OpenManage Integration for VMware vCenter pour client Bureau

Guide d'utilisation Version 2.3

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser l'ordinateur.

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessure corporelle ou de mort.

2015

Rev. A00

Table des matières

1

Présentation

OpenManage Integration for VMware vCenter

VMware vCenter est la console principalement utilisée par les administrateurs pour gérer et surveiller les hôtes VMware vSphere ESX / ESXi. Dans un environnement virtualisé standard, les alertes et la surveillance VMware sont utilisés pour inviter un administrateur à lancer une console distincte pour résoudre les problèmes matériels. Aujourd'hui, grâce à OpenManage Integration for VMware vCenter, les administrateurs disposent de nouvelles capacités de gestion et surveillance du matériel Dell dans l'environnement virtualisé, telles que :

- Alertes et surveillance de l'environnement
- Surveillance et rapports de serveur unique
- Mises à jour du micrologiciel
- Options de déploiement améliorées

Principales fonctions

Vous pouvez utiliser OpenManage Integration for VMware vCenter pour effectuer les tâches suivantes :

Inventaire	Faire l'inventaire des principaux actifs, effectuer des tâches de configuration, et offrir des vues de cluster et de centre de données des plates-formes Dell.
Surveillance et alertes	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 maintenance).
Mises à jour du micrologiciel	Mettre à jour le matériel Dell à la version la plus récente du BIOS et du micrologiciel
Déploiement et provisionnement	Créer des profils matériels, des profils d'hyperviseur et déployer n'importe quelle combinaison des deux sur des serveurs Dell PowerEdge sans système d'exploitation, à distance et sans PXE, en utilisant vCenter.
Informations de service	Récupérer les informations de garantie à partir de Dell en ligne.

Comment le service de gestion du stockage OpenManage Integration for VMware vCenter aide pour vCenter Administration

OpenManage Integration for VMware vCenter fournit des fonctionnalités de virtualisation supplémentaires qui complètent les fonctions d'administration actuelles de vCenter :

- Compresse les tâches et ajoute des processus de gestion, tels que les mises à jour du micrologiciel et le déploiement de serveurs sans systèmes d'exploitation, à la Console d'administration de serveur vCenter.

- Organise le déploiement de plusieurs serveurs métal nu sans environnement d'exécution de pré-amorçage (Preboot Execution Environment — PXE).
- Fournit des renseignements supplémentaires (inventaire, événements, alarmes) pour diagnostiquer les problèmes de serveur.
- S'intègre avec les rôles, autorisations et l'authentification vCenter standard.

Fonctions OpenManage Integration for VMware vCenter

Voici des fonctionnalités de haut niveau de l'OpenManage Integration for VMware vCenter :

- Surveiller les serveurs Dell à l'aide du sous-système d'alarmes et d'événements vCenter standard.
- Effectuer la configuration et gestion avancées du matériel
- Effectuer le déploiement automatique d'hyperviseurs VMware ESX / ESXi sur des systèmes sans systèmes d'exploitation sans l'aide de PXE
- Construire du matériel et des profils d'hyperviseurs VMware ESX / ESXi
- Effectuer les mises à jour du micrologiciel
- Résoudre les problèmes d'infrastructure
- Rapport depuis la vue de centre de données et de cluster — exportation vers un fichier CSV
- Intégrer les fonctionnalités OpenManage Integration for VMware vCenter aux rôles et autorisations vCenter

2

Configuration OpenManage Integration for VMware vCenter

Les sections suivantes fournissent, étape par étape, les instructions relatives à la configuration initiale du OpenManage Integration for VMware vCenter. Les informations de mise à niveau, désinstallation et de rôles de sécurité sont également traitées dans les sections suivantes.

Autorisations et rôles de sécurité

L'OpenManage Integration for VMware vCenter crypte et stocke les informations d'identification d'utilisateur. Il ne fournit pas les mots de passe aux applications clients afin d'éviter toute demande abusive pouvant entraîner des problèmes. Les sauvegardes de base de données sont entièrement cryptées à l'aide de phrases de sécurité personnalisées ce qui prévient toute utilisation abusive de ces données.

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 dans VMware vCenter ou dans le client Web. Si vous souhaitez qu'un utilisateur nonadmin gère le produit, créez un rôle incluant tous les rôles Dell et ensuite attribuez des autorisations sur les nœuds racine/sommet de l'inventaire et propagez les autorisations, le cas échéant, sur les nœuds enfants auxquels vous souhaitez octroyer un accès à l'utilisateur. Par exemple : si vous souhaitez qu'un utilisateur gère uniquement le cluster A, conservez les autorisations sur le cluster A et supprimez les autorisations sur d'autres clusters.

Intégrité des données

Les communications entre l'appliance virtuelle OpenManage Integration for VMware vCenter, la Console d'administration et le vCenter sont réalisées en utilisant SSL / HTTPS. Le OpenManage Integration for VMware vCenter génère un certificat SSL, qui est utilisé pour effectuer les communications de confiance entre le vCenter et l'appliance. Il vérifie également et fait confiance au certificat du serveur vCenter avant d'effectuer la communication et l'enregistrement du OpenManage Integration for VMware vCenter. L'onglet OpenManage Integration for VMware vCenter Console (dans VMware vCenter) utilise des procédures de sécurité afin d'éviter des demandes abusives pendant le transfert des clés entre la console d'administration et les services dorsaux. Ce type de sécurité entraîne l'échec des fausses requêtes intersites.

Une session de console d'administration sécurisée a un délai d'inactivité de cinq minutes, et la session n'est valide que dans la fenêtre et/ou l'onglet actuel du navigateur. Si l'utilisateur essaie d'ouvrir la session dans une nouvelle fenêtre et/ou un nouvel onglet, une erreur de sécurité demandant une session valide est créée. Cette action empêche également l'utilisateur de cliquer sur une URL malveillante qui pourrait essayer d'attaquer la session de Console d'administration.

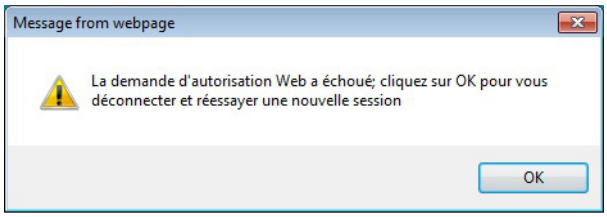

Figure 1. Message d'erreur

Rôles, autorisation et authentification de contrôle d'accès

L'OpenManage Integration for VMware vCenter utilise la session utilisateur actuelle du client vSphere et les informations d'identification d'administrateur enregistrées de l'appliance virtuelle pour effectuer les opérations vCenter. L'OpenManage Integration for VMware vCenter utilise le modèle de rôles et de privilèges intégrés du serveur vCenter pour autoriser les actions d'utilisateurs sur l'appliance virtuelle et les objets gérés vCenter (hôtes et clusters).

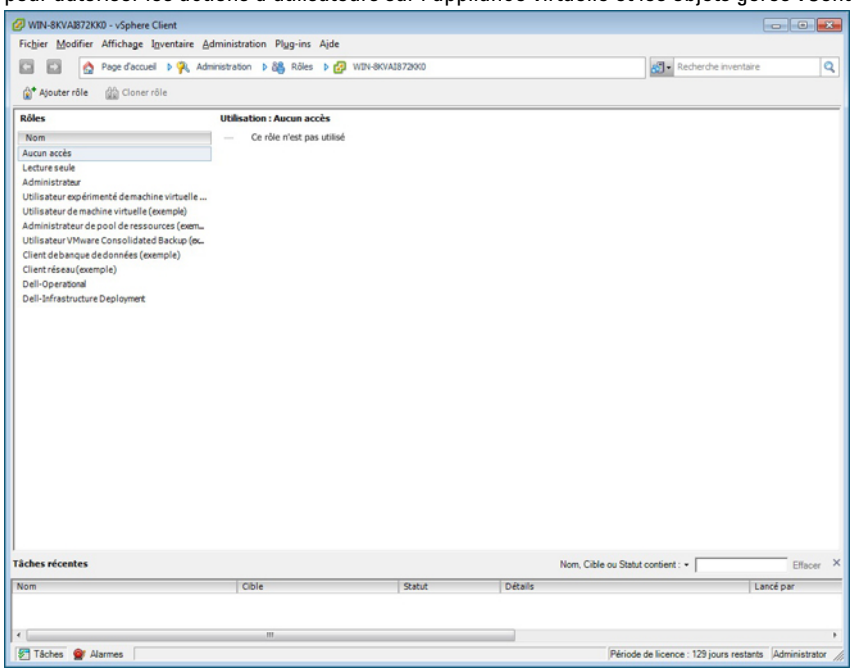

Figure 2. Rôles et privilèges du client vCenter vSphere

Rôle d'opérations Dell

Comprend les privilèges/groupes permettant d'effectuer les tâches d'appliances et de serveurs vCenter, notamment les mises à jour de micrologiciel, les inventaires de matériel, le redémarrage d'un hôte, le placement d'un hôte en mode maintenance ou la création d'une tâche de serveur vCenter

Ce rôle comprend les groupes de privilèges suivants.

Groupe de privilèges : Dell.Configuration	Privilège : Effectuer les tâches associées à l'hôte, Effectuer les tâches associées à vCenter, Configurer SelLog, Configurer ConnectionProfile, Configurer ClearLed, Mise à jour du micrologiciel

Groupe de privilèges : Dell.Inventory	Privilège : Configurer l'inventaire, Configurer la récupération de garantie, Configurer ReadOnly
Groupe de privilèges : Dell.Monitoring	Privilège : Configurer la surveillance, Surveiller
Groupe de privilèges : Dell.Reporting (Non utilisé)	Privilège : Créer un rapport, Exécuter un rapport

Rôle de déploiement de l'infrastructure Dell

Ce rôle contient les privilèges associés spécifiquement aux fonctionnalités de déploiement d'hyperviseur.

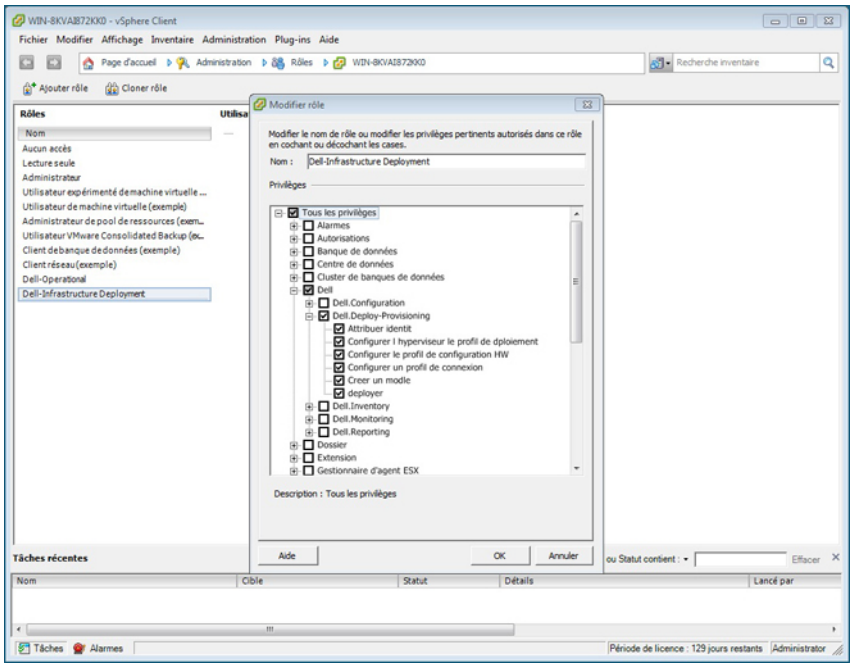

Figure 3. Rôle de déploiement de l'infrastructure Dell

Ce rôle permet de créer un modèle, de configurer le profil de configuration matérielle, de configurer le profil de déploiement d'hyperviseur, de configurer le profil de connexion, d'attribuer une identité et de déployer.

Dell.Déploiement — Provisionnement	Créer un modèle, Configurer le profil de configuration matérielle, Configurer le profil de déploiement d'hyperviseur, Configurer le profil de connexion, Attribuer une identité et Déployer

Comprendre les privilèges

Chaque action effectuée par le OpenManage Integration for VMware vCenter est associée à un privilège. Les sections suivantes répertorient les actions disponibles et les privilèges associés :

- Dell.Configuration.Perform vCenter-Related Tasks

- Sortir et entrer en mode de maintenance
- Obtenir le groupe d'utilisateurs vCenter pour demander les autorisations
- Enregistrer et configurer les alertes ; par exemple, activer / désactiver les alertes sur la page Event Settings (Paramètres d'événement).
- Publier les événements / alertes sur vCenter
- Configurer les paramètres d'événement sur la page Event Settings (Paramètres d'événement).
- Restaurer les alertes par défaut sur la page Event Settings (Paramètres d'événement).
- Vérifier l'état DRS sur les clusters lors de la configuration des paramètres d'alertes / événements.
- Redémarrer l'hôte après l'exécution de mise à jour ou de toute autre action de configuration
- Surveiller l'état / le progrès des tâches vCenter
- Créer des tâches vCenter ; par exemple, la tâche de mise à jour du micrologiciel, la tâche de configuration d'hôte, et la tâche d'inventaire.
- Mettre à jour l'état / le progrès des tâches vCenter
- Obtenir les profils d'hôte
- Ajouter un hôte au centre de données
- Ajouter un hôte au cluster
- Appliquer un profil à un hôte
- Obtenir les informations d'identification CIM
- Configurer la conformité des hôtes
- Obtenir l'état des tâches de conformité

- Dell.Inventory.Configure ReadOnly
  - Obtenir tous les hôtes vCenter pour construire l'arborescence lors de la configuration des profils de connexion vCenter
  - Vérifier si l'hôte est un serveur Dell lorsque l'onglet est sélectionné
  - Obtenir l'adresse IP vCenter
  - Obtenir l'adresse IP de l'hôte
  - Obtenir l'utilisateur de la session vCenter actuelle à partir de l'ID de session du client vSphere
  - Obtenir l'arborescence d'inventaire vCenter pour afficher l'inventaire vCenter dans une structure arborescente
- Dell.Monitoring.Monitor
  - Obtenir le nom d'hôte pour publier l'événement
  - Effectuer des opérations sur le journal d'événements ; par exemple, obtenir le nombre d'événements, ou modifier les paramètres du journal d'événements
  - Enregistrer, désenregistrer et configurer les événements / alertes — Recevoir des interruptions SNMP et publier des événements
- Dell.Configuration.Firmware Update
  - Effectuer mise à jour du micrologiciel
  - Charger les informations de référentiel du micrologiciel et de fichier DUP sur la page de l'assistant de mise à jour du micrologiciel
  - Interroger l'inventaire du micrologiciel
  - Configurer les paramètres de l'espace de stockage du micrologiciel
  - Configurer le dossier de préparation et effectuer une mise à jour à l'aide de la fonctionnalité de préparation
  - Tester les connexions réseau et de l'espace de stockage
- Dell.Deploy-Provisioning.Create Template

  - Créer, afficher, supprimer et modifier des modèles de déploiement

- Dell.Configuration.Perform Host-Related Tasks
  - Faire clignoter un voyant, Éteindre un voyant, Configurer l'URL OMSA à partir de l'onglet Dell Server Management
  - Lancer la console OMSA
  - Lancer la console iDRAC
  - Afficher et effacer le journal SEL
- Dell.Inventory.Configure Inventory
  - Afficher l'inventaire du système dans l'onglet Dell Server Management
  - Obtenir les détails du stockage
  - Obtenir les détails de la surveillance de l'alimentation
  - Créer, afficher, modifier, supprimer et tester les profils de connexion sur la page Connection Profiles (Profils de connexion)
  - Planifier, mettre à jour et supprimer la planification de l'inventaire
  - Exécuter l'inventaire sur les hôtes

3

Comprendre comment configurer ou modifier l'OpenManage Integration for VMware vCenter

Après avoir effectué l'installation de base de l'OpenManage Integration for VMware vCenter, vous pouvez passer à la configuration de l'appliance à l'aide d'une des méthodes suivantes décrites plus loin dans cette section :

- **Tâches de configuration à l'aide de l'Assistant Configuration**
- **Tâches de configuration à l'aide des options Paramètres**

Bien que l'utilisation de l'Assistant Configuration constitue la méthode la plus utilisée, vous pouvez aussi accomplir cette tâche à l'aide de la page Paramètres de l'appliance dans le Dell Management Center.

L'interface utilisateur est similaire dans les deux cas, sauf que dans l'Assistant vous cliquez sur *Enregistrer et continuer*, alors qu'avec les options Paramètres, vous cliquez sur *Appliquer*.

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

Utilisez ces tâches lorsque vous configurez l'OpenManage Integration for VMware vCenter à l'aide de l'Assistant Configuration :

1. Page d'accueil de l'Assistant Configuration
2. Création d'un nouveau profil de connexion
3. Configuration des événements et alarmes
4. Configuration d'un serveur proxy
5. Planification des tâches d'inventaire
6. Exécution d'une tâche de récupération de la garantie
7. Configuration des références de déploiement
8. Configuration de l'espace de stockage de mise à jour du micrologiciel par défaut
9. Activation du lien OMSA

Tâches de configuration à l'aide des options Paramètres

Utilisez ces tâches pour configurer ou modifier les tâches de configuration de l'OpenManage Integration for VMware vCenter :

- Création d'un nouveau profil de connexion
- Configuration des événements et alarmes
- Configuration d'un serveur proxy
- Modification d'une planification de tâche d'inventaire
- Récupération de la garantie
- Affichage ou modification des références de déploiement
- Configuration des références et de l'espace de stockage du micrologiciel
- Activation du lien OMSA

Page Accueil d'OpenManage Integration for VMware vCenter

Lorsque vous vous connectez à la page d'accueil de l'OpenManage Integration for VMware vCenter, les boutons de navigation sont dans le volet gauche, et le volet droit fournit des liens et des informations utiles. Cette présentation vous fournit des liens essentiels vers les tâches que vous effectuez le plus souvent. Bien que toutes ces tâches se trouvent dans le volet gauche de navigation, elles se trouvent également sur la page d'accueil pour faciliter l'utilisation. Les tâches fournies sur cette page relèvent des catégories suivantes :

- Déploiement d'hôtes et de serveurs

  Cette section fournit plus d'informations sur le déploiement d'hôtes et de serveurs.
- Conformité des hôtes vSphere et des serveurs sans système d'exploitation

  Cette section fournit plus d'informations et vous permet d'afficher les détails sur les hôtes vSphere et les serveurs sans système d'exploitation non conformes ou d'exécuter les Assistants pour les corriger.
- Planification de l'inventaire

  Cette section contient des informations sur la planification de l'inventaire.
- Planification de la récupération des données de garantie

  Cette section vous permet d'afficher/modifier les planifications de garantie et d'en savoir plus.
- Licences

  Cette section vous permet d'en savoir plus sur les licences. Utilisez les liens pour atteindre les tâches de licence.
- Paramètres d'événements et alarmes

  Cette section contient des informations sur les paramètres d'événements et alarmes et le lien permettant de les configurer.
- Licences de connexion hôte

  Dans cette section, vous pouvez afficher les licences de connexion hôte en temps réel. En outre, vous pouvez utiliser le lien Acheter maintenant pour acheter une licence de version complète afin de gérer plusieurs hôtes. Le lien Acheter maintenant apparaît uniquement si vous utilisez une licence de démonstration.
- Licences de connexions vCenter: vous pouvez afficher les informations liées aux licences de connexions vCenter VMware. Pour plus d'informations sur les licences de connexions vCenter, voir À propos des licences OpenManage Integration for VMware vCenter

Page d'accueil de l'Assistant Configuration

Une fois installé, l'OpenManage Integration for VMware vCenter doit être configuré.

1. Dans le **Client vSphere**, à partir de la page d'**accueil** , sous l'onglet **Gestion**, cliquez sur l'icône **Dell Management Center**.
2. La première fois que vous cliquez sur l'icône **Dell Management Center**, elle ouvre l'**Assistant Configuration**. Vous pouvez aussi accéder à cet Assistant sur la page **Dell Management Center** → **Paramètres**.
3. Dans l'onglet **Accueil**, examinez les étapes à suivre, puis cliquez sur **Suivant**.

Création d'un nouveau profil de connexion [Assistant]

Un profil de connexion stocke les références que l'appliance virtuelle utilise pour communiquer avec les serveurs Dell. Chaque serveur Dell doit être associé à un seul profil de connexion qui sera géré par le Dell Management Plug-in. Vous pouvez attribuer plusieurs serveurs à un profil de connexion unique. La création d'un nouveau profil de connexion dans l'Assistant Configuration est similaire à la création dans Dell Management Center, à l'aide de l'option Paramètres.

REMARQUE : L'installation de l'agent OMSA n'est pas requise pour les installations sur des hôtes utilisant des serveurs PowerEdge de 12e génération ou de générations ultérieures. Pour les installations sur des serveurs de 11e génération, l'agent OMSA est maintenant installé automatiquement au cours du processus de déploiement.

Pour créer un nouveau profil de connexion avec l'Assistant :

1. Dans l'onglet **Profils de connexion**, cliquez sur **Créer nouveau**.
2. Dans le volet **Nom et description du profil**, entrez le **Nom du profil** et une **Description** facultative (ce nom et cette description servent à gérer les profils de connexion personnalisés), puis cliquez sur **Suivant**.
3. Dans le volet **Hôtes associés**, sélectionnez les hôtes associés au profil de connexion, puis cliquez sur **Suivant**.
4. Examinez les informations à propos des références et des protocoles de connexion et cliquez sur **Suivant**.
5. Dans le volet iDRAC, entrez les **références iDRAC**.
   a. Entrez le **Nom d'utilisateur**, **Mot de passe** et **Confirmez le mot de passe**. Le mot de passe peut contenir au plus 16 caractères, y compris des espaces. Les mots de passe doivent correspondre et utiliser uniquement des caractères imprimables ASCII.

      REMARQUE : Les mots de passe peuvent contenir au plus 20 caractères imprimables ASCII. Le nom de domaine peut contenir des caractères alphanumériques, un - (tiret) et un . (point) uniquement.

   b. Pour la **Vérification du certificat**, sélectionnez **Activer** pour télécharger et stocker le certificat iDRAC et le valider durant toutes les futures connexions ou sélectionnez **Désactiver** pour ne pas effectuer de vérification et ne pas stocker le certificat.

      Vous devez sélectionner Activer si vous utilisez Active Directory.
6. Cliquez sur **Suivant**.
7. Dans le volet **Références de racine hôte**, procédez ainsi :
   a. Entrez le **Nom d'utilisateur** et le **Mot de passe**, puis **Vérifiez le mot de passe**. Les mots de passe doivent concorder.

      REMARQUE : Les mots de passe ne doivent pas dépasser 127 caractères, ni contenir de caractères spéciaux.

      REMARQUE : Pour les serveurs non dotés de carte iDRAC Express ou Enterprise, lors de l'exécution du test de connexion iDRAC, le message *Non applicable pour ce système* s'affiche.

      REMARQUE : Les références OMSA sont les mêmes que celles utilisées pour les hôtes ESX et ESXi.

   b. Pour **Vérification du certificat**, sélectionnez **Activer** pour télécharger et stocker le certificat OMSA et le valider durant toutes les futures connexions ou sélectionnez **Désactiver** pour ne pas effectuer de vérification et ne pas stocker le certificat. Sélectionnez Activer si vous utilisez Active Directory.
8. Cliquez sur **Suivant**.
9. La fenêtre **Tester la connexion** teste les références iDRAC et de racine hôte entrées sur les serveurs sélectionnés. Procédez ainsi :
   - Pour commencer le test, cliquez sur **Tester sélectionné**. Les autres options sont inactives.
   - Pour arrêter les tests, cliquez sur **Interrompre tous les tests**.
10. Pour enregistrer le profil, cliquez sur **Enregistrer**.
11. Pour passer à la configuration des événements et alarmes, cliquez sur **Enregistrer et continuer**.

Configuration des événements et alarmes [Assistant]

Configurez les événements et alarmes à l'aide de l'Assistant Configuration ou depuis Dell Management Center, sous l'onglet Événements et alarmes dans l'option Paramètres.

REMARQUE : Sur les hôtes antérieurs à 12G, cette fonction exige que l'appliance virtuelle soit configurée comme destination d'interruption dans OMSA pour afficher les événements d'hôte dans vCenter.

Pour configurer les événements et alarmes :

1. Dans l'**Assistant Configuration**, sous **Niveaux de publication d'événement**, sélectionnez l'une des options suivantes :
   - Ne publier aucun événement : bloquer les événements matériels.
   - Publier tous les événements : publier tous les événements matériels.
   - Publier uniquement les événements critiques et d'avertissement : publier uniquement les événements matériels de niveau critique et d'avertissement.
   - Publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation : publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation ; c'est le niveau de publication d'événement par défaut.
2. Pour activer tous les événements et alarmes matériels, cochez la case **Activer les alarmes d'hôtes Dell**.

   REMARQUE : Les hôtes Dell pour lesquels les alarmes sont activées répondent aux événements critiques en entrant en mode de maintenance.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Continuer** pour accepter cette modification ou cliquez sur **Annuler**.

   REMARQUE : Cette étape n'apparaît que si **Activer les alarmes d'hôtes Dell** est sélectionné.
4. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell gérés, cliquