# OpenManage Integration pour VMware vCenter version 5.3

## Guide de configuration de la sécurité

Mars 2021
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

# Figures

# Tableaux

# 1

# PRÉFACE

En vue d'améliorer sa ligne de produits, Dell EMC publie régulièrement des révisions de son matériel et de ses logiciels. Il se peut que certaines fonctionnalités décrites dans le présent document ne soient pas prises en charge par l'ensemble des versions logicielles ou matérielles actuellement utilisées. Les notes de mise à jour des produits fournissent les toutes dernières informations concernant les fonctionnalités produit.

Si un produit ne fonctionne pas correctement ou ne fonctionne pas comme indiqué dans ce document, contactez un professionnel du support technique Dell EMC. Ce document était précis au moment de sa publication. Afin de vérifier que vous utilisez bien la dernière version de ce document, rendez-vous sur **https://www.dell.com/support**.

## Objectif

Ce document contient des informations concernant les fonctionnalités de sécurité d'OpenManage Integration pour VMware vCenter (OMIVV).

## Public

Ce document s'adresse aux personnes chargées de la gestion de la sécurité d'OMIVV.

## Historique des révisions

Le tableau ci-dessous présente l'historique des révisions de ce document.

**Tableau 1. Historique des révisions**

| Révision | Date | Description |
|---|---|---|
| A00_5.2,0 | Octobre 2020 | Version originale du Guide de configuration de la sécurité d'OpenManage Integration pour VMware v Center version 5.2. |
| A00_5.3,0 | Mars 2021 | Ajout d'informations relatives aux API RESTful dans les rubriques d'authentification et de sécurité des données. |

## Documentation connexe

La documentation complète relative à OMIVV est disponible sur **https://www.dell.com/support**. Cliquez sur **Parcourir tous les produits**, puis sur **Logiciel** > **Solutions de virtualisation**. Cliquez sur **OpenManage Integration pour VMware vCenter** pour accéder aux documents suivants :

- *Guide de l'utilisateur d'OpenManage Integration pour VMware vCenter version 5.3*
- *Notes de mise à jour d'OpenManage Integration pour VMware vCenter version 5.3*
- *Matrice de compatibilité d'OpenManage Integration pour VMware vCenter version 5.3*
- *Guide API d'OpenManage Integration pour Vmware vCenter version 5.3*
- *Guide d'installation d'OpenManage Integration pour Vmware vCenter version 5.3*

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

# 2

# Termes utilisés dans ce document

**Tableau 2. Termes utilisés dans ce document**

| Terminologie | Description |
|---|---|
| OMIVV | OpenManage Integration pour VMware vCenter |
| OVF | Format de virtualisation ouvert |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| NFS | Network File System |
| CIFS | Common Internet File System |
| OM MP | OpenManage Management Pack pour vRealize Operations |
| CMC | Chassis Management Controller (M1000e, FX, VRTX) |
| OME-M | OpenManage Modular Edition (MX7000) |
| iDRAC | Integrated Dell Remote Access Controller |
| SNMP | Simple Network Management Protocol |
| VM | Machine virtuelle |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| PEM | Privacy-Enhanced Mail |
| RPM | Red Hat Package Manager |
| SE | Système d'exploitation |

# 3

# Modèles de déploiement

Vous pouvez déployer OpenManage Integration pour VMware vCenter (OMIVV) en tant qu'OVF dans l'environnement VMware vCenter.

**Sujets :**



## Déploiement de OVF (Open Virtualization Format)

Si vous disposez de l'environnement de machine virtuelle VMware vSphere, le déploiement d'OMIVV en tant qu'OVF (Open Virtualization Format) est recommandé.

Le modèle de déploiement OVF comprend une offre groupée préconfigurée avec le logiciel OMIVV et le système d'exploitation Linux sur lequel s'exécute le logiciel OMIVV.

L'environnement OVF inclut également un pare-feu préconfiguré réglé sur les exigences de communication OMIVV avec les systèmes surveillés.

Le déploiement OVF se réalise à l'aide d'un fichier de modèle OVF. Pour plus d'informations sur le déploiement d'OMIVV en tant qu'OVF, consultez le *Guide d'installation d'OpenManage Integration pour VMware vCenter 5.3* disponible sur **https://www.dell.com/support**.

