôtes gérés ● Consommation totale électrique
Mode System Lockdown	Affiche l'état du mode de verrouillage de l'iDRAC. Les différents états du mode de verrouillage de l'iDRAC du nombre total des hôtes est affiché comme suit : ● Activé ● Désactivé ● Non applicable (uniquement pour les serveurs basés sur l'iDRAC9) Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.
Ressources matérielles	Affiche les éléments suivants :

Tableau 16. Aperçu des datacenters et clusters (suite)

Informations	Description
	• Nombre total de processeurs • Mémoire totale • Capacité du disque virtuel
Récapitulatif de garantie	Affiche l'état de garantie de l'hôte sélectionné. Les options État disponibles sont les suivantes : • Garantie expirée • Garantie active • Dépassement du seuil d'avertissement • Dépassement du seuil critique • Garantie inconnue Pour un hôte disposant de plusieurs garanties ou de différentes garanties (par exemple, le code de niveau de service, comme ND et 4DP), OMIVV prend en compte le statut du type de garantie avec le plus petit nombre de jours encore couverts par la garantie.
Hôte	Affiche le nom d'hôte
Numéro de série	Affiche le numéro de série de l'hôte
Modèle	Affiche le modèle du PowerEdge
Numéro d'inventaire	Affiche le numéro d'inventaire, s'il a été défini
Numéro de série du châssis	Affiche le numéro de série 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 System Lockdown	Uniquement pour les serveurs basés sur l'iDRAC9 : affiche le mode de verrouillage de l'hôte iDRAC, qui est activé, désactivé ou inconnu. Pour tous les serveurs PowerEdge antérieurs aux serveurs basés sur l'iDRAC9, le mode System Lockdown affiché est **Non applicable**. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.
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 du CMC ou du module de gestion	Affiche l'URL du CMC ou du module de gestion, qui correspond à l'URL du châssis pour les serveurs modulaires, 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
Profil d'identification d'hôte	Affiche le nom du profil d'identification
Version de la carte d'accès distant	Affichage la version de la carte d'accès distant
Version du firmware du BIOS	Affiche la version du firmware du BIOS

Affichage des informations matérielles du datacenter et du cluster

Tableau 17. Informations sur le matériel des datacenters et des clusters

Matériel : *Composant*	Informations
Matériel : unité remplaçable	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série de l'hôte. • **Nom de pièce** : affiche le nom de pièce du composant remplaçable. • **Numéro de référence** : affiche le numéro de référence du composant 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	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série de l'hôte. • **Socket** : affiche le numéro de logement. • **Vitesse** : affiche la vitesse actuelle. • **Marque** : affiche la marque du processeur. • **Version** : affiche la version du processeur. • **Cœurs** : affiche le nombre de cœurs du processeur.

Matériel : bloc d'alimentation	• **Hôte** : affiche le nom de l'hôte.
	• **Numéro de série** : affiche le numéro de série de l'hôte.
	• **Type** : affiche le type du bloc d'alimentation. Les types de blocs d'alimentation sont les suivants :
	  ○ 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.
	• **État** : affiche l'état du bloc d'alimentation. Les options État disponibles sont les suivantes :
	  ○ AUTRE
	  ○ INCONNU
	  ○ OK
	  ○ CRITIQUE
	  ○ NON CRITIQUE
	  ○ RÉCUPÉRABLE
	  ○ IRRÉCUPÉRABLE
	  ○ ÉLEVÉ
	  ○ FAIBLE

Matériel : mémoire	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série de l'hôte. • **Logement** : affiche Le logement DIMM. • **Taille** : affiche la taille de la mémoire.

Tableau 17. Informations sur le matériel des datacenters et des clusters (suite)

Matériel : *Composant*	Informations
	• **Type** : affiche le type de la mémoire.
Matériel : cartes réseau	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série 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	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série de l'hôte. • **Logement** : affiche le logement. • **Fabricant** : affiche le nom du fabricant du logement PCI. • **Description** : affiche la description de l'appareil PCI. • **Type** : affiche le type de logement PCI. • **Largeur** : affiche la largeur du bus de données, si disponible.
Matériel : carte d'accès distant	• **Hôte** : affiche le nom de l'hôte. • **Numéro de série** : affiche le numéro de série de l'hôte. • **Adresse IP** : affiche l'adresse IP de la carte d'accès distant. • **Adresse MAC** : affiche l'adresse MAC de la carte d'accès distant. • **Type de RAC** : affiche le type de la carte d'accès distant. • **URL** : affiche l'URL active de l'iDRAC associé à cet hôte.

Affichage des informations relatives au stockage du datacenter et du cluster

Tableau 18. Détails du stockage pour un datacenter et un cluster

Stockage : disques	Description

Disque physique	• **Hôte** : affiche le nom de l'hôte.
	• **Numéro de série** : affiche le numéro de série de l'hôte.
	• **Capacité** : affiche la capacité du disque physique.
	• **État du disque** : affiche l'état du disque physique. Les options possibles incluent :
	  ○ EN LIGNE
	  ○ PRÊT
	  ○ DÉGRADÉ
	  ○ EN ÉCHEC
	  ○ HORS LIGNE
	  ○ RECONSTRUCTION
	  ○ INCOMPATIBLE
	  ○ SUPPRIMÉ
	  ○ EFFACÉ
	  ○ DÉTECTION D'ALERTE INTELLIGENTE
	  ○ INCONNU
	  ○ ÉTRANGER
	  ○ NON PRIS EN CHARGE
	REMARQUE : Pour en savoir plus sur la signification de ces alertes, voir le Guide de l'utilisateur de Dell EMC OpenManage Server Administrator Storage Management à l'adresse `dell.com/support`
	• **Numéro de modèle** : affiche le numéro de modèle du disque de stockage physique.
	• **Dernier inventaire** : affiche le jour, le mois et l'heure de la dernière exécution de l'inventaire.

Tableau 18. Détails du stockage pour un datacenter et un cluster (suite)

Stockage : disques	Description

	• **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.
	• **Endurance d'écriture nominale restante** : affiche l'endurance d'écriture SSD restante.
	• **Type de disque de secours** (non applicable pour PCIe) : affiche le type de disque de secours. Les options possibles incluent :
	  ○ 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 lecteur virtuel. Lorsqu'un disque physique du lecteur 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	• **Hôte** : affiche le nom de l'hôte.
	• **Numéro de série** : affiche le numéro de série de l'hôte.
	• **Nom** : affiche le nom du lecteur virtuel.
	• **Disque physique** : indique le disque physique où se trouve le lecteur virtuel.
	• **Capacité** : affiche la capacité du lecteur virtuel.
	• **Disposition** : affiche le type de disposition du stockage virtuel. C'est-à-dire le type de RAID configuré pour ce lecteur virtuel.
	• **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 lecteur virtuel. Les valeurs possibles sont :
	  ○ SCSI
	  ○ SAS
	  ○ SATA
	  ○ PCIe
	• **Taille de répartition** : affiche la taille de répartition du disque virtuel. La taille de répartition fait référence à la quantité d'espace utilisée par chaque répartition 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 :
	  ○ Lecture anticipée
	  ○ Sans lecture anticipée
	  ○ Lecture anticipée adaptative
	  ○ Cache de lecture activé
	  ○ Cache de lecture désactivé
	• **Stratégie d'écriture par défaut** : affiche la stratégie d'écriture par défaut prise en charge par le contrôleur. Les options possibles incluent :
	  ○ Écriture différée
	  ○ Forcer l'écriture différée

Tableau 18. Détails du stockage pour un datacenter et un cluster (suite)

Stockage : disques	Description
	○ Écriture différée activée ○ Écriture immédiate ○ Cache en écriture activé et protégé ○ Cache en écriture désactivé • **Stratégie de cache de disque** : affiche la stratégie de mise en cache par défaut prise en charge par le contrôleur. Les options possibles incluent : ○ Activé : E/S de cache ○ Désactivé : E/S directe

Affichage des informations relatives au firmware du datacenter et du cluster

Les informations suivantes sur les composants du firmware s'affichent :

- **Hôte** : affiche le nom de l'hôte.
- **Numéro de série** : affiche le numéro de série de l'hôte.
- **Nom** : affiche le nom de tous les firmwares sur cet hôte.
- **Version** : affiche la version de tous les firmwares sur cet hôte.

Affichage des informations relatives à la surveillance de l'alimentation du datacenter et du cluster

- **Hôte** : affiche le nom de l'hôte.
- **Numéro de série** : affiche le numéro de série 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 électrique** : 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.

Affichage des informations relatives à la garantie du datacenter et du cluster

Pour consulter l'état d'une garantie, exécutez une tâche de garantie. Voir la section Planification des tâches de récupération de la garantie , page 109. 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.

- **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 de l'hôte.
- **Numéro de série** : affiche le numéro de série 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 :

- 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.
- 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.

Mise à jour du micrologiciel

OMIVV vous permet d'effectuer des tâches de mise à jour du BIOS et du firmware 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.

REMARQUE : Dans un environnement à plusieurs appliances, pour exécuter la mise à jour du firmware sur un cluster ou un hôte, assurez-vous que l'appliance enregistrée auprès de la vCenter cible est chargée.

Voici les deux méthodes permettant d'effectuer les mises à jour du firmware :

- DUP unique : effectue une mise à jour de firmware pour l'iDRAC et le BIOS 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.
- Profils de logithèque : effectue les mises à jour des firmwares et des pilotes. Cette méthode peut être utilisée à la fois au niveau hôte et au niveau cluster.

  Vous trouverez ci-dessous les profils de logithèque utilisés pour les mises à jour de firmware et de pilote :

  - Logithèque de firmwares : profil de logithèque qui utilise le catalogue de firmwares pour obtenir les informations sur le firmware.

    Voici les deux types de logithèques de firmwares :

    - Logithèque de firmwares créée par l'utilisateur
    - Logithèque de firmwares créée en usine : les deux types de catalogues sont créés en usine. Les catalogues créés en usine ne sont pas applicables à la mise à jour du firmware de cluster vSAN et à la configuration de la ligne de base.
      - Catalogue par défaut Dell : profil de logithèque de firmwares créé en usine qui utilise le catalogue Dell EMC en ligne pour obtenir les dernières informations sur le firmware. Si l'appliance n'a pas de connexion Internet modifiez cette logithèque de sorte qu'elle pointe vers un partage local basé sur CIFS ou NFS ou HTTP ou HTTPS.
      - Catalogue de piles MX validées : profil de logithèque de micrologiciels créé en usine qui utilise le catalogue Dell EMC en ligne pour obtenir les informations sur le micrologiciel validées pour le châssis MX et ses traîneaux correspondants.

  - Logithèque de pilotes : profil de logithèque contenant des lots hors ligne qui peuvent être utilisés pour mettre à jour le pilote des clusters vSAN.

  L'assistant de mise à jour du firmware vérifie toujours les niveaux minimum du firmware d'iDRAC et du BIOS, et tente de les mettre à jour aux versions minimales requises. Voir *OpenManage Integration for VMware vCenter Compatibility Matrix* (Matrice de compatibilité d'OpenManage Integration for VMware vCenter) pour plus d'informations sur les niveaux minimums de firmware pour l'iDRAC et le BIOS. Lorsque les versions du firmware d'iDRAC et du BIOS satisfont les conditions minimales, le processus de mise à jour du firmware permet d'effectuer les mises à jour de toutes les versions du firmware, y compris : iDRAC, RAID, contrôleur, carte NIC, BIOS, etc.

REMARQUE : Pour mettre à jour le serveur PowerEdge XR2, OMIVV utilise les composants de firmware R440 présents dans le catalogue en ligne Dell. Si vous souhaitez créer un catalogue personnalisé (à l'aide de DRM) à utiliser pour la logithèque de firmware hors ligne afin de prendre en charge PowerEdge XR2, utilisez les composants de firmware applicables au serveur PowerEdge R440.

Mise à jour du firmware et du pilote sur un hôte vSAN

Avant de planifier la mise à jour du firmware sur les hôtes vSAN (hôtes dans un cluster avec vSAN activé), assurez-vous que les conditions suivantes sont réunies dans l'environnement :

- Assurez-vous que l'hôte est conforme (CSIOR activé et l'hôte doit avoir la version de ESXi prise en charge) et qu'il est associé à un profil d'identification d'hôte et correctement inventorié.
- Les conditions préalables suivantes sont vérifiées avant la planification de la mise à jour du firmware :
  - L'option DRS est activée.

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

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

- Pour les composants du contrôleur de stockage, du disque dur et du disque SSD, les versions des pilotes et firmwares sélectionnées dans les logithèques sélectionnées sont conformes aux instructions de VMware en fonction de la version de vSAN.
- Pour les pilotes, OMIVV ne prend en charge que les lots hors ligne répertoriés dans la liste de compatibilité matérielle VMware.
- Le cluster répond aux exigences vSAN pour l'option de migration de données sélectionnée. Si le cluster vSAN ne répond pas aux exigences de l'option de migration de données sélectionnée, la mise à jour expire.
- Dell EMC recommande de sélectionner la logithèque de pilotes ou de firmwares de la ligne de base (Profil de cluster).
- Assurez-vous qu'il n'y a pas de tâches de mise à jour de firmware actives pour tous les hôtes du cluster que vous mettez à jour.
- Veillez à spécifier la valeur de délai d'attente requis pour la tâche « Accéder au mode de maintenance ». Si le temps d'attente dépasse le délai spécifié, la tâche de mise à jour échoue. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.
- Exécutez de nouveau l'inventaire après avoir activé vSAN.

Pendant le processus de mise à jour du firmware, Dell EMC recommande de ne pas supprimer ou déplacer les éléments suivants :

- Hôte de vCenter visé par la tâche de mise à jour de micrologiciel en cours.
- Profil d'identification d'hôte visé par la tâche de mise à jour de firmware en cours.
- Les logithèques situées dans CIFS ou NFS.

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.

1. Pour lancer l'assistant de mise à jour du firmware, sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, puis effectuez l'une des actions suivantes :
   - Faites un clic droit sur un hôte, sélectionnez **Actions de l'hôte OMIVV** > **Mise à jour du firmware**.
   - Sélectionnez un hôte dans le volet de droite, sélectionnez **Surveiller** > **Informations sur l'hôte OMIVV** > **Firmware** > **Lancer l'assistant du firmware**.
   - Sélectionnez un hôte, dans le volet de droite, sélectionnez **Résumé**, puis accédez à **Informations sur l'hôte OMIVV** > **Actions de l'hôte** > **Lancer l'assistant du firmware**.
2. Sur la page **Liste de vérification de la mise à jour du firmware**, assurez-vous que toutes les conditions préalables sont vérifiées avant de planifier la mise à jour, puis cliquez sur **DÉMARRER**.
3. Sur la page **Source de la mise à jour**, sélectionnez l'une des options suivantes :
   - **Profils de logithèque**
   - **Un DUP**
4. Pour charger une seule mise à jour de micrologiciel depuis un fichier, sélectionnez **DUP unique**.
   a. Un DUP unique peut résider sur un partage CIFS ou NFS qui est accessible par l'appliance OMIVV. Saisissez l'emplacement du fichier dans l'un des formats suivants, puis passez à l'étape 9.
      - NFS : `<hôte>:/<chemin_partage/NomFichier.exe`
      - CIFS : `\\<chemin de partage accessible d'hôte>\<NomFichier>.exe`

      REMARQUE : Assurez-vous que le nom de fichier des DUP de composant unique ne comprend pas d'espace.

      Pour le partage CIFS, OMIVV vous invite à entrer le nom d'utilisateur et le mot de passe pour accéder au lecteur de partage.
5. Si vous sélectionnez l'option **Profils de logithèques**, sélectionnez les profils de logithèque de firmwares et de pilotes.

   Si le profil de cluster est associé au cluster dans lequel l'hôte est présent, par défaut, les profils de firmwares et de pilotes associés sont sélectionnés.

   Si vous modifiez les profils de logithèque de firmwares ou de pilotes, un message s'affiche pour indiquer que le profil de logithèque sélectionné n'est pas associé à une ligne de base et que l'utilisation d'un autre référentiel peut affecter la comparaison de la ligne de base.

   REMARQUE : Si vous avez des logithèques de pilotes et de firmwares associés au profil de cluster, celui-ci est recommencé pour mettre à jour simultanément les pilotes et les firmwares.

   Si vous ne souhaitez pas mettre à jour le firmware ou le pilote, ou que le firmware ou le pilote est déjà à jour, dans le menu déroulant, sélectionnez **Aucune logithèque sélectionnée**.

Les catalogues de firmware par défaut (catalogue par défaut Dell EMC et catalogue de piles MX validé) ne s'affichent pas dans l'option Profil de logithèque. Pour utiliser les profils de logithèque, créez une logithèque personnalisée dans OMIVV.

Pour créer un profil de logithèque personnalisée, procédez comme suit :

a. Accédez à Dell EMC Repository Manager (DRM) et créez un catalogue.

   Pour plus d'informations sur la création d'un catalogue en utilisant DRM, voir Création d'un catalogue dans Dell EMC Repository Manager (DRM) en utilisant l'OMIVV , page 137.

b. Téléchargez le catalogue et les fichiers correspondants.

c. Créez un profil de logithèque dans l'OMIVV à l'aide du catalogue téléchargé.

   Pour plus d'informations sur la création d'un profil de logithèque, voir Création d'un profil de logithèque , page 48.

6. En fonction du profil de logithèque de firmwares que vous avez sélectionné, sélectionnez un ensemble approprié, puis cliquez sur **SUIVANT**. Seuls les lots 64 bits sont pris en charge.
7. Sur la page **Sélectionner les composants du pilote**, sélectionnez les composants de firmware qui nécessitent une mise 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.

   Vous pouvez utiliser l'option de filtre pour filtrer les données en fonction des noms de colonne spécifiques.
8. Sur la page **Sélectionner les composants du firmware**, sélectionnez les composants du firmware qui nécessitent une mise à jour, puis cliquez sur **SUIVANT**.

   Le nombre de composants en fonction de l'état de gravité (urgent, recommandé, facultatif et rétrogradation) s'affiche.

   Les composants dont la version est inférieure à la version disponible dans le catalogue ou qui sont dans le même niveau (à jour) ou planifiés pour une mise à jour ne peuvent pas être sélectionnés. Pour sélectionner les composants dont la version est inférieure à la version disponible, cochez la case **Autoriser la rétrogradation du firmware**.

   Pour sélectionner tous les composants du firmware sur toutes les pages, cliquez sur  .

   Pour désélectionner tous les composants du firmware sur toutes les pages, cliquez sur  .
9. Sur la page **Planifier les mises à jour**, saisissez le nom et la description de la tâche de mise à jour du firmware. La description est facultative.

   Le nom de la tâche de mise à jour du firmware est obligatoire. Si vous supprimez le nom d'une tâche de mise à jour du micrologiciel, vous pouvez le réutiliser.
10. Sous la section **Paramètres supplémentaires**, procédez comme suit :

    a. Saisissez une valeur d'expiration du délai en mode maintenance entre 60 et 1440 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.

    b. Dans le menu déroulant **Saisir l'option de mode de maintenance**, sélectionnez une option de migration de données appropriée. Pour plus d'informations sur l'option de migration des données, reportez-vous à la documentation VMware.

       REMARQUE : La tâche pour passer en mode maintenance échoue si la configuration du cluster ne prend pas en charge la migration complète des données ou si la capacité de stockage est insuffisante.

       Par défaut, les options suivantes sont sélectionnées.

       - **Quitter le mode de maintenance après la fin de la mise à jour du firmware** : si vous désactivez cette option, l'hôte reste en mode de maintenance.
       - **Déplacer les machines virtuelles hors tension et suspendues sur d'autres hôtes du cluster** : la désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.

    c. En cas de problèmes lors de la mise à jour du firmware, sélectionnez **Supprimer la file d'attente des travaux et réinitialiser iDRAC**. Cela peut permettre de mener à bien le processus de mise à jour. Ceci augmente la vitesse globale de mise à jour nécessaire pour terminer la tâche, annule toutes les tâches ou activités en attente planifiées sur l'iDRAC et réinitialise l'iDRAC.

       La suppression de la file d'attente n'est pas prise en charge pour les hôtes gérés à l'aide du profil d'identification de châssis.

       Par défaut, l'option **Vérifier les conditions préalables** est sélectionnée.
11. Dans la section **Planification des mises à jour**, sélectionnez l'une des options suivantes :

    - **Mettre à jour maintenant**
    - **Planifier une mise à jour**
    - **Appliquer les mises à jour lors du prochain redémarrage**
12. Sur la page **Aperçu du résumé**, vérifiez les informations de mise à jour du firmware, puis cliquez sur **TERMINER**.
    Les tâches de mise à jour du firmware peuvent nécessiter plusieurs heures en fonction des composants et du nombre de serveurs sélectionnés. Vous pouvez afficher l'état des tâches de mise à jour du firmware sur la page **Tâches**.

Une fois la tâche de mise à jour du firmware 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**.

Création d'un catalogue dans Dell EMC Repository Manager (DRM) en utilisant l'OMIVV

Cette section décrit le processus de création d'un catalogue dans un serveur d'applications DRM, versions 3.0 et ultérieures.

1. Accédez à Télécharger DRM et téléchargez DRM.
2. Sur la page d'accueil de DRM, cliquez sur **Ajouter une logithèque**.
   La fenêtre **Ajouter une logithèque** s'affiche.
3. Dans la fenêtre **Ajouter une logithèque**, effectuez les opérations suivantes :
   a. Saisissez le **Nom de la logithèque** et la **Description**.
   b. Dans le menu déroulant **Catalogue de base**, sélectionnez un catalogue.
   c. Dans le menu déroulant **Type d'intégration**, sélectionnez **OpenManage Integration for VMware vCenter**.
4. Dans la fenêtre **OpenManage Integration for VMware vCenter**, saisissez l'**IP de l'appliance virtuelle**, l'**IP du serveur vCenter**, les **Nom d'utilisateur** et **Mot de passe**, puis cliquez sur **Connecter**.
   Le catalogue créé s'affiche sur la page d'accueil.
5. Pour exporter le catalogue, sélectionnez un catalogue et cliquez sur **Exporter**.

Mise à jour du firmware et du pilote sur le cluster vSAN

Avant de planifier la mise à jour du firmware, assurez-vous que les conditions suivantes sont réunies dans l'environnement :

- Assurez-vous que l'hôte est conforme (CSIOR activé et l'hôte doit avoir la version de ESXi prise en charge) et qu'il est associé à un profil d'identification d'hôte et correctement inventorié. Si l'hôte n'est pas répertorié, lancez l'assistant de conformité de gestion pour les hôtes à partir d'OMIVV, puis utilisez l'assistant de mise à jour du firmware.
- Les conditions préalables suivantes sont vérifiées avant la planification de la mise à jour du firmware :
  - L'option DRS est activée.
  - L'hôte n'est pas déjà en mode de maintenance.
  - Les objets de données vSAN sont intègres.
- Pour les composants du contrôleur de stockage, du disque dur et du disque SSD, assurez-vous que les versions des pilotes et firmwares sélectionnées dans les logithèques sélectionnées sont conformes aux instructions de VMware en fonction de la version de vSAN.
- Pour les pilotes, OMIVV ne prend en charge que les lots hors ligne répertoriés dans la liste de compatibilité matérielle VMware.
- Le cluster répond aux exigences vSAN pour l'option de migration de données sélectionnée. Si le cluster vSAN ne répond pas aux exigences de l'option de migration de données sélectionnée, la mise à jour expirera.
- Dell EMC recommande de sélectionner la logithèque de pilotes ou de firmwares de la ligne de base (Profil de cluster).
- Assurez-vous qu'il n'y a pas de tâches de mise à jour de firmware actives pour tous les hôtes du cluster que vous mettez à jour.
- Veillez à spécifier la valeur de délai d'attente requis pour la tâche « Accéder au mode de maintenance ». Si le temps d'attente dépasse le délai spécifié, la tâche de mise à jour échoue. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.
- Veillez à exécuter de nouveau l'inventaire après avoir activé vSAN.

Pendant le processus de mise à jour du firmware, Dell EMC recommande de ne pas supprimer ou déplacer les éléments suivants :

- Les hôtes d'un cluster de vCenter pour lesquels la tâche de mise à jour du firmware est en cours.
- Profil d'identification d'hôte visé par la tâche de mise à jour de firmware en cours.
- Les logithèques situées dans CIFS ou NFS.

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

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.

1. Pour lancer l'assistant de mise à jour du firmware, sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, puis effectuez l'une des actions suivantes :
   - Faites un clic droit sur un cluster, sélectionnez **Actions du cluster OMIVV** > **Mise à jour du firmware**.

- Sélectionnez un cluster dans le volet de droite, sélectionnez **Surveiller** > **Informations sur le cluster OMIVV** > **Firmware** > **Lancer l'assistant du firmware**.

2. Sur la page **Liste de vérification de la mise à jour du firmware**, assurez-vous que toutes les conditions préalables sont vérifiées avant de planifier la mise à jour, puis cliquez sur **DÉMARRER**.
3. Sur la page **Source de la mise à jour**, sélectionnez les profils de logithèque de firmwares et de pilotes.

   Si le profil de cluster est associé au cluster dans lequel l'hôte est présent, par défaut, les profils de firmwares et de pilotes associés sont sélectionnés.

   Si vous modifiez les profils de logithèque de firmwares ou de pilotes, un message s'affiche pour indiquer que le profil de logithèque sélectionné n'est pas associé à une ligne de base et que l'utilisation d'un autre référentiel peut affecter la comparaison de la ligne de base.

   REMARQUE : Si vous avez des logithèques de pilotes et de firmwares associés au profil de cluster, celui-ci est recommencé pour mettre à jour simultanément les pilotes et les firmwares.

   Si vous ne souhaitez pas mettre à jour le firmware ou le pilote, ou que le firmware ou le pilote est déjà à jour, dans le menu déroulant, sélectionnez **Aucune logithèque sélectionnée**.

   Les catalogues de firmware par défaut (catalogue par défaut Dell EMC et catalogue de piles MX validé) ne s'affichent pas dans l'option Profil de logithèque. Pour utiliser les profils de logithèque, créez une logithèque personnalisée dans OMIVV.

   Pour créer un profil de logithèque personnalisée, procédez comme suit :

   a. Accédez à Dell EMC Repository Manager (DRM) et créez un catalogue.

      Pour plus d'informations sur la création d'un catalogue en utilisant DRM, voir Création d'un catalogue dans Dell EMC Repository Manager (DRM) en utilisant l'OMIVV , page 137.

   b. Téléchargez le catalogue et les fichiers correspondants.
   c. Créez un profil de logithèque dans l'OMIVV à l'aide du catalogue téléchargé.

      Pour plus d'informations sur la création d'un profil de logithèque, voir Création d'un profil de logithèque , page 48.

4. En fonction du profil de logithèque de firmwares que vous avez sélectionné, sélectionnez un ensemble approprié, puis cliquez sur **SUIVANT**. Seuls les lots 64 bits sont pris en charge.

   REMARQUE : Vous ne pouvez sélectionner qu'un seul lot pour les serveurs OEM (démarqués), même s'ils sont de différents modèles. Même si le lot ne s'applique pas à un ou plusieurs serveurs OEM, la page Composants de l'assistant de mise à jour du firmware répertorie chaque paire de serveurs OEM ou de composants de firmware. En cas d'échec de la mise à jour du firmware pour une paire de composants firmwares donnée, réessayez avec l'autre lot affiché pour le serveur OEM.

5. Sur la page **Sélectionner les composants du pilote**, sélectionnez les composants de firmware qui nécessitent une mise 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.

   Vous pouvez utiliser l'option de filtre pour filtrer les données en fonction des noms de colonne spécifiques.
6. Sur la page **Sélectionner les composants du firmware**, sélectionnez les composants du firmware qui nécessitent une mise à jour, puis cliquez sur **SUIVANT**.

   Le nombre de composants en fonction de l'état de gravité (urgent, recommandé, facultatif et rétrogradation) s'affiche.

   Vous pouvez utiliser l'option de filtre pour filtrer les données en fonction des noms de colonne spécifiques.

   Les composants dont la version est inférieure à la version disponible dans le catalogue ou qui sont dans le même niveau (à jour) ou planifiés pour une mise à jour ne peuvent pas être sélectionnés. Pour sélectionner les composants dont la version est inférieure à la version disponible, cochez la case **Autoriser la rétrogradation du firmware**.

   Pour sélectionner tous les composants du firmware sur toutes les pages, cliquez sur  .

   Pour désélectionner tous les composants du firmware sur toutes les pages, cliquez sur  .
7. Sur la page **Planifier les mises à jour**, saisissez le nom et la description de la tâche de mise à jour du firmware. La description est facultative.

   Le nom de la tâche de mise à jour du firmware est obligatoire. Si vous supprimez le nom d'une tâche de mise à jour du micrologiciel, vous pouvez le réutiliser.
8. Sous la section **Paramètres supplémentaires**, procédez comme suit :

   a. Saisissez une valeur d'expiration du délai en mode maintenance entre 60 et 1440 minutes. Si le temps d'attente dépasse le temps indiqué, les tâches 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.
   b. Dans le menu déroulant **Saisir l'option de mode de maintenance**, sélectionnez une option de migration de données appropriée. Pour plus d'informations sur l'option de migration des données, reportez-vous à la documentation VMware.

REMARQUE : La tâche pour passer en mode maintenance échoue si la configuration du cluster ne prend pas en charge la migration complète des données ou si la capacité de stockage est insuffisante.

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

c. En cas de problèmes lors de la mise à jour du firmware, sélectionnez **Supprimer la file d'attente des travaux et réinitialiser iDRAC**. Cela peut permettre de mener à bien le processus de mise à jour. Ceci augmente la vitesse globale de mise à jour nécessaire pour terminer la tâche, annule toutes les tâches ou activités en attente planifiées sur l'iDRAC et réinitialise l'iDRAC.

La suppression de la file d'attente n'est pas prise en charge pour les hôtes gérés à l'aide du profil d'identification de châssis.

9. Dans la section **Planification des mises à jour**, sélectionnez l'une des options suivantes :
   - **Mettre à jour maintenant**
   - **Planifier une mise à jour**
10. Sur la page **Aperçu du résumé**, vérifiez les informations de mise à jour du firmware, puis cliquez sur **TERMINER**.
    Les tâches de mise à jour du firmware peuvent nécessiter plusieurs heures en fonction des composants et du nombre de serveurs sélectionnés. Vous pouvez afficher l'état des tâches de mise à jour du firmware sur la page **Tâches**.

    Une fois la tâche de mise à jour du firmware 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**.

Mise à jour du firmware sur l'hôte vSphere

Avant de planifier la mise à jour du firmware sur les hôtes vSphere (ESXi uniquement), assurez-vous que les conditions suivantes sont réunies dans l'environnement :

- Assurez-vous que l'hôte est conforme (CSIOR activé et l'hôte doit avoir la version de ESXi prise en charge) et qu'il est associé à un profil d'identification d'hôte et correctement inventorié.
- La DRS est activée.

  REMARQUE : Dans le cas d'un hôte autonome, la vérification de la DRS ne s'applique pas.

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

  REMARQUE : La mise à jour du pilote n'est pas prise en charge sur le cluster et l'hôte vSphere.

Pendant le processus de mise à jour du firmware, Dell EMC recommande de ne pas supprimer ou déplacer les éléments suivants :

- Hôte de vCenter visé par la tâche de mise à jour de micrologiciel en cours.
- Profil d'identification d'hôte visé par la tâche de mise à jour de firmware en cours.
- Les logithèques situées dans CIFS ou NFS.

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.

1. Pour lancer l'assistant de mise à jour du firmware, sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, puis effectuez l'une des actions suivantes :
   - Faites un clic droit sur un hôte, sélectionnez **Actions de l'hôte OMIVV** > **Mise à jour du firmware**.
   - Sélectionnez un hôte dans le volet de droite, sélectionnez **Surveiller** > **Informations sur l'hôte OMIVV** > **Firmware** > **Lancer l'assistant du firmware**.
   - Sélectionnez un hôte, dans le volet de droite, sélectionnez **Résumé**, puis accédez à **Informations sur l'hôte OMIVV** > **Actions de l'hôte** > **Lancer l'assistant du firmware**.
2. Sur la page **Liste de vérification de la mise à jour du firmware**, assurez-vous que toutes les conditions préalables sont vérifiées avant de planifier la mise à jour, puis cliquez sur **DÉMARRER**.
3. Sur la page **Source de la mise à jour**, sélectionnez l'une des options suivantes :
   - **Profils de logithèque**
   - **Un DUP**
4. Pour charger une seule mise à jour de micrologiciel depuis un fichier, sélectionnez **DUP unique**.
   a. Un DUP unique peut résider sur un partage CIFS ou NFS qui est accessible par l'appliance OMIVV. Saisissez l'emplacement du fichier dans l'un des formats suivants, puis passez à l'étape 8.
      - NFS : `<hôte>:/<chemin_partage/NomFichier.exe`

- CIFS : `\\<chemin de partage accessible d'hôte>\<NomFichier>.exe`

REMARQUE : Assurez-vous que le nom de fichier des DUP de composant unique ne comprend pas d'espace.

Pour le partage CIFS, OMIVV vous invite à entrer le nom d'utilisateur et le mot de passe pour accéder au lecteur de partage.

5. Si vous sélectionnez l'option **Profils de logithèques**, sélectionnez le profil de logithèque de firmwares.

   Si le profil de cluster est associé au cluster dans lequel l'hôte est présent, par défaut, le profil de firmwares associé est sélectionné. Sinon, c'est l'option **Catalogue Dell par défaut** qui est sélectionnée.

   Si vous modifiez les profils de logithèque de firmwares, un message s'affiche pour indiquer que le profil de logithèque sélectionné n'est pas associé à une ligne de base et que l'utilisation d'un autre référentiel peut affecter la comparaison de la ligne de base.

6. En fonction du profil de logithèque de firmwares que vous avez sélectionné, sélectionnez un ensemble approprié, puis cliquez sur **SUIVANT**. Seuls les lots 64 bits sont pris en charge.
7. Sur la page **Sélectionner les composants du firmware**, sélectionnez les composants du firmware qui nécessitent une mise à jour, puis cliquez sur **SUIVANT**.

   Le nombre de composants en fonction de l'état de gravité (urgent, recommandé, facultatif et rétrogradation) s'affiche.

   Vous pouvez utiliser l'option de filtre pour filtrer les données en fonction des noms de colonne spécifiques.

   Les composants dont la version est inférieure à la version disponible dans le catalogue ou qui sont dans le même niveau (à jour) ou planifiés pour une mise à jour ne peuvent pas être sélectionnés. Pour sélectionner les composants dont la version est inférieure à la version disponible, cochez la case **Autoriser la rétrogradation du firmware**.

   Pour sélectionner tous les composants du firmware sur toutes les pages, cliquez sur .

   Pour désélectionner tous les composants du firmware sur toutes les pages, cliquez sur .
8. Sur la page **Planifier les mises à jour**, saisissez le nom et la description de la tâche de mise à jour du firmware. La description est facultative.

   Le nom de la tâche de mise à jour du firmware est obligatoire. Si vous supprimez le nom d'une tâche de mise à jour du micrologiciel, vous pouvez le réutiliser.
9. Sous la section **Paramètres supplémentaires**, procédez comme suit :
   a. Saisissez une valeur d'expiration du délai en mode maintenance entre 60 et 1440 minutes. Si le temps d'attente dépasse le temps indiqué, les tâches 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.

      Par défaut, les options suivantes sont sélectionnées.

      - **Quitter le mode de maintenance après la fin de la mise à jour du firmware** : si vous désactivez cette option, l'hôte reste en mode de maintenance.
      - **Déplacer les machines virtuelles hors tension et suspendues sur d'autres hôtes du cluster** : la désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que le périphérique hôte soit en ligne.

   b. En cas de problèmes lors de la mise à jour du firmware, sélectionnez **Supprimer la file d'attente des travaux et réinitialiser iDRAC**. Cela peut permettre de mener à bien le processus de mise à jour. Ceci augmente la vitesse globale de mise à jour nécessaire pour terminer la tâche, annule toutes les tâches ou activités en attente planifiées sur l'iDRAC et réinitialise l'iDRAC.

      La suppression de la file d'attente n'est pas prise en charge pour les hôtes gérés à l'aide du profil d'identification de châssis.

      Par défaut, l'option **Vérifier les conditions préalables** est sélectionnée.
10. Dans la section **Planification des mises à jour**, sélectionnez l'une des options suivantes :

    - **Mettre à jour maintenant**
    - **Planifier une mise à jour**
    - **Appliquer les mises à jour lors du prochain redémarrage**
    - **Appliquer les mises à jour et forcer le redémarrage sans passer en mode Maintenance**
11. Sur la page **Aperçu du résumé**, vérifiez les informations de mise à jour du firmware, puis cliquez sur **TERMINER**.
    Les tâches de mise à jour du firmware peuvent nécessiter plusieurs heures en fonction des composants et du nombre de serveurs sélectionnés. Vous pouvez afficher l'état des tâches de mise à jour du firmware sur la page **Tâches**.

    Une fois la tâche de mise à jour du firmware 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**.

Mise à jour du firmware sur le cluster vSphere

Avant de planifier la mise à jour du firmware, assurez-vous que les conditions suivantes sont réunies dans l'environnement :

- Assurez-vous que l'hôte est conforme (CSIOR activé et l'hôte doit avoir la version de ESXi prise en charge) et qu'il est associé à un profil d'identification d'hôte et correctement inventorié. Si l'hôte n'est pas répertorié, lancez l'assistant de conformité de gestion pour les hôtes à partir d'OMIVV, puis utilisez l'assistant de mise à jour du firmware.
- La DRS est activée.
- Assurez-vous qu'il n'y a pas de tâches de mise à jour de firmware actives pour tous les hôtes du cluster que vous mettez à jour.
- Veillez à spécifier la valeur de délai d'attente requis pour la tâche « Accéder au mode de maintenance ». Si le temps d'attente dépasse le délai spécifié, la tâche de mise à jour échoue. Cependant, les composants peuvent être mis à jour automatiquement lorsque l'hôte est redémarré.

REMARQUE : La mise à jour du pilote n'est pas prise en charge sur le cluster et l'hôte vSphere.

Pendant le processus de mise à jour du firmware, Dell EMC recommande de ne pas supprimer ou déplacer les éléments suivants :

- Les hôtes d'un cluster de vCenter pour lesquels la tâche de mise à jour du firmware est en cours.
- Profil d'identification d'hôte visé par la tâche de mise à jour de firmware en cours.
- Les logithèques situées dans CIFS ou NFS.

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

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.

1. Pour lancer l'assistant de mise à jour du firmware, sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, puis effectuez l'une des actions suivantes :
   - Faites un clic droit sur un cluster, sélectionnez **Actions du cluster OMIVV** > **Mise à jour du firmware**.
   - Sélectionnez un cluster dans le volet de droite, sélectionnez **Surveiller** > **Informations sur le cluster OMIVV** > **Firmware** > **Lancer l'assistant du firmware**.
2. Sur la page **Liste de vérification de la mise à jour du firmware**, assurez-vous que toutes les conditions préalables sont vérifiées avant de planifier la mise à jour, puis cliquez sur **DÉMARRER**.
3. Sur la page **Source de la mise à jour**, si le profil de cluster est associé au cluster dans lequel l'hôte est présent, la logithèque de firmwares associée est sélectionnée par défaut. Sinon, c'est l'option **Catalogue Dell par défaut** qui est sélectionnée.

   Si vous modifiez les profils de logithèque de firmwares, un message s'affiche pour indiquer que le profil de logithèque sélectionné n'est pas associé à une ligne de base et que l'utilisation d'un autre référentiel peut affecter la comparaison de la ligne de base.
4. En fonction du profil de logithèque de firmwares que vous avez sélectionné, sélectionnez un ensemble approprié, puis cliquez sur **SUIVANT**. Seuls les lots 64 bits sont pris en charge.

   REMARQUE : Vous ne pouvez sélectionner qu'un seul lot pour les serveurs OEM (démarqués), même s'ils sont de différents modèles. Même si le lot ne s'applique pas à un ou plusieurs serveurs OEM, la page Composants de l'assistant de mise à jour du firmware répertorie chaque paire de serveurs OEM ou de composants de firmware. En cas d'échec de la mise à jour du firmware pour une paire de composants firmwares donnée, réessayez avec l'autre lot affiché pour le serveur OEM.
5. Sur la page **Sélectionner les composants du firmware**, sélectionnez les composants du firmware qui nécessitent une mise à jour, puis cliquez sur **SUIVANT**.

   Le nombre de composants en fonction de l'état de gravité (urgent, recommandé, facultatif et rétrogradation) s'affiche.

   Les composants dont la version est inférieure à la version disponible dans le catalogue ou qui sont dans le même niveau (à jour) ou planifiés pour une mise à jour ne peuvent pas être sélectionnés. Pour sélectionner les composants dont la version est inférieure à la version disponible, cochez la case **Autoriser la rétrogradation du firmware**.

   Vous pouvez utiliser l'option de filtre pour filtrer les données en fonction des noms de colonne spécifiques.

   Pour sélectionner tous les composants du firmware sur toutes les pages, cliquez sur l'  .

   Pour désélectionner tous les composants du firmware sur toutes les pages, cliquez sur l'  .
6. Sur la page **Planifier les mises à jour**, saisissez le nom et la description de la tâche de mise à jour du firmware. La description est facultative.

   Le nom de la tâche de mise à jour du firmware est obligatoire. Si vous supprimez le nom d'une tâche de mise à jour du micrologiciel, vous pouvez le réutiliser.

7. Sous la section **Paramètres supplémentaires**, procédez comme suit :
   a. Saisissez une valeur d'expiration du délai en mode maintenance entre 60 et 1440 minutes. Si le temps d'attente dépasse le temps indiqué, les tâches 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.

      Par défaut, l'option **Déplacer les machines virtuelles hors tension et suspendues sur d'autres hôtes du cluster** est sélectionnée. La désactivation de cette option déconnecte la machine virtuelle jusqu'à ce que l'appareil de l'hôte soit en ligne.
   b. En cas de problèmes lors de la mise à jour du firmware, sélectionnez **Supprimer la file d'attente des travaux et réinitialiser iDRAC**. Cela peut permettre de mener à bien le processus de mise à jour. Ceci augmente la vitesse globale de mise à jour nécessaire pour terminer la tâche, annule toutes les tâches ou activités en attente planifiées sur l'iDRAC et réinitialise l'iDRAC.

      La suppression de la file d'attente n'est pas prise en charge pour les hôtes gérés à l'aide du profil d'identification de châssis.
8. Dans la section **Planification des mises à jour**, sélectionnez l'une des options suivantes :
   - **Mettre à jour maintenant**
   - **Planifier une mise à jour**
9. Sur la page **Aperçu du résumé**, vérifiez les informations de mise à jour du firmware, puis cliquez sur **TERMINER**.
   Les tâches de mise à jour du firmware peuvent nécessiter plusieurs heures en fonction des composants et du nombre de serveurs sélectionnés. Vous pouvez afficher l'état des tâches de mise à jour du firmware sur la page **Tâches**.

   Une fois la tâche de mise à jour du firmware 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**.

Mise à jour du même type de composant de firmware

Vous trouverez ci-après les points clés à retenir lors de la mise à jour des composants de firmware du même type :

- Si plusieurs composants du même type dotés de mêmes versions sont présents sur le serveur, une seule version du composant est affichée sur la page **Sélectionner les composants du firmware**. La mise à jour s'applique à tous les composants et les détails de la dérive s'affichent pour une seule version du composant.

  Par exemple :

  Tableau 19. Exemple pour plusieurs composants avec le même type présents sur le serveur

Composant	Version actuelle	Version disponible
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

  Dans ce cas, la page **Sélectionner les composants du firmware** affiche les éléments suivants :

  Tableau 20. Exemple pour plusieurs composants de la même version présents sur le serveur

Composant	Version actuelle	Version disponible
HDD1	V1	V3

- Si plusieurs composants du même type avec différentes versions sont présents sur le serveur, un seul composant s'affiche pour chaque version. Dans ce cas, si vous sélectionnez un composant, la mise à jour sera appliquée à tous les composants, quelles que soient leurs versions de firmware actuelles. Les informations de dérive s'affichent pour tous les composants, quelles que soient leurs versions de firmware actuelles.

  Par exemple :

  Tableau 21. Exemple pour plusieurs composants avec différentes versions présents sur le serveur

Composant	Version actuelle	Version disponible
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

  Dans ce cas, la page **Sélectionner les composants du firmware** affiche les éléments suivants :

Tableau 22. Exemple pour plusieurs composants avec différentes versions présents sur le serveur

Composant	Version actuelle	Version disponible
HDD1	V1	V3
HDD2	V2	V3

- Si le catalogue contient plusieurs versions disponibles, il est recommandé de ne sélectionner qu'une seule des versions disponibles pour un type de composant. Le firmware sélectionné est alors appliqué à tous les composants applicables, quelle que soit leur version actuelle.

  Par exemple :

Tableau 23. Exemple pour plusieurs versions disponibles présentes dans le catalogue

Composant	Version actuelle	Version disponible
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

Dans ce cas, la page **Sélectionner les composants du firmware** affiche les éléments suivants :

Tableau 24. Exemple pour plusieurs versions disponibles présentes dans le catalogue

Composant	Version actuelle	Version disponible
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

Présentation de vSphere Lifecycle Manager

vSphere Lifecycle Manager est un service qui s'exécute dans le serveur vCenter (applicable pour vCenter 7.0 et versions ultérieures).

vSphere Lifecycle Manager vous permet de créer une image de base composée de l'image ESXi, du firmware et du pilote. Il s'assure que chaque hôte du cluster est aligné sur l'image de base en effectuant une vérification de conformité. En cas de non-conformité, il fournit une option pour corriger le cluster.

Dans vSphere Lifecycle Manager, OMIVV agit en tant que fournisseur du module complémentaire de firmwares. Pour plus d'informations sur vSphere Lifecycle Manager, reportez-vous à la documentation VMware.

Pour utiliser vSphere Lifecycle Manager avec OMIVV, l'enregistrement de vCenter est requis. Pour plus d'informations sur l'enregistrement de vCenter et de vSphere Lifecycle Manager, reportez-vous à la section Enregistrement d'un nouveau serveur vCenter , page 13.

Vous pouvez enregistrer vSphere Lifecycle Manager (applicable pour vCenter 7 0 et versions ultérieures) dans la console d'administration Dell EMC lors de l'enregistrement de vCenter. Une fois l'enregistrement de vCenter terminé, vous pouvez modifier (enregistrer ou désenregistrer) l'état de l'enregistrement de vSphere Lifecycle Manager sur la page **ENREGISTREMENT VCENTER** de la console d'administration Dell EMC. Pour de plus amples informations, consultez Inscription de vSphere Lifecycle Manager dans la Console Administration Dell EMC , page 144 et Annulation de l'enregistrement de vSphere Lifecycle Manager dans la Console Administration Dell EMC , page 144.

Afficher l'état du vSphere LifeCycle Manager dans la console d'administration Dell EMC

Vous trouverez ci-dessous les états possibles de vSphere Lifecycle Manager que vous pouvez afficher dans la colonne **vSphere Lifecycle Manager** :

- **Enregistrer** (applicable uniquement pour vCenter 7.0 et versions ultérieures) : s'affiche lorsque vSphere Lifecycle Manager n'est pas enregistré.
- **Désenregistrer** (applicable uniquement pour vCenter 7.0 et versions ultérieures) : s'affiche lorsque vSphere Lifecycle Manager est déjà enregistré.
- **NA** : s'affiche uniquement si la version du vCenter enregistré est antérieure à 7.0. Si le vCenter est mis à niveau vers la version 7.0, l'état reste **NA**. Pour refléter l'état, redémarrez l'appliance OMIVV.

Inscription de vSphere Lifecycle Manager dans la Console Administration Dell EMC

La version de vCenter doit être 7.0 et versions supérieures.

1. Accédez à https://<ApplianceIP/hostname/>.
2. Sur la page **ENREGISTREMENT VCENTER**, sous **vSphere Lifecycle Manager**, cliquez sur **Enregistrer**.
   La boîte de dialogue **ENREGISTRER VSPHERE LIFECYCLE MANAGER** <nom de vCenter> s'affiche.
3. Cliquez sur **Enregistrer vSphere Lifecycle Manager**.
   Un message s'affiche indiquant que vSphere Lifecycle Manager a bien été enregistré.

Annulation de l'enregistrement de vSphere Lifecycle Manager dans la Console Administration Dell EMC

La version de vCenter doit être 7.0 et versions supérieures.

1. Accédez à https://<ApplianceIP/hostname/>.
2. Sur la page **ENREGISTREMENT VCENTER**, sous **vSphere Lifecycle Manager**, cliquez sur **Désenregistrer**.
   La boîte de dialogue **DÉSENREGISTRER VSPHERE LIFECYCLE MANAGER** <nom de vCenter> s'affiche.
3. Cliquez sur **Désenregistrer**.
   Un message s'affiche indiquant que le désenregistrement de vSphere Lifecycle Manager a bien été pris en compte. **OMIVV Dell EMC** est supprimé de la liste du **Gestionnaire de support matériel** dans vSphere Lifecycle Manager. Il n'y a pas d'impact sur les fonctionnalités d'OMIVV.

Gestion des clusters à l'aide de vSphere Lifecycle Manager

Configuration requise :

Avant de gérer les clusters à l'aide de vSphere Lifecycle Manager, assurez-vous que :

- vSphere Lifecycle Manager est activé dans la console d'administration Dell EMC. Pour plus d'informations, voir Inscription de vSphere Lifecycle Manager dans la Console Administration Dell EMC , page 144.
- Les hôtes des clusters sont conformes à la norme de gestion. Pour plus d'informations, voir Gestion de la conformité , page 71.
- Le profil de cluster est créé pour le cluster sélectionné et le profil de cluster est associé à la logithèque de firmwares dans OMIVV. Pour en savoir plus sur les profils cluster, voir Création d'un profil de cluster , page 52.

Vous pouvez gérer les clusters à l'aide de l'interface utilisateur et de l'API d'automatisation vSphere dans vSphere Lifecycle Manager. OMIVV prend en charge la gestion des clusters à l'aide de l'interface utilisateur et des API d'automatisation vSphere.

REMARQUE : Vous pouvez utiliser les actions du cluster OMIVV, telles que le verrouillage du système et la mise à jour du firmware dans les clusters gérés par vSphere Lifecycle Manager, mais cela peut avoir un impact sur les rapports de base.

Utilisation d'OMIVV en tant que fournisseur de module complémentaire de firmware dans vSphere LifeCycle Manager : interface utilisateur

Vous pouvez utiliser OMIVV avec vSphere Lifecycle Manager en tant que fournisseur du module complémentaire de firmware.

Le profil de cluster est appelé Hardware Support Package (HSP) dans le contexte de vSphere Lifecycle Manager. Le profil de cluster créé dans OMIVV est sélectionné en tant que **module complémentaire de firmware et de pilotes** dans vSphere Lifecycle Manager. Pour en savoir plus sur les profils cluster, voir Profil de cluster , page 52.

Pour configurer une image pour le cluster sélectionné et associer OMIVV en tant que **module complémentaire de firmware et de pilotes**, procédez comme suit :

1. Dans vSphere Client, cliquez sur **Hôtes et clusters**, puis sélectionnez le cluster que vous souhaitez gérer à l'aide d'une image.
2. Sur la page **Mises à jour**, dans le volet de gauche, développez **Hôtes**, puis cliquez sur **Images**.
3. Pour sélectionner un module de firmware et pilotes, cliquez sur l'icône Sélectionner.
   La page **Sélectionner un module complémentaire de firmware et de pilote** s'affiche.
4. Dans la section **Sélectionner le gestionnaire de support matériel**, sélectionnez **DellEMC OMIVV**.

   Après avoir sélectionné le **DellEMC OMIVV**, tous les profils de cluster associés à la logithèque de firmware et liés à un cluster dans le vCenter sélectionné sont répertoriés dans la section **Sélectionner un module complémentaire de firmware et de pilotes**.
5. Sélectionnez un profil de cluster applicable pour le cluster sélectionné, puis cliquez sur **SÉLECTIONNER**.

   Pour identifier le profil de cluster associé au cluster sélectionné, reportez-vous à la description présente dans le profil de cluster.

   REMARQUE : Si vous n'avez pas créé de profil de cluster dans OMIVV, une liste vide s'affiche. Pour en savoir plus sur la création d'un profil de cluster, voir Création d'un profil de cluster , page 52.

   - **Version du module complémentaire** : indique la version actuelle du profil de cluster. Si le profil de cluster est modifié ou si la version est incrémentée dans OMIVV, assurez-vous d'utiliser la version la plus récente du profil de cluster dans vSphere Lifecycle Manager.

     REMARQUE : Parfois, vSphere Lifecycle Manager affiche la non-conformité du firmware. Toutefois, le firmware non conforme n'est pas répertorié dans vSphere Lifecycle Manager. Pour résoudre ce problème, corrigez le cluster. La correction du cluster n'entraîne pas le redémarrage de vSphere Lifecycle Manager.
   - **Versions ESXi prises en charge** : indique la version ESXi prise en charge par OMIVV (7.0.0).

   Le profil de cluster sélectionné s'affiche en tant que module complémentaire de firmware sur la page **Mises à jour**.
6. Cliquez sur **ENREGISTRER**.
   vSphere Lifecycle Manager effectue la vérification de la conformité du cluster. Les résultats de la vérification de conformité s'affichent dans la section **Conformité d'image** de vSphere Lifecycle Manager.

   La conformité globale comprend la conformité du logiciel et la conformité des firmwares. OMIVV gère la partie conformité de firmware des tâches du vSphere Lifecycle Manager.

Afficher l'état de conformité du cluster

Vous trouverez ci-dessous l'état de conformité possible du firmware pour chaque hôte :

- **Conforme** : s'affiche lorsque les versions de firmwares de tous les composants de firmware installés sur l'hôte sont identiques à la version de firmware présente dans le profil de cluster dans OMIVV.
- **Non conforme** : s'affiche lorsqu'une ou plusieurs versions de firmwares installées sur l'hôte ne sont pas identiques à la version de firmware présente dans le profil de cluster dans OMIVV.

  REMARQUE : Après la mise à niveau de l'appliance OMIVV, la tâche de vérification de la conformité de vSphere Lifecycle Manager échoue pour les images créées avec une version antérieure d'OMIVV. Pour résoudre ce problème, enregistrez l'image avec la dernière version du Hardware Support Package (HSP).
- **Incompatible** : s'affiche dans les cas suivants :
  - Le cluster sélectionné dans vCenter n'est pas associé au **module complémentaire de firmware et de pilotes** sélectionné (profil de cluster dans OMIVV).
  - Si la logithèque de firmwares dans le profil de cluster est mise à jour après l'enregistrement de l'image vSphere Lifecycle Manager pour le cluster sélectionné.

- **Inconnu** : s'affiche si l'hôte n'est pas correctement inventorié dans OMIVV. Pour plus d'informations, voir Profil d'identification d'hôte , page 39.

REMARQUE : Il est possible que vous remarquiez une incohérence entre OMIVV et le rapport de dérive de vSphere Lifecycle Manager. Cela est dû au fait que le vSphere Lifecycle Manager affiche toujours le rapport de dérive en temps réel et OMIVV affiche le rapport de dérive basé sur la date et l'heure planifiées. En cas d'incohérence entre les rapports de dérive, exécutez la tâche de détection de dérive à la demande sur la page **Tâches de détection de dérive** d'OMIVV.

Résoudre les problèmes de conformité de cluster

1. Si l'état de l'hôte est **conforme**, aucune autre action n'est requise pour cet hôte.
2. Si l'état de l'hôte est **non conforme**, poursuivez la correction. Pour plus d'informations, voir Correction de cluster dans vSphere LifeCycle Manager , page 147.
3. Si l'état de l'hôte est **incompatible** :
   a. Vérifiez que le cluster sélectionné dans vCenter est associé à un profil de cluster. Sélectionnez le même profil de cluster que le **module complémentaire de firmware et de pilotes** dans vSphere Lifecycle Manager.
   b. Modifiez l'image du vSphere Lifecycle Manager et resélectionnez le profil de cluster mis à jour (module complémentaire de firmwares et de pilotes), puis enregistrez l'image.
4. Si l'état de l'hôte est **Inconnu**, assurez-vous que l'hôte est ajouté à un profil d'identification d'hôte dans OMIVV et que l'inventaire s'est correctement exécuté.

Vérification de compatibilité matérielle

vSphere Lifecycle Manager offre la possibilité d'effectuer une vérification de compatibilité matérielle pour le cluster vSAN avant d'effectuer la correction du firmware. La vérification de compatibilité matérielle compare le firmware et le pilote présents dans l'image avec le matériel et le pilote pris en charge qui sont répertoriés dans la liste de compatibilité matérielle (HCL) vSAN. vSphere Lifecycle Manager effectue des vérifications de compatibilité matérielle uniquement pour le contrôleur de stockage (périphériques PCIe). Pour obtenir la liste des firmwares pris en charge : dans vSphere Client, accédez à **Surveiller** > **vSAN** > **Intégrité Skyline**.

Pour effectuer la vérification de compatibilité matérielle, dans la section **Conformité d'image**, cliquez sur **VÉRIFIER LA CONFORMITÉ**.

Lors de l'exécution de la vérification de compatibilité matérielle, OMIVV renvoie les versions de firmware qui se trouvent dans le profil de cluster.

Si la version du firmware est compatible avec le firmware répertorié dans la liste de compatibilité matérielle (HCL), vSphere Lifecycle Manager affiche l'état de conformité **Compatible**. Pour plus d'informations sur l'état de conformité, reportez-vous à la documentation VMware.

Les résultats de la vérification de compatibilité matérielle s'affichent sur la page **Compatibilité matérielle**.

Exécuter une vérification préalable aux mesures correctives

L'opération de vérification préalable effectue différentes vérifications par rapport à chaque hôte dans un cluster afin de garantir la préparation du cluster pour la correction du firmware.

La vérification préalable est une tâche facultative qui peut être effectuée au niveau de l'hôte ou du cluster.

Vous pouvez ignorer l'opération de vérification préalable, vSphere Lifecycle Manager effectue une vérification préalable lors de la correction.

Dans le cadre de la vérification préalable, OMIVV effectue la vérification des conditions préalables des éléments suivants :

- Accessibilité à l'iDRAC
- Mode de verrouillage de l'iDRAC
- État de la tâche de mise à jour des firmwares (le cas échéant) déclenchée à partir d'OMIVV pour tous les hôtes du cluster sélectionné
- Activation de la fonction Collecter l'inventaire système au redémarrage (CSIOR)
- Connectivité à la logithèque de firmwares et aux composants requis.

Pour vérifier les conditions préalables pour la correction du firmware, cliquez sur **EXÉCUTER LA VÉRIFICATION PRÉALABLE**. L'état et les résultats de la tâche de vérification préalable s'affichent dans la section **Conformité d'image**.

Si la vérification préalable échoue pour un hôte, résolvez le problème et réexécutez la vérification préalable ou poursuivez la tâche de correction.

Correction de cluster dans vSphere LifeCycle Manager

Dans la section **Conformité d'image**, vous pouvez corriger un hôte individuel ou tous les hôtes du cluster à la fois.

a. Pour exécuter la tâche de correction pour un hôte individuel, dans la section **Image Compliance**, cliquez sur l'icône points de suspension verticaux à côté de l'hôte, puis sélectionnez **Corriger**.

b. Pour effectuer la tâche de correction pour tous les hôtes du cluster, dans la section **Conformité d'image**, cliquez sur **CORRIGER TOUT**.

   Il vous est recommandé d'effectuer une réinitialisation de l'iDRAC avant d'exécuter la mise à jour des firmwares. L'exécution de la réinitialisation de l'iDRAC réduit la possibilité d'échec.

   Pour réinitialiser automatiquement l'iDRAC avant d'effectuer la mise à jour du firmware à l'aide de vSphere Lifecycle Manager sur chaque hôte, cochez la case **Effacer les tâches et réinitialiser l'iDRAC** dans OMIVV. Pour plus d'informations, voir Paramètres de mise à jour de firmware , page 91.

Pour consulter l'état de la tâche de correction, cliquez sur **AFFICHER PLUS** sur la page **Mises à jour**.

Vous pouvez consulter les journaux relatifs à OMIVV sur la page **Journaux** d'OMIVV.

Utilisation d'OMIVV en tant que fournisseur de modules complémentaires de firmware dans vSphere Lifecycle Manager — API d'automatisation vSphere

Avant de gérer les clusters à l'aide de l'API d'automatisation vSphere, assurez-vous que vous avez effectué les tâches suivantes à l'aide de l'interface utilisateur de vSphere Lifecycle Manager :

- Sélectionnez DellEMC OMIVV comme gestionnaire de support matériel.
- Sélectionnez un profil de cluster applicable au cluster sélectionné, puis enregistrez l'image.

Analyser la conformité des firmwares

Commande : POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan

```
{
    "spec" : {
      "message": "test commit"
    }
}
```

Description : analysez tous les hôtes du cluster en fonction de l'état souhaité du cluster. Le résultat de cette opération peut être interrogé en appelant le `cis/tasks/{task-id}`, où l'ID de tâche est la réponse de cette opération.

Codes de réponse HTTP : 200. Pour obtenir la liste de tous les codes de réponse, voir Codes de réponse , page 182.

Exemple de réponse :

```
{task ID}
```

Obtenir l'état des tâches de conformité

Commande : GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

Description : renvoie des informations sur une tâche.

Codes de réponse HTTP : 200. Pour obtenir la liste de tous les codes de réponse, voir Codes de réponse , page 182.

Exemple de réponse : l'exemple suivant contient uniquement la non-conformité du firmware.


```
"result":
[
{
 "value":
[
{
"value":
{
"hardware_modules":
[
{
 "value":
 {
 "current":
 {
 "version": "25.5.6.0009"
 },
 "details":
 {
 "component_class": "PCI_DEVICE",
 "description": "PERC H730 Mini"
 } "notifications":
 {
  "info":
 [
 {
 "id": "Different versions.",
 "time": "2020-02-04T10:47:54.422Z",
 "message":
 {
 "args": [],
 "default_message": "Different versions.",
 "id": "Different versions."
  }
  }
 ]
 },
 "status": "NON_COMPLIANT",
 "target": {
 "version": "25.5.5.0005"
  }
  }
 "key": ""
  }
  ],
 "notifications":
 {
 "info":
 [
 {
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>]              The host is non-compliant",
 "time": "2020-02-04T10:47:54.423Z",
 "message":
 {
 "args": [],
 "default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host
is non-compliant"
 }
 }]
 },
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
 "version": "0.0.0-0"
 }
 },
 "key": "com.dell.plugin.OpenManager_HWSupportManager"
```

```
 }
 ],
```

Exécuter une vérification préalable à la correction

Commande : POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

Description : exécute des vérifications sur le cluster avant l'application de l'état souhaité sur tous les hôtes du cluster. Vérifie que tous les hôtes du cluster sont dans un état correct pour être mis à jour avec l'état souhaité.

Codes de réponse HTTP : 200. Pour obtenir la liste de tous les codes de réponse, voir Codes de réponse , page 182.

Exemple de réponse :

```
{task-id}
```

Obtenir l'état de la tâche de vérification préalable à la correction

Commande : GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

Description : renvoie des informations sur une tâche.

Codes de réponse HTTP : 200. Pour obtenir la liste de tous les codes de réponse, voir Codes de réponse , page 182.

Exemple de réponse :

```
{
 "value":
{
"parent": "",
"cancelable": true,
"end_time": "2020-02-12T18:03:59.391Z",
"description":
{
 "args": [],
 "default_message": "Task created by VMware vSphere Lifecycle Manager",
 "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
  },
 "target":
{
"id": "domain-c8",
 "type": "ClusterComputeResource"
 },
 "result":
{
"start_time": "2020-02-12T17:52:09.264Z",
"commit": "",
"end_time": "2020-02-12T18:03:59.386Z",
 "entity_results":
[
{
"host": "host-47",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 }
 {
"host": "host-41",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 },
 {
 "host": "host-22",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
  },
{
```

```
  "host": "host-16",
  "type": "HOST",
  "check_statuses": [
{
  "check":
 {
   "name":
  {
  "args": [],
  "default_message": "Host Hardware support check.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
   },
  "description":
 {
  "args": [],
  "default_message": "Checks if the hardware update can be performed.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
  },
  "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
  },
 "issues": [
 {
 "args": [],
 "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster:
R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown
Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
"id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host:
100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP,
172.20.5.5; hence Firmware update cannot continue."
 }
],
"status": "ERROR"
 }
 ],
"status": "ERROR"
 },
 {
 "host": "host-19",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
 },
 {
"host": "host-13",
 "type": "HOST",

 "check_statuses": [],
 "status": "OK"
  },
```


Corriger le cluster

Commande : POST https://{{VC IP/FQDN}/}}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=apply

```
{
 "accept_eula" : true
}
```

Description : applique l'état souhaité associé au cluster donné aux hôtes au sein du cluster.

Codes de réponse HTTP : 200. Pour obtenir la liste de tous les codes de réponse, voir Codes de réponse , page 182.

Exemple de réponse :

```
{task-id}
```

Configuration de l'indicateur de clignotement

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. Pour lancer l'assistant **Indicateur de clignotement LED du serveur**, exécutez l'une des opérations suivantes :
   a. Sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, faites un clic droit sur un hôte ou un cluster, puis accédez à **Résumé** > **Informations sur l'hôte OMIVV** > **Actions de l'hôte** > **Indicateur de clignotement LED du serveur**.
   b. Faites un clic droit sur un hôte, accédez à **Actions de l'hôte OMIVV** > **Indicateur de clignotement LED du serveur**.
2. Dans le volet de droite, cliquez sur Résumé, puis accédez à **Informations sur l'hôte OMIVV** > **Actions de l'hôte** > **Indicateur de clignotement LED du serveur**.
   La boîte de dialogue **Indicateur de clignotement LED du serveur** s'affiche.
3. Sélectionnez l'une des options suivantes :
   a. Pour allumer l'indicateur LED du serveur et définir une période, cliquez sur **Activé**.
   b. Pour éteindre l'indicateur LED du serveur, cliquez sur **Désactivé**.

Configuration du mode de verrouillage du système

Le mode de verrouillage du système est pris en charge uniquement pour les serveurs basés sur l'iDRAC9 et dotés d'une licence Enterprise. Lorsque vous activez le mode de verrouillage du système, verrouillez la configuration du système, y compris les mises à jour du firmware. Le paramètre du mode de verrouillage du système 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. De plus, iDRAC doit posséder une licence d'entreprise pour activer le mode de verrouillage.

REMARQUE : Vous ne pouvez pas modifier le mode de verrouillage du système des hôtes qui sont gérés par un profil d'identification de châssis.

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 firmware, 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.

1. Pour lancer l'assistant de configuration du mode de verrouillage du système, exécutez l'une des actions suivantes :
   a. Sur la page d'accueil d'OMIVV, cliquez sur **Menu**, sélectionnez **Hôtes et clusters**, faites un clic droit sur un hôte ou un cluster, puis accédez à **Résumé** > **Informations sur l'hôte OMIVV** > **Actions de l'hôte** > **Configurer le mode de verrouillage du système**.
   b. Faites un clic droit sur un hôte ou un cluster, accédez à **Actions de l'hôte OMIVV** > **Configurer le mode de verrouillage du système**.
   c. Sélectionnez un hôte ou un cluster, puis accédez à **Surveiller** > **Informations de l'hôte ou du cluster OMIVV** > **Firmware** > **Configurer le mode de verrouillage du système**.
2. Pour le niveau du cluster, saisissez le nom et la description de la tâche du mode de verrouillage du système. La description est facultative.
3. Pour activer le mode de verrouillage du système, cliquez sur **Activer**. Cette option limite les modifications apportées aux configurations du système (y compris les versions du firmware et du BIOS) dans le système.
4. Pour désactiver le mode de verrouillage du système, cliquez sur **Désactiver**. Cette option permet d'apporter des modifications aux configurations du système (y compris les versions du firmware et du BIOS) dans le système.

   Si vous essayez de configurer le mode de verrouillage du système pour les serveurs PowerEdge de la 13e génération ou version antérieure, un message indiquant que cette fonctionnalité n'est pas prise en charge s'affiche sur cette plate-forme.
5. Cliquez sur **OK**.
   Une tâche a été créée avec succès pour la configuration du mode de verrouillage du système. Pour vérifier l'état de la tâche, accédez à **Tâches** > **Mode de verrouillage du système**. Pour plus d'informations sur la tâches du mode de verrouillage du système, voir Tâches du mode de verrouillage du système , page 78.

18

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 à la fois le rôle opérationnel Dell et le rôle de déploiement de l'infrastructure Dell.

Intégrité des données

La communication entre OpenManage Integration pour VMware vCenter, la console d'administration et vCenter s'effectue via HTTPS. OpenManage Integration pour VMware vCenter génère un certificat qui est utilisé pour une communication de confiance entre vCenter et l'appliance. Il vérifie également le certificat du serveur vCenter avant la communication et l'enregistrement d'OpenManage Integration pour Vmware vCenter.

Une session de la console d'administration sécurisée a un délai d'inactivité de 15 minutes, et la session n'est valide que dans la fenêtre et/ou l'onglet du navigateur en cours. Si vous essayez d'ouvrir la session dans une nouvelle fenêtre ou un nouvel onglet, une erreur de sécurité s'affiche et vous demande une session valide. Cette action empêche également l'utilisateur de cliquer sur une URL malveillante susceptible d'attaquer la session de la console d'administration.

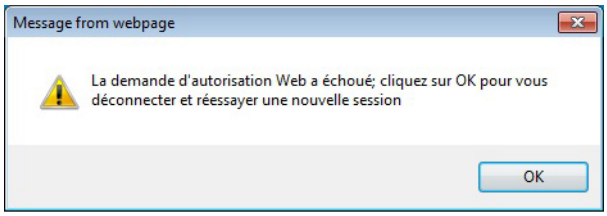


Figure 1. Message d'erreur de sécurité

Rôles, autorisation et authentification de contrôle d'accès

Pour exécuter les opérations vCenter, OpenManage Integration pour Vmware vCenter utilise la session d'utilisateur actuelle du client vSphere et les informations d'identification d'administration enregistrées pour OpenManage Integration.
OpenManage Integration pour 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 firmware, 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 25. 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 firmware
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 délivrés par ce rôle sont la configuration du profil d'identification d'hôte, l'attribution d'une identité et le déploiement.

Groupe de privilèges : Dell.Deploy-Provisioning

Configurer le profil d'identification d'hôte, Attribuer une identité, Déployer.

À propos des privilèges

Chaque action exécutée par OpenManage Integration pour 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 alarmes, par exemple, activer/désactiver les alarmes sur la page des paramètres d'événement
  - Publier les événements / alertes sur vCenter
  - Configurer les paramètres d'événement sur la page Paramètres d'événement.
  - Restaurer les alertes par défaut sur la page 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 de firmware, la tâche de configuration 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 datacenter
  - 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 de l'hôte pour publier l'événement

- Effectuer des opérations sur le journal des événements ; par exemple, obtenir le nombre d'événements, ou modifier les paramètres du journal des événements
- Enregistrer, désenregistrer et configurer les événements / alertes — Recevoir des interruptions SNMP et publier des événements

- Dell.Configuration.Firmware Update
  - Effectuer mise à jour de firmware
  - Charger les informations de référentiel du firmware et de fichier DUP sur la page de l'assistant de mise à jour de firmware
  - Interroger l'inventaire du firmware
  - Configurer les paramètres de l'espace de stockage du firmware
  - 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 la LED, éteindre la LED
  - 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 Profils de connexion
  - Planifier, mettre à jour et supprimer la planification de l'inventaire
  - Exécuter l'inventaire sur les hôtes

19

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 sur matériel vierge , page 172

Questions fréquemment posées (FAQ)

Cette section répertorie certaines questions et solutions courantes.

Le type de licence iDRAC et sa description ne s'affichent pas correctement pour les hôtes vSphere non conformes

Si un hôte n'est pas conforme lorsque CSIOR est désactivé ou n'a pas été exécuté, les informations sur la licence iDRAC s'affichent de manière incorrecte même si la licence iDRAC valide est disponible. Par conséquent, vous pouvez afficher l'hôte dans la liste des hôtes vSphere, mais lorsque vous cliquez sur l'hôte pour obtenir des détails, les informations dans **Type de licence iDRAC** sont vides et **Description de la licence iDRAC** s'affiche suit : « Votre licence doit être mise à niveau ».

Résolution : pour résoudre ce problème, activez CSIOR sur un serveur de référence.

Versions concernées : 4.0 et versions ultérieures

Le fournisseur Dell Inc ne s'affiche pas en tant que fournisseur de mise à jour d'intégrité

Lorsque vous enregistrez un serveur vCenter auprès d'OMIVV, puis que vous mettez à niveau la version du serveur vCenter, par exemple de vCenter 6.0 vers vCenter 6.5, le fournisseur Dell ne s'affiche pas dans la liste des **Fournisseurs Proactive HA**.

Résolution : vous pouvez mettre à niveau un vCenter enregistré pour les utilisateurs non-administrateurs ou les utilisateurs administrateurs. Pour effectuer la mise à niveau vers la dernière version du serveur vCenter, reportez-vous à la documentation VMware, puis exécutez l'une des opérations suivantes, le cas échéant :

- Pour les utilisateurs non-administrateurs :
  1. Attribuez des privilèges supplémentaires aux utilisateurs non-administrateurs, si nécessaire. Voir la section Privilèges requis pour les utilisateurs non administrateurs , page 15.
  2. Redémarrez l'appliance OMIVV enregistrée.
  3. Fermez la session dans le client vSphere, puis reconnectez-vous.
- Pour les utilisateurs administrateurs :
  1. Redémarrez l'appliance OMIVV enregistrée.
  2. Fermez la session dans le client vSphere, puis reconnectez-vous.

Le fournisseur Dell est maintenant répertorié dans la liste **Fournisseurs HA Proactive**.

Versions concernées : 4.0 et versions ultérieures

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 du profil d'identification d'hôte , page 39.

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 avoir enregistré vCenter avec une appliance OMIVV, plusieurs privilèges Dell sont ajoutés à la liste de privilèges vCenter. Une fois que vous avez annulé l'enregistrement de 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.

Versions concernées : 3.1 et versions ultérieures

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 ancrages 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 plus d'informations, voir https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 et https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689.

Versions concernées : 3.0 et versions ultérieures, vCenter 6.0 et versions ultérieures

Remplacement des certificats sur l'installation vCenter Windows

Pour en savoir plus, voir https://kb.vmware.com/s/article/2121689.

Remplacement des certificats sur l'appliance vCenter Server

Pour en savoir plus, voir https://kb.vmware.com/s/article/2121689.

Récupération de l'ancien certificat à partir de Managed Object Browser (MOB)

Pour en savoir plus, voir https://kb.vmware.com/s/article/2121701.

Extraction de l'empreinte de l'ancien certificat

Pour en savoir plus, voir https://kb.vmware.com/s/article/2121701.

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.

Résolution : dans la **Console d'administration**, 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 au référentiel de mise à jour**.

Que faire lorsqu'une erreur de communication Web dans le client vCenter HTML-5 s'ouvre après la modification des paramètres DNS dans OMIVV ?

Si une erreur de communication Web s'affiche dans le client vCenter HTML-5 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.
- Déconnectez-vous, puis reconnectez-vous à partir du client vSphere.

La date d'installation s'affiche sous la forme 12-31-1969 pour certains firmwares sur la page du firmware

Dans le client vSphere, la date d'installation s'affiche sous la forme 12/31/1969 pour certains firmwares sur la page du firmware d'un hôte. Si la date d'installation du firmware n'est pas disponible, l'ancienne date s'affiche.

Résolution : Si vous voyez cette ancienne date pour n'importe quel composant du firmware, considérez que la date d'installation n'est pas disponible pour ce dernier.

Versions concernées : 2.2 et versions ultérieures

Je ne vois pas l'icône OpenManage Integration dans le client HTML-5, même si l'enregistrement du plug-in auprès de vCenter a réussi

L'icône OpenManage Integration ne s'affiche pas dans le client vSphere à moins que les services du client vSphere soient redémarrés. Lorsque vous enregistrez l'appliance OpenManage Integration pour Vmware vCenter, elle est enregistrée auprès du client vSphere. Si vous annulez l'enregistrement de l'appliance, puis enregistrez à nouveau la même version ou que vous enregistrez une nouvelle version de l'appliance, l'enregistrement est effectué correctement, mais l'icône OMIVV peut ne pas s'afficher dans le client vSphere. Ceci est dû à un problème de cache de VMware. Pour résoudre le problème, assurez-vous que vous redémarrez le service client vSphere sur le vCenter Server. Ensuite, le plug-in s'affiche dans l'interface utilisateur.

Résolution : redémarrez les services clients vSphere sur le serveur vCenter.

Versions concernées : 2.2 et versions ultérieures

Pourquoi les paramètres de configuration de DNS sont-ils restaurés à leurs paramètres d'origine après le redémarrage de l'appliance si les paramètres IP de l'appliance et DNS sont remplacés par des valeurs de DHCP

Il existe un défaut connu, dans lequel les paramètres DNS affectés de manière statique sont remplacés par les valeurs de DHCP. Cela peut se produire lorsque DHCP est utilisé pour obtenir les paramètres IP et que les valeurs DNS sont attribuées de manière statique. Lorsque le bail DHCP est renouvelé ou que l'appliance est redémarrée, les paramètres DNS attribués de manière statique sont supprimés.

Résolution : attribuez les paramètres IP de manière statique lorsque les paramètres du serveur DNS sont différents de ceux du DHCP.

Versions concernées : Toutes

L'exécution de la mise à jour du firmware peut afficher un message d'erreur, le fichier de la logithèque de firmwares n'existe pas ou est non valide.

Lors de l'exécution de l'Assistant de mise à jour du firmware au niveau du cluster, un message d'erreur peut s'afficher : **le fichier de la logithèque de firmwares n'existe pas ou est non valide**. Cela peut être dû à un processus en arrière-plan quotidien qui n'a pas pu télécharger et mettre en cache le fichier de catalogue à partir de la logithèque. Cela se produit si le fichier de catalogue n'est pas accessible au moment de l'exécution du processus en arrière-plan.

Résolution : après avoir résolu les éventuels problèmes de connectivité du catalogue, vous pouvez relancer le processus en arrière-plan en modifiant l'emplacement de la logithèque de firmwares, puis en le redéfinissant sur l'emplacement d'origine. Attendez environ cinq minutes que le processus en arrière-plan se termine. Assurez-vous qu'aucun caractère @ n'est présent dans les informations d'identification fournies pour le CIFS. En outre, assurez-vous que le fichier DUP existe à l'emplacement de partage.

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 EMC PowerEdge et certaines cartes réseau Intel dotées de la version 13.5.2 du firmware. La mise à jour de certains modèles de cartes réseau Intel vers cette version du firmware échoue lorsque la mise à jour du firmware est appliquée en utilisant iDRAC avec 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 est dotée d'une version de micrologiciel autre que 13.5.2 , vous pouvez effectuer la mise à jour à l'aide d'OMIVV. Pour plus d'informations, voir 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 : Lorsque vous utilisez la mise à jour de firmware 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

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 de l'utilisateur du firmware Dell EMC 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 de 12e génération et de génération ultérieure, 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.

Quels sont les paramètres de port requis pour OMIVV ?

Utilisez les paramètres de port suivants pour OMIVV :

Tableau 26. Appliance virtuelle

Numéro de port	Protocoles	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.
68	DHCP	UDP	Aucun	Entrant	Serveur DHCP vers appliance OMIVV	Configuration du réseau dynamique	Pour obtenir des informations détaillées sur le réseau, telles que l'adresse IP, la passerelle, le masque de réseau et le DNS.

Tableau 26. Appliance virtuelle (suite)

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
69	TFTP	UDP	128 bits	Sortant	OMIVV pour iDRAC	Protocole simplifié de transfert de fichiers	Permet de mettre à jour le serveur sans système d'exploitation vers la version de firmware minimale prise en charge.
123	NTP	UDP	Aucun	Entrant	NTP vers appliance OMIVV	Synchronisation de l'heure	Pour synchroniser avec un fuseau horaire spécifique.
162	Agent SNMP	UDP	Aucun	Entrant	iDRAC ou CMC ou OME-Modular vers l'appliance OMIVV	Agent SNMP (serveur)	Pour recevoir des traps SNMP à partir de nœuds gérés.
80/443	HTTP/ HTTPS	TCP	Aucun	Sortant	Appliance OMIVV vers Internet	Accès Dell Online Data	Connectivité à la garantie en ligne (Internet), au micrologiciel et aux dernières informations RPM.
443	HTTPS	TCP	128 bits	Entrant	Interface utilisateur OMIVV vers appliance OMIVV	Serveur HTTPS	Services Web offerts par OMIVV. Ces services Web sont consommés par le client vSphere et le portail d'administration Dell.
443	HTTPS	TCP	128 bits	Entrant	Serveur ESXi vers appliance OMIVV	Serveur HTTPS	Utilisé dans le flux de déploiement du système d'exploitation afin que les scripts post-installation communiquent avec l'appliance OMIVV.
443	HTTPS	TCP	128 bits	Entrant	iDRAC vers appliance OMIVV	Découverte automatique	Serveur de configuration utilisé pour la détection automatique de nœuds gérés.
443	WS-MAN	TCP	128 bits	Entrée/ Sortie	Appliance OMIVV vers/depuis iDRAC	Communication iDRAC	Communications iDRAC ou CMC ou OME-Modular utilisées pour gérer et surveiller les nœuds gérés.
445/139	SMB	TCP	128 bits	Sortant	Appliance OMIVV vers CIFS	Communication CIFS	Pour communiquer avec le partage Windows.
2049/111	NFS	UDP/ TCP	Aucun	Entrée/ Sortie	Appliance OMIVV vers NFS	Partage public	Partage public NFS exposé par l'appliance OMIVV vers les nœuds gérés et utilisé dans la mise à jour du micrologiciel et les flux de déploiement du système d'exploitation.
4001 à 4004	NFS	UDP/ TCP	Aucun	Entrée/ Sortie	Appliance OMIVV vers NFS	Partage public	Ces ports doivent être maintenus ouverts pour exécuter les services statd, quotd, lockd et mountd par les protocoles V2 et V3 du serveur NFS.
Défini par l'utilisateur	N'importe lequel	UDP/ TCP	Aucun	Sortant	Appliance OMIVV vers serveur proxy	Proxy	Pour communiquer avec le serveur proxy.

Tableau 27. Nœuds gérés (ESXi)

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
162	SNMP	UDP	Aucun	Sortant	ESXi vers appliance OMIVV	Événements matériels	Traps SNMP asynchrones envoyés par ESXi. Ce port doit s'ouvrir à partir d'ESXi.

Tableau 27. Nœuds gérés (ESXi) (suite)

Numéro de port	Protocoles	Type de port	Niveau de cryptage maximum	Direction	Destination	Utilisation	Description
443	WS-MAN	TCP	128 bits	Entrant	Appliance OMIVV vers ESXi	Communication iDRAC	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.
443	HTTPS	TCP	128 bits	Entrant	Appliance OMIVV vers ESXi	Serveur HTTPS	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.

Pour plus d'informations sur l'iDRAC et pour obtenir des informations sur le port CMC, reportez-vous au *Guide de l'utilisateur de Integrated Dell Remote Access Controller* et au *Guide de l'utilisateur du Chassis Management Controller Dell* disponibles à l'adresse **https://www.dell.com/support**.

Pour plus d'informations sur les ports OME-Modular, voir le *Guide de l'utilisateur de Dell EMC OME-Modular* disponible à l'adresse **https://www.dell.com/support**.

REMARQUE : Pour les serveurs basés sur iDRAC9, l'iDRAC monte le NFS via TCP sur le port 2049. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.

Le mot de passe utilisé pour la détection sans système d'exploitation ne change pas pour l'utilisateur après l'application réussie 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 profil système (configuration du matériel) 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**.

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 6.0 et les versions ultérieures.

Quand j'ai essayé d'utiliser le mode de verrouillage, celui-ci a échoué

Quand j'ai ajouté un hôte au profil d'informations d'identification 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 que vous retirez un hôte du mode verrouillage, vous devez attendre 30 minutes avant d'exécuter l'opération suivante dans OMIVV.

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 accessible par l'appliance virtuelle.
3. Veillez à sélectionner les cartes réseau de gestion en fonction de la connectivité réseau à OMIVV.
4. 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.
5. Assurez-vous qu'au moins un disque virtuel, IDSDM ou BOSS est détecté par le système.

Les systèmes détectés automatiquement s'affichent sans information de modèle dans l'assistant Déploiement

Cela indique généralement que la version du firmware 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 qu'iDRAC peut 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 OMIVV de vCenter

1. Rendez-vous sur vSphere Client et décochez la case par rapport au fournisseur de Dell pour tous les clusters activés pour Proactive HA.
2. Allez à **https://<vcenter_AdresseIPserveur>/mob**
3. Saisissez les informations d'identification de l'administrateur Vmware vCenter .
4. Cliquez sur **Accueil** > **Contenu** > **Gestionnaire de mise à jour d'intégrité**.
5. Cliquez sur **Liste de fournisseur de requêtes** > **Appeler une méthode**.
6. Copiez la valeur de la chaîne ID de fournisseur et fermez la fenêtre.
7. Cliquez sur **Désenregistrer le fournisseur de mise à jour de l'intégrité** et saisissez la valeur de chaîne d'ID de fournisseur copiée.
8. Cliquez sur **Appeler une méthode**.
9. Accédez à **Accueil** > **Contenu**
10. Cliquez sur **Gestionnaire d'extension**.
11. Cliquez sur **Désenregistrer l'extension**.
12. Entrez la clé d'extension pour désenregistrer com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient, puis cliquez sur **Appeler une méthode**.
13. Dans le client vSphere, mettez hors tension l'appliance OMIVV puis supprimez-la. La touche de désenregistrement doit être destinée au client vSphere.
14. Dans vCenter, effacez les entrées de gravité et redémarrez le service vCenter.

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 n'est pas visible dans la fenêtre SAUVEGARDER MAINTENANT. Faites défiler la page vers le bas pour saisir le mot de passe de cryptage.

Que dois-je faire en cas d'échec d'une mise à jour de micrologiciel ?

Vérifiez les journaux de l'appliance OMIVV 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. 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 pour 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 d'informations d'identification d'hôte 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 :
   - iDRAC7 : sélectionnez **Paramètres de l'iDRAC** > **Onglet Utilisateurs**.
   - iDRAC8 : sélectionnez **Paramètres de l'iDRAC** > **Onglet Utilisateurs**.
   - iDRAC9 : sélectionnez **Paramètres de l'iDRAC** > **Onglet Utilisateurs**.

   Pour iDRAC 7 et 8 :

   a. Pour modifier les paramètres, dans la colonne ID d'utilisateur, cliquez sur le lien correspondant à l'utilisateur admin (root).
   b. Cliquez sur **Configurer l'utilisateur**, puis cliquez sur **Suivant**.
   c. 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**.

   Pour iDRAC 9 :

   a. Sélectionnez l'utilisateur **root** et cliquez sur **Activer**.

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.

Un serveur peut apparaître comme non conforme avec l'état CSIOR, « Inconnu »

Résolution : un état CSIOR inconnu indique un iDRAC sans réponse sur l'hôte. Une réinitialisation manuelle de l'iDRAC sur l'hôte résout ce problème.

Versions concernées : Toutes

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. 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.

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 l'interface utilisateur d'OMIVV, onglet **Paramètres**, modifiez manuellement les paramètres d'**Événements et alarmes**.

Échec du déploiement du système d'exploitation lorsqu'un NPAR est activé sur un nœud cible et désactivé sur le profil système

Le déploiement du système d'exploitation 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 Déploiement.

Versions concernées : 4.1 et versions ultérieures

La version disponible de l'appliance OMIVV 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 et ultérieur

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, l’application du profil matériel échoue en raison d’une erreur iDRAC

Lors du déploiement, OMIVV tente de créer une tâche de mise à jour de configuration dans iDRAC. Cependant, la création de la tâche peut échouer et affiche un message indiquant qu’une tâche de configuration est déjà créée.

Résolution : effacez les entrées obsolètes et relancez le déploiement. Connectez-vous à iDRAC pour effacer les tâches.

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 le logement 1 d’un châssis FX2s peut uniquement être appliqué sur un autre serveur FC640 résidant dans le logement 1 d’un autre châssis FX2s.

La détection de dérive montre une non-conformité pour les serveurs modulaires qui ont une carte PCIe dans le châssis FX

Les profils système recherchent une instance exacte (FQDD) lors de la comparaison avec la ligne de base, ce qui fonctionne avec succès sur les serveurs rack (identiques), mais peut avoir quelques restrictions sur les serveurs modulaires. Par exemple, dans FC640, le profil système (ligne de base) créé à partir d'un serveur modulaire affiche une dérive par rapport à d'autres serveurs modulaires dans le même châssis FX en raison de mauvaises correspondances FQDD.

Versions concernées : 4.1 et versions ultérieures

Résolution : lors de la création du profil système, effacez les FQDD qui ne sont pas communs avec d'autres serveurs.

Impossible de déployer un système d'exploitation sur des serveurs PowerEdge lorsque l'iDRAC ne remplit pas l'adresse MAC de la carte réseau sélectionnée

Le déploiement du système d'exploitation échoue sur les serveurs PowerEdge lorsque l'iDRAC ne remplit pas l'adresse MAC pour le port NIC sélectionné.

Résolution : mettre à jour le micrologiciel NIC et le micrologiciel iDRAC vers la dernière version et s'assurer que l'adresse MAC est renseignée sur le port NIC.

Versions concernées : 4.3 et versions ultérieures

Lors de la création d'un profil d'informations d'identification pour l'hôte ayant ESXi 6.5 U1, le numéro de série de l'hôte n'est pas affiché sur la page Sélectionner les hôtes

Lorsque l'OMIVV interroge vCenter pour le numéro de service ESXi, vCenter ne peut pas renvoyer le numéro de service parce que la valeur du numéro de service est nulle.

Résolution : mettre à jour la version ESXi vers ESXi 6.5 U2 ou ESXi 6.7 U1.

Versions concernées : 4.3 et versions ultérieures

L'icône Dell ne s'affiche pas après la sauvegarde et la restauration d'une version d'OMIVV précédente vers une version d'OMIVV ultérieure

Après la sauvegarde et la restauration d'une version antérieure d'OMIVV vers une version ultérieure d'OMIVV, les problèmes suivants sont observés :

- Le logo Dell EMC ne s'affiche pas sur vCenter.
- L'erreur 2000000
- L'erreur 3001

  Résolution :

  - Redémarrez le client vSphere sur le serveur vCenter.
  - Si le problème persiste :
    - Pour l'appliance VMware vCenter Server, accédez à `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` et pour la version Windows de vCenter, accédez au dossier `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` dans l'appliance vCenter, puis vérifiez si les anciennes données sont présentes, par exemple : com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
    - Supprimez manuellement le dossier correspondant à la version antérieure d'OMIVV.

Lors de la mise à niveau ou de la rétrogradation de certaines versions du firmware iDRAC utilisant OMIVV, et même lorsque la mise à jour du firmware a réussi, OMIVV peut indiquer que la tâche a échoué.

Au cours de la mise à jour du micrologiciel, lorsque vous rétrogradez ou mettez à niveau les versions de l'iDRAC telles que les versions 3.20.20.20, 3.21.21.21 et 3.21.21.22, l'état de la tâche est indiqué comme ayant échoué, même lorsque la tâche a été exécutée avec succès.

Résolution : actualisez l'inventaire après l'échec de la tâche et exécutez à nouveau la tâche pour les autres composants.

Version concernée : 4.3

La configuration du mode System Lockdown à un niveau cluster affiche parfois le message « Aucun hôte sous le cluster ne dispose d'inventaire réussi »

La configuration du mode System Lockdown à un niveau cluster affiche parfois le message « Aucun hôte sous le cluster ne dispose d'inventaire réussi ». Ce message s'affiche même lorsque le cluster a correctement inventorié les serveurs basés sur l'iDRAC9 qui sont gérés par l'OMIVV. Pour obtenir la liste des serveurs basés sur iDRAC9, reportez-vous à la matrice de compatibilité.

Résolution : redémarrez le vCenter.

Pour redémarrer le vCenter, procédez comme suit :

1. Ouvrez une session sur le client vSphere à l'aide d'un compte administrateur vCenter à authentification unique.
2. Accédez à **Administration** > **Déploiement** > **Déploiement** > **Configuration système**.
3. Cliquez sur **Nœuds**, sélectionnez le nœud de l'appliance vCenter Server, puis cliquez sur l'onglet **Objets liés**.
4. Redémarrez le nœud vCenter.

Après la mise à niveau RPM de l'appliance OMIVV, plusieurs entrées de journaux sont parfois visibles dans les tâches récentes de vCenter

Après la mise à niveau RPM, plusieurs entrées apparaissent parfois dans les journaux affichés dans les tâches récentes de vCenter

Résolution : redémarrez les services vCenter.

Version concernée : 4.3

Après l'enregistrement de vCenter, le logo Dell EMC d'OMIVV ne s'affiche pas sur la page d'accueil de VMware

Description : il est possible que le logo Dell EMC d'OMIVV ne s'affiche pas sur la page d'**Accueil** de VMware, car VMware vCenter valide le plug-in juste après l'enregistrement.

Résolution : effectuez les opérations suivantes :

1. Actualisez le navigateur, effacez le cache du navigateur ou redémarrez les services client pour vSphere Client (HTML-5).
2. Fermez la session dans le client vSphere, puis reconnectez-vous.

Version concernée : 5.0

Les serveurs PowerEdge 11G non conformes sont conservés dans l'inventaire OMIVV après la sauvegarde et la restauration

Après avoir effectué les opérations de sauvegarde et de restauration dans OMIVV, les hôtes 11G non conformes et non inventoriés restent associés au profil d'identification d'hôte. Toutefois, si vous tentez de corriger la conformité de la configuration et d'exécuter un nouvel inventaire, la tâche échoue sur les serveurs 11G non pris en charge.

Résolution : les serveurs de 11e génération ne sont pas pris en charge avec OMIVV 5.0. Supprimez manuellement les hôtes de 11e génération non pris en charge à partir du profil d'informations d'identification d'hôte.

Version concernée : 5.0

Impossible de lancer vCenter depuis le client Flex après la mise à niveau de l'appliance OMIVV

Résolution : reportez-vous à l'article de la base de connaissances VMware : https://KB.VMware.com/s/article/54751.

Version concernée : 5.0

Lors de l'ajout ou de la suppression de cartes réseau dans OMIVV, les cartes réseau existantes disparaissent de la console OMIVV

Parfois, lorsque vous ajoutez ou supprimez une carte réseau de l'appliance OMIVV à l'aide du client vSphere, les cartes réseau existantes disparaissent de la console OMIVV.

Contournement : Exécutez l'une des tâches suivantes :

1. a. Supprimer tous les adaptateurs de travail de l'utilitaire de la console de terminal.
   b. Arrêter l'appliance.
   c. Retirer les cartes réseau de l'appliance.
   d. Redémarrer l'appliance OMIVV.
   e. Arrêter l'appliance.
   f. Ajouter la ou les cartes réseau requises et les configurer.
   g. Redémarrer l'appliance.
2. a. Sauvegarder OMIVV depuis le portail d'administration.
   b. Créer une appliance OMIVV.
   c. Arrêter l'appliance.
   d. Ajouter la ou les cartes réseau requises et les configurer.
   e. Redémarrer l'appliance.
   f. Restaurer les données sauvegardées les plus récentes.

Version concernée : OMIVV 5.0

Après l'ajout ou le retrait de la deuxième carte réseau, la page Configuration réseau affiche trois cartes réseau

Une fois que vous avez ajouté ou supprimé une carte réseau à partir de l'appliance OMIVV à l'aide du client vSphere, et lorsque vous avez démarré l'appliance OMIVV et que vous vous êtes connecté à la console de terminal OMIVV, la page **Configuration réseau** affiche parfois un nombre de cartes réseau incohérent.

Résolution : utilisez l'adresse MAC pour comparer et configurer la bonne carte réseau et utilisez le bouton **–** pour supprimer les cartes réseau en trop.

Version concernée : 5.0

Un serveur dont l'état est inconnu dans la version antérieure n'est pas répertorié sur la page serveurs sans système d'exploitation après la sauvegarde et la restauration vers la version OMIVV la plus récente

Après la restauration d'une sauvegarde à partir de versions antérieures, les serveurs non pris en charge (11G et versions antérieures) sont supprimés de l'inventaire des serveurs sans système d'exploitation. Les serveurs dont la génération n'a pas été identifiée par la version antérieure avant la suppression de la sauvegarde sont également supprimés.

Résolution : relancez la détection du serveur. Si le serveur manquant est pris en charge, il est répertorié dans l'inventaire des périphériques sans système d'exploitation.

Version concernée : 5.0

Après le déploiement du SE, OMIVV n'a pas pu ajouter l'hôte ESXi à vCenter, n'a pas pu ajouter un profil d'hôte ou le passage en mode maintenance de l'hôte échoue

Après le déploiement du SE, OMIVV interroge vCenter pour exécuter les actions de l'hôte (ajouter l'hôte, ajouter un profil d'hôte ou passer en mode maintenance). Si la requête ne reçoit pas de réponse dans les deux minutes, l'action en question sur vCenter arrive à expiration, et un message s'affiche dans l'historique des tâches indiquant que la communication a échoué. Toutefois, dans certains cas, les opérations de requête vCenter aboutissent.

Résolution : retrouvez l'adresse IP de l'hôte à partir de l'historique des tâches et ajoutez-la manuellement.

L'état de la licence iDRAC s'affiche comme étant conforme sur la page Gestion de la conformité lorsque l'adresse IP iDRAC n'est pas accessible

Après avoir effectué l'inventaire périodique, si iDRAC n'est pas accessible, l'état de la licence iDRAC s'affiche comme étant conforme sur la page Gestion de la conformité.

Résolution : assurez-vous qu'iDRAC est accessible, puis exécutez à nouveau l'inventaire pour obtenir les détails de la licence iDRAC.

L'hôte ESXi est déconnecté ou ne répond pas après un déploiement réussi du SE à l'aide d'OMIVV.

L'hôte ESXi ne parvient pas à envoyer des paquets de pulsations à vCenter car son DNS n'est pas correctement configuré pour rechercher le FQDN de vCenter.

Résolution : exécutez les tâches suivantes :

1. Retirez les hôtes ESXi de l'inventaire vCenter.
2. Ajoutez l'hôte dans vCenter à l'aide de l'assistant **Ajouter un hôte**.
3. Créez un profil d'identification d'hôte et exécutez l'inventaire.

La tâche de déploiement expire lorsque la carte d'interface réseau (NIC) d'OMIVV n'est pas connectée au réseau de l'hôte ESXi

Le déploiement du système d'exploitation dépend de la carte NIC sélectionnée. Si la carte NIC sélectionnée n'est pas la bonne, la tâche OSD expire.

Résolution : sélectionnez la bonne « Carte NIC de l'appliance connectée à l'hôte » à partir de la page Configurer les paramètres de l'hôte de l'Assistant Déploiement. Ceci est requis par OMIVV pour pouvoir atteindre le réseau ESXi au cours du processus d'installation du système d'exploitation.

La tâche de garantie ne s'exécute pas pour certains hôtes

Dans un environnement PSC comportant plusieurs vCenters, si vous ajoutez un hôte à l'aide de FQDN à un vCenter et une adresse IP à un autre vCenter, la tâche de garantie ne s'exécute que pour une seule instance de l'hôte.

Résolution : supprimez l'instance d'hôte déconnectée du profil d'identification d'hôte et exécutez la tâche d'inventaire et de garantie.

Version concernée : 5.0

L'initialisation de Proactive HA ne se produit pas après l'exécution de la sauvegarde et de la restauration

Lorsque vous restaurez OMIVV à partir de la version précédente enregistrée auprès du client vSphere, le fournisseur Dell est déconnecté pour les clusters compatibles Proactive HA.

Résolution : désactivez et activez Proactive HA pour les clusters.

Version concernée : 5.0

La page OMIVV affiche des erreurs de session non valide, d'expiration de délai d'attente ou 2 millions dans le navigateur Firefox

Si la page OMIVV est inactive pendant un certain temps (5 à 10 minutes), des erreurs de session non valide, d'expiration de délai d'attente ou 2 millions s'affichent.

Résolution : actualisez le navigateur. `Si le problème persiste, déconnectez-vous, puis connectez-vous à partir de vCenter.`

Pour afficher les données correctes dans OMIVV, assurez-vous que vous avez effectué la tâche répertoriée dans la résolution.

Version concernée : 5.0

Dans vCenter, le volet Tâches récentes n'affiche pas la colonne Détails pour certaines notifications de tâche OMIVV

Résolution : pour voir les notifications de tâches, dans vCenter, accédez à la **Console des tâches** de vCenter.

Version concernée : 5.0

Lors de l'utilisation de vCenter 6.5 U2, un message d'erreur 2000002 peut s'afficher sur toutes les pages d'OMIVV

Solution : utilisez le dernier correctif de VMware pour la version 6.5 U2 ou pour migrer vers la version 6.5 U3 et versions ultérieures.

Version concernée : 5.1

L'erreur 2000002 s'affiche sur toutes les pages d'OMIVV après la mise à niveau ou la sauvegarde du RPM et la restauration d'OMIVV vers une version ultérieure

Avant d'enregistrer la version actuelle, si vous disposez d'une version antérieure d'OMIVV dans le serveur vCenter, une exception d'établissement de liaison SSL rend la nouvelle version d'OMIVV inaccessible jusqu'à ce que vCenter actualise les nouvelles données du plug-in. Cela est dû au fait que vCenter contient les données de la version antérieure d'OMIVV, qui gère le trafic SSL différemment.

Résolution :

- Redémarrez le client vSphere sur le serveur vCenter.
- Si le problème persiste :
  - Pour l'appliance VMware vCenter Server, accédez à `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` et pour la version Windows de vCenter, accédez au dossier `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` dans l'appliance vCenter, puis vérifiez si les anciennes données sont présentes, par exemple : com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
  - Supprimez manuellement le dossier correspondant à la version antérieure d'OMIVV.
  - Redémarrez les services client vSphere pour vSphere Client (HTML5)

Versions concernées : 5.0 et versions ultérieures

Parfois, OMIVV prend beaucoup de temps à désenregistrer vCenter

Lorsque vous désenregistrez un vCenter doté d'un grand nombre d'hôtes (plus de 300), OMIVV reste à l'état de chargement pendant longtemps.

Résolution : actualisez le navigateur.

Si le désenregistrement du vCenter échoue, désenregistrez à nouveau le vCenter.

Version concernée : 5.1

Après la mise à jour du certificat OMIVV, le message d'erreur « Échec de la connexion de l'appliance OMIVV. Le certificat SSL n'est pas valide » s'affiche.

Résolution : redémarrez le service client vCenter.

Versions concernées : Toutes

Échec de la tâche de déploiement dans OMIVV

La tâche de déploiement échoue, car LifeCycle Controller est occupé à exécuter les tâches en attente ou en cours d'exécution.

Résolution : effectuez les opérations suivantes :

1. Effacer la file d'attente des tâches de l'iDRAC dans l'iDRAC [en option]
2. Réinitialisation de l'iDRAC
3. Réexécutez la tâche de déploiement.

Versions concernées : toutes

Échec du test de connexion et de l'inventaire dans OMIVV après la modification du mot de passe vCenter

Pour ESXi version 6.7 et les versions supérieures, OMIVV récupère une adresse IP de l'iDRAC de l'hôte ESXi à l'aide du protocole IPMI (Intelligent Platform Management Interface). Cette opération ne dépend pas de WBEM.

Si OMIVV ne parvient pas à récupérer une adresse IP de l'iDRAC pour quelque raison que ce soit, OMIVV tente le protocole CIM (Common Information Model) en tant qu'action de secours, qui dépend de l'état WBEM. Si le mot de passe utilisateur de vCenter utilisé pour l'enregistrement est modifié, vous pouvez observer un problème lié à WBEM lors de l'exécution du test de connexion et de l'inventaire.

Résolution : après avoir modifié le mot de passe vCenter, modifiez les informations d'identification vCenter dans la console d'administration OMIVV, avant d'effectuer une opération dans vCenter. Pour en savoir plus sur la modification des informations d'identification, voir Modification des informations d'identification pour la connexion à vCenter , page 16.

Versions concernées : Toutes

L'instance OMIVV n'est pas supprimée de vCenter après la réinitialisation de l'appliance OMIVV sur les paramètres d'usine

Ce problème se produit lorsque vous réinitialisez l'appliance sur les paramètres d'usine. L'entrée de l'appliance OMIVV reste dans le dossier `vsphere-client-serenity` de vCenter, ce qui empêche l'enregistrement de vCenter après la réinitialisation des paramètres d'usine.

Résolution : retirez l'entrée OMIVV de vCenter. Pour plus d'informations, voir Comment puis-je forcer la suppression de l'appliance OMIVV de vCenter , page 162.

Versions concernées : Toutes

OMIVV affiche uniquement les attributs du BIOS et de l'iDRAC sur la page Paramètres de profil du profil du système

Solution : mettez à niveau Google Chrome vers la version la plus récente.

Version concernée : 5.2

Le déploiement du système d'exploitation s'est terminé avec une erreur inconnue

Ce problème se produit lorsque vous effectuez le déploiement du système d'exploitation avec un autre utilisateur que celui utilisé pour découvrir le serveur. Le message d'erreur sur la page **Journaux** d'OMIVV affiche l'erreur Catégorie non trouvée.

Solution : N/A, ce problème n'affecte pas les fonctionnalités OMIVV.

Version concernée : 5.2

Échec de la mise à jour de firmware du contrôleur CMC (Chassis Management Controller) dans le châssis FX2

OMIVV vous permet de mettre à jour le firmware du CMC du châssis FX2 via l'iDRAC du serveur. La mise à jour de firmware du CMC échoue si l'option **Autoriser les mises à jour du CMC via le système d'exploitation et Lifecycle Controller** est désactivée dans l'iDRAC.

Résolution : effectuez les opérations suivantes dans l'iDRAC.

1. Accédez à **Paramètres** > **Mise à jour et restauration**.
2. Configurez l'option **Autoriser les mises à jour du CMC via le système d'exploitation et Lifecycle Controller** sur **Activé**.

Version concernée : 5.2

Échec du déploiement du profil ISO dans OMIVV

La tâche de déploiement de profil ISO planifiée dans une version antérieure d'OMIVV n'est pas valide dans la dernière version d'OMIVV.

Solution : annulez la tâche planifiée et créez une tâche de déploiement selon vos besoins.

La tâche de déploiement échoue si la tâche planifiée n'est pas annulée. Dans ce cas, découvrez le serveur en tant que matériel vierge et créez une tâche de déploiement de profil ISO.

Version concernée : 5.2

Problèmes de déploiement de serveurs sur matériel vierge

Cette section traite des problème 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 firmware 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.
- Exécutez la configuration du BIOS 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 détection automatique sur un système récemment acheté

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 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
```

A

Attributs spécifiques au système

iDRAC

Tableau 28. 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
Adresse :	Adresse IPv4	Informations statiques sur IPv4
Masque réseau	Masque réseau	Informations statiques sur IPv4
Passerelle	Passerelle	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 29. 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	Initiator IP Address (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

Tableau 29. Attributs spécifiques au système pour le BIOS (suite)

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
IscsiDev1Con1TargetName	Nom de la cible	Paramètres de la connexion 1
IscsiDev1Con2Gateway	Passerelle de l'initiateur	Paramètres de la connexion 1
IscsiDev1Con2Ip	Initiator IP Address (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
iscsiInitiatorName	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 30. 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 31. 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	CHAP Secret (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
IscsiInitiatorChapId	ID CHAP	Paramètres de l'initiateur iSCSI

Tableau 31. Attributs spécifiques au système pour CNA (suite)

Nom de l'attribut	Nom d'affichage de l'attribut	Nom d'affichage de groupe
IscsiInitiatorChapPwd	CHAP Secret (Secret CHAP)	Paramètres de l'initiateur iSCSI
IscsiInitiatorGateway	Passerelle par défaut	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpAddr	Adresse IP	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv4Addr	Adresse IPv4	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv4Gateway	Passerelle IPv4 par défaut	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv4PrimDns	DNS principal IPv4	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv4SecDns	DNS secondaire IPv4	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv6Addr	Adresse IPv6	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv6Gateway	Passerelle IPv6 par défaut	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv6PrimDns	DNS principal IPv6	Paramètres de l'initiateur iSCSI
IscsiInitiatorIpv6SecDns	DNS secondaire IPv6	Paramètres de l'initiateur iSCSI
iscsiInitiatorName	Nom iSCSI	Paramètres de l'initiateur iSCSI
IscsiInitiatorPrimDns	DNS principal	Paramètres de l'initiateur iSCSI
IscsiInitiatorSecDns	DNS secondaire	Paramètres de l'initiateur iSCSI
IscsiInitiatorSubnet	Masque de sous-réseau	Paramètres de l'initiateur iSCSI
IscsiInitiatorSubnetPrefix	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	CHAP Secret (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 32. 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

B

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*

C

Attributs de personnalisation

Tableau 33. 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	RAIDPDState	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.
PCIeSSD	PCIeSSDSecureErase	Toujours désactivé

D

Matrice de comparaison de la version du composant avec la version de ligne de base

Tableau 34. 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	Les attributs matériels du composant ne correspondent 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	Le composant matériel est disponible dans la ligne de base associée, mais le composant ou l'attribut n'est pas disponible dans l'hôte.	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	La version du composant de firmware correspond à la ligne de base associée.	Conforme
	Disponible	Disponible	La version du composant de firmware ne correspond pas à la ligne de base associée.	Non conforme
	Non disponible	Disponible	La version du composant de firmware n'est pas disponible dans la ligne de base associée, mais le composant est disponible dans l'hôte. L'état de comparaison n'est pas calculé et est ignoré.	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	La version du composant du pilote correspond à la ligne de base associée.	Conforme

Tableau 34. Matrice de comparaison de la version du composant avec la version de ligne de base (suite)

Type de dérive				
	Disponible	Disponible	La version du composant du 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 du pilote est disponible dans la ligne de base associée, mais le composant n'est pas disponible dans l'hôte.	Non conforme
	Non disponible	Non disponible	L'état de comparaison n'est pas calculé et est ignoré.	Conforme

E

Codes de réponse

Tableau 35. Codes de réponse

Codes de réponse	Description
200	Génération/retour réussi(e) des informations de la tâche ou de la liste de tâches.
202	Lancement réussi d'une tâche.
400	Demande incorrecte
401	Demande non autorisée
404	Introuvable
409	Conflit
500	Erreur de serveur interne
503	Service non disponible