## Profils de sécurité

OMIVV dispose d'un profil de sécurité par défaut pour l'accès HTTP sécurisé. Il est vivement recommandé de remplacer les certificats signés par l'autorité de certification (AC) pour les environnements de sécurité plus puissants.

4

# Sécurité des produits et des sous-systèmes

**Sujets :**



## Mappage des contrôles de sécurité

OMIVV effectue le déploiement, l'inventaire et la mise à jour des serveurs PowerEdge à l'aide d'iDRAC et reçoit des traps SNMP de la part d'iDRAC.

L'interface utilisateur d'OMIVV est la page Web d'administration de l'appliance. L'interface utilisateur du plug-in OMIVV fonctionne à partir du client VMware vCenter et fournit des fonctionnalités de surveillance et de gestion du matériel de l'hôte.

Toutes les informations d'identification du système sont stockées dans le stockage sécurisé OMIVV.

La figure suivante illustre le mappage des contrôles de sécurité OMIVV :

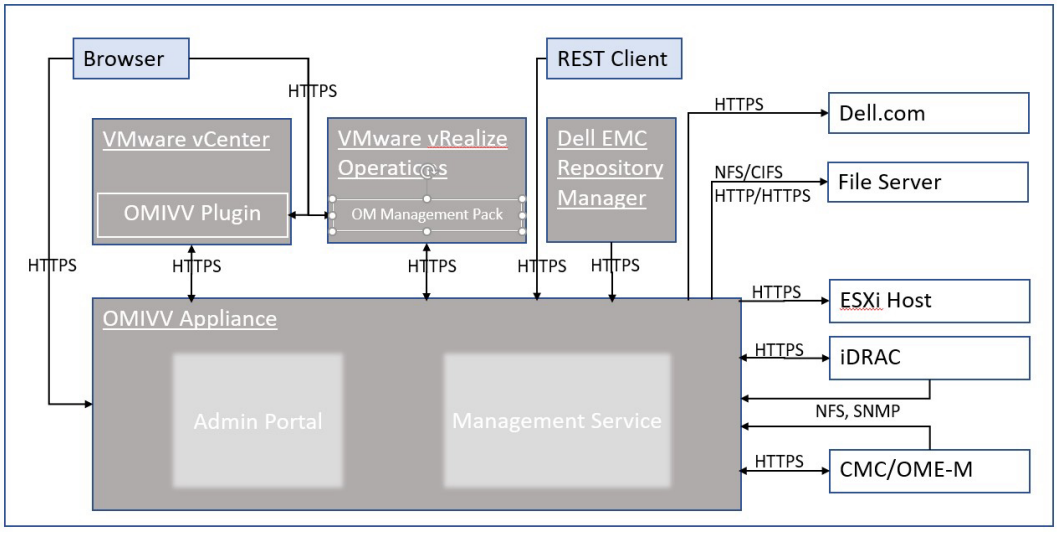


**Figure 1. Mappage des contrôles de sécurité**

# Authentification

## Contrôle d'accès

Les paramètres de contrôle d'accès protègent les ressources contre tout accès non autorisé. Les pages du plug-in OMIVV sont accessibles aux utilisateurs VMware vCenter disposant des rôles et privilèges appropriés configurés dans VMware vCenter. L'accès à la console d'administration OMIVV et aux API RESTful est accordé au compte administrateur de l'appliance OMIVV.

## Comptes d'utilisateur par défaut

OMIVV inclut les comptes d'utilisateur par défaut suivants :

- Compte d'utilisateur local
- Compte d'utilisateur en lecture seule
- Compte racine

### Compte d'utilisateur local

OMIVV fournit un seul compte d'utilisateur administrateur par défaut. Le nom d'utilisateur de ce compte interne est admin.

L'administrateur local a uniquement accès à toutes les opérations de la console d'administration OMIVV Dell EMC.

La première fois que vous déployez OMIVV, vous êtes invité à définir le mot de passe. Suivez les instructions qui s'affichent à l'écran pour définir le mot de passe.

### Compte d'utilisateur en lecture seule

OMIVV fournit un seul compte d'utilisateur local en lecture seule par défaut. Le nom d'utilisateur du compte en lecture seule est lecture seule.

L'administrateur peut uniquement se connecter à OMIVV à l'aide de la console distante de la machine virtuelle.

Ce compte peut être utilisé lors du dépannage afin d'afficher les états et les journaux critiques de l'appliance.

La première fois que vous déployez OMIVV, vous êtes invité à définir le mot de passe. Suivez les instructions qui s'affichent à l'écran pour définir le mot de passe.

### Compte racine

L'appliance OMIVV dispose d'un compte racine du système d'exploitation.

Ce compte par défaut n'est pas accessible. L'équipe de support technique utilise le compte racine afin de déboguer les problèmes de champ.

## Comptes d'utilisateur externes

Les utilisateurs VMware vCenter peuvent accéder aux éléments de l'interface utilisateur du plug-in OMIVV à partir du client HTML5 vCenter lorsque les utilisateurs disposent des rôles et des privilèges appropriés sur vCenter. Pour en savoir plus sur les rôles et les privilèges, consulter Privilèges requis pour les utilisateurs non administrateurs , page 14.

# Paramètres de sécurité de connexion

## Échec du comportement de la connexion

En cas de multiples échecs d'authentification, OMIVV inclut des paramètres de sécurité.

## Verrouillage du compte d'utilisateur local

Après 6 échecs de connexion consécutifs au compte d'utilisateur local, OMIVV interdit temporairement l'accès à l'utilisateur pendant une période d'une minute.

## Délai d'expiration automatique de la session

### Délai d'expiration de la session d'un navigateur inactif

Par défaut, après 15 minutes d'inactivité, la session OMIVV expire et vous êtes automatiquement déconnecté.

# Considérations relatives à la configuration et aux types d'authentification

## Authentification des utilisateurs vCenter

OMIVV dépend de l'authentification vCenter pour accéder aux pages de plug-in et aux API RESTful en rapport avec les opérations vCenter. Les pages de plug-in et les API RESTful relatives aux opérations vCenter nécessitent les privilèges créés par Dell EMC sur vCenter lors de l'enregistrement.

## Enregistrement d'un nouveau serveur vCenter

**Prérequis**

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 14.

**À propos de cette tâche**

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 (avec ou sans mode lié) 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 :

**Étapes**

1. Accédez à https://<IPAppliance ou nomhôte>.
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 de l'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 de l'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 de l'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 versionssupérieures.
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.

### Résultats

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. Par exemple, un utilisateur X disposant des privilèges nécessaires enregistre OMIVV avec vCenter et l'utilisateur Y ne dispose que des privilèges Dell. L'utilisateur Y peut désormais se connecter au vCenter et déclencher une tâche de mise à jour 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, déconnectez-vous, puis reconnectez-vous à vCenter. Si le problème persiste, redémarrez les services clients vSphere sur le serveur vCenter.

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

### Prérequis

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.

### À propos de cette tâche

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

### Étapes

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 15.

**Résultats**

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 15.

# Attribution de privilèges Dell à un rôle existant

**À propos de cette tâche**

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.

**Étapes**

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 Rôle opérationnel Dell , page 16.
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.

# Sécurité des utilisateurs vCenter

## Autorisations et rôles de sécurité

OpenManage Integration pour 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 pour 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.

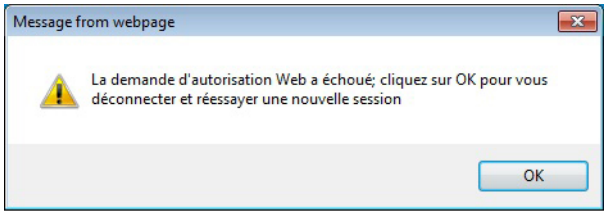


**Figure 2. Message d'erreur de sécurité**

## 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 3. 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

# Gestion des utilisateurs et des informations d'identification

# Comptes préchargés

Le tableau suivant donne une description des comptes préchargés OMIVV :

### Tableau 4. Comptes préchargés

| Compte d'utilisateur | Description |
|---|---|
| Administrateur OpenManage Integration pour VMware vCenter | Utilisateur par défaut de l'administration de l'application Web OMIVV. |
| Utilisateur en lecture seule. | OMIVV fournit un seul compte d'utilisateur local en lecture seule par défaut.<br>L'administrateur peut uniquement se connecter à OMIVV à l'aide de la console distante de la machine virtuelle.<br>Ce compte peut être utilisé lors du dépannage afin d'afficher les états et les journaux critiques de l'appliance. |
| Racine du système d'exploitation Linux | Impossible d'accéder au compte racine du système d'exploitation. L'équipe de support technique utilise le compte racine afin de déboguer les problèmes de champ. |

# Références par défaut

Le tableau suivant donne une description des informations d'identification par défaut pour les comptes OMIVV préchargés.

### Tableau 5. Références par défaut

| Compte | Utilisateur | Mot de passe |
|---|---|---|
| Administrateur OpenManage Integration pour VMware vCenter | Admin | Définir lors du premier démarrage après le déploiement. Pour plus d'informations sur la manière dont modifier le mot de passe administrateur, consulter Modification du mot de passe de l'appliance OMIVV , page 18. |
| Utilisateur en lecture seule | Lecture seule | Définir lors du premier démarrage après le déploiement. Une fois connecté en tant qu'utilisateur en lecture seule, il est possible de reconfigurer le mot de passe de l'utilisateur en lecture seule à l'aide des commandes standard de modification du mot de passe Linux. |
| Racine du système d'exploitation Linux | Racine | Le mot de passe racine du système d'exploitation est défini lors du déploiement d'OMIVV. |

# Gestion des informations d'identification

Si vous vous connectez pour la première fois à la console d'administration Dell EMC, connectez-vous en tant qu'administrateur (le nom d'utilisateur par défaut est admin).

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

## Modification du mot de passe de l'appliance OMIVV

**À propos de cette tâche**

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

**Étapes**

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**.

## Autorisation

L'appliance OMIVV prend en charge un seul utilisateur administrateur.

Une fois connecté à OMIVV, l'administrateur peut accéder uniquement aux fonctions de configuration de l'appliance OMIVV, telles que :

- Enregistrement d'un nouveau serveur vCenter
- Configuration de l'appliance
- Mise à niveau de l'appliance OMIVV à l'aide de RPM, des sauvegardes et des restaurations
- Configuration des serveurs NTP (Network Time Protocol)
- Configuration du mode de déploiement
- Génération d'une requête de signature de certificat (CSR)
- Chargement d'un certificat HTTPS
- Configuration des alertes globales
- Génération et téléchargement du lot de dépannage

# Sécurité du réseau

L'appliance OMIVV utilise un pare-feu préconfiguré afin d'améliorer la sécurité en restreignant le trafic réseau entrant et sortant aux ports TCP et UDP. Les tableaux de cette section répertorient les ports entrants et sortants utilisés par OMIVV.

## Exposition du réseau

OpenManage Integration pour VMware vCenter utilise des ports entrants et sortants pour communiquer avec des systèmes distants.

## Ports sortants

Les ports sortants peuvent être utilisés par OMIVV lors de la connexion à un système distant.

Les ports répertoriés dans le tableau suivant sont les ports sortants OMIVV.

### Tableau 6. Ports sortants

| Numéro de port | Protocole de couche 4 | Prestataires |
|---|---|---|
| 7 | TCP, UDP | ECHO |
| 22 | TCP | SSH |
| 25 | TCP | SMTP |
| 53 | UDP, TCP | DNS |
| 67,68 | TCP | DHCP |
| 80 | TCP | HTTP |
| 88 | TCP, UDP | Kerberos |
| 111 | TCP, UDP | ONC RPC |

### Tableau 6. Ports sortants

| Numéro de port | Protocole de couche 4 | Prestataires |
|---|---|---|
| 123 | TCP, UDP | NTP |
| 161-163 | TCP, UDP | SNMP |
| 389 | TCP, UDP | LDAP |
| 443 | TCP | HTTPS |
| 448 | TCP | API REST administrateur de Data Protection Search |
| 464 | TCP, UDP | Kerberos |
| 514 | TCP, UDP | rsh |
| 587 | TCP | SMTP |
| 636 | TCP, UDP | LDAPS |
| 902 | TCP | VMware ESXi |
| 2049 | TCP, UDP | NFS |
| 2052 | TCP, UDP | mountd, clearvisn |
| 3009 | TCP | API REST de Data Domain |
| 5672 | TCP | RabbitMQ sur AMQP |
| 8443 | TCP | MCSDK 8443 est une alternative à 443 |
| 9002 | TCP | API REST de Data Protection Advisor |
| 9443 | TCP | Service Web de la console de gestion Avamar |

## Ports entrants

Il s'agit des ports entrants disponibles pour une utilisation par un système distant lors de la connexion à OMIVV.

Les ports répertoriés dans le tableau suivant sont les ports entrants OMIVV.

### Tableau 7. Ports entrants

| Numéro de port | Protocole de couche 4 | Prestataires |
|---|---|---|
| 22 | TCP | SSH |
| 80 | TCP | HTTP |
| 443 | TCP | HTTPS |
| 5671 | TCP | RabbitMQ sur AMQP |

# Sécurité des données

Les données gérées par OMIVV sont stockées et sécurisées dans des bases de données internes de l'appliance, et ne sont pas accessibles depuis l'extérieur.

Les données qui transitent par OMIVV sont sécurisées par un canal de communication sécurisé.

**REMARQUE :** Il est recommandé que les utilisateurs des API RESTful stockent les informations d'identification et les données récupérées en toute sécurité en fonction de vos restrictions d'environnement.

# Chiffrement

OMIVV utilise le chiffrement pour les composants suivants :

- Contrôle d'accès
- Authentification
- Signatures numériques

# Gestion des certificats

OMIVV utilise des certificats pour l'accès HTTP sécurisé (HTTPS).

Par défaut, OMIVV installe et utilise le certificat autosigné pour les transactions sécurisées HTTPS.

Pour renforcer la sécurité, il est recommandé d'utiliser les certificats d'autorité de certification (AC) signés ou personnalisés.

Le certificat autosigné suffit à établir un canal chiffré entre les navigateurs Web et le serveur. Le certificat autosigné ne peut pas être utilisé pour l'authentification.

Vous pouvez utiliser les types de certificats suivants pour l'authentification OMIVV :

- Un certificat autosigné

  OMIVV génère des certificats autosignés lorsque le nom d'hôte de l'appliance change.

- Un certificat signé par un fournisseur d'autorité de certification (AC) de confiance.

**REMARQUE :** Tenez compte des règles de la société lors de la création de certificats.

## Mise à jour des certificats des serveurs vCenter inscrits

### À propos de cette tâche

L'OpenManage Integration pour 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.

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

### Étapes

1. Accédez à https://<IPAppliance ou nomhôte>.
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 de l'hôte ou de l'adresse IP d'un serveur vCenter, cliquez sur **Mettre à jour**.

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

### Prérequis

Par défaut, OMIVV est doté d'un certificat auto-signé. Si vous avez besoin d'un certificat signé par une autorité de certification (AC) pour OMIVV, il est recommandé de charger le nouveau certificat avant de procéder à l'enregistrement de vCenter.

### À propos de cette tâche

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 :

### Étapes

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 demande, dans la boîte de dialogue **GÉNÉRER UNE REQUÊTE DE SIGNATURE DE CERTIFICAT**, saisissez les informations concernant le nom commun, le nom de l'organisation, la localité, l'État, le pays, l'adresse e-mail et le nom alternatif de l'objet (SAN), puis cliquez sur **Continuer**.

   **REMARQUE :** OMIVV ne prend pas en charge les valeurs multiples pour SAN.

3. Cliquez sur **Télécharger**, puis sauvegardez la CSR résultant dans un emplacement accessible.

## Chargement d'un certificat HTTPS

### Prérequis

Assurez-vous que le certificat utilise le format PEM.

### À propos de cette tâche

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.

### Étapes

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.

### Résultats

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

### Étapes

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**.

### Résultats

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.

# Audit et journalisation

L'utilisateur administrateur peut utiliser la console d'administration OMIVV pour générer une offre groupée de dépannage avec tous les journaux pertinents.

Pour plus d'informations, voir Création et téléchargement d'un lot de dépannage , page 23.

Le compte en lecture seule permet de dépanner l'appliance en permettant à l'utilisateur de lire les différents paramètres de l'appliance pendant son exécution. Pour des informations de dépannage plus détaillées, le support technique recommande de consulter les paramètres spécifiques.

**REMARQUE :** Seul l'utilisateur administrateur OMIVV peut effectuer des opérations d'écriture sur l'appliance. L'audit d'utilisateur n'est pas disponible dans les journaux OMIVV. Pour plus d'informations sur les opérations de vCenter effectuées à partir du plug-in

vCenter, reportez-vous aux journaux d'audit vCenter. Pour les API RESTful, le client doit être en mesure de gérer la journalisation des audits.

## Création et téléchargement d'un lot de dépannage

**À propos de cette tâche**

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.

**Étapes**

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**.
   La page de connexion à la console d'administration OMIVV Dell EMC s'affiche.
4. Connexion à la console d'administration OMIVV Dell EMC.
5. Téléchargement de l'ensemble de dépannage. Pour plus d'informations, voir Génération et téléchargement du lot de dépannage , page 23.

## Génération et téléchargement du lot de dépannage

**Prérequis**

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

**À propos de cette tâche**

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.

**Étapes**

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

# Facilité de maintenance

Le site Web de support **https://www.dell.com/support** permet d'accéder à des informations sur les licences, de la documentation produit, des conseils, des téléchargements et des informations de dépannage. Ces informations vous aideront à résoudre les problèmes concernant les produits avant de contacter l'équipe de support technique.

Aucune connexion spéciale à OMIVV n'est requise pour le personnel de maintenance. Si l'offre groupée de dépannage est insuffisante, le personnel peut autoriser l'utilisateur root à collecter des informations supplémentaires.

Assurez-vous d'installer les correctifs de sécurité et autres mises à jour dès qu'ils sont disponibles, notamment la mise à jour du système d'exploitation OMIVV vCenter.

## Correctifs de sécurité

Il s'agit des mises à jour périodiques de OMIVV qui incluent les mises à jour de sécurité et les mises à jour uniquement de sécurité publiées en cas de besoin.

Les mises à jour sont cumulatives et publiées sur le support et les utilisateurs OMIVV reçoivent des notifications également sur le vCenter.

# Mise à jour du système d'exploitation OMIVV

Régulièrement, des correctifs de sécurité et autres sont publiés pour le système d'exploitation OMIVV.

Ces correctifs doivent être installés sur des déploiements OVF existants d'OMIVV à l'aide d'un package de mise à jour RPM. Si possible, il est fortement recommandé d'installer ces correctifs de sécurité et autres sur le serveur OMIVV à l'aide de la mise à jour RPM.

# Intégrité du code de produit

Le programme d'installation du logiciel OMIVV est signé par Dell. Il est recommandé de vérifier l'authenticité de la signature du programme d'installation d'OMIVV.

# 5

# Configuration et gestion diverses

**Sujets :**



## 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 licence standard écrase une licence d'évaluation.

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.

Utilisez l'API RESTful OMIVV pour obtenir plus d'informations sur la licence. Pour plus d'informations, reportez-vous au *Guide de l'API OpenManage Integration pour VMware* sur https://www.dell.com/support.

**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.

# Protection de l’authenticité et de l’intégrité

Pour garantir l’intégrité du produit, les composants d’installation et de mise à jour d’OMIVV sont signés.

Pour garantir l’intégrité des communications, il est recommandé d’utiliser un certificat signé par une autorité de certification.

# Gestion des sauvegardes et restaurations dans OMIVV

Pour protéger OMIVV d’un scénario de reprise après sinistre, il est recommandé d’effectuer des sauvegardes d’OMIVV. Le cas échéant, vous pouvez restaurer OMIVV à partir de ces sauvegardes. Pour plus d’informations sur les sauvegardes et restaurations, consultez le Guide de l’utilisateur d’OMIVV disponible sur le site **https://www.dell.com/support**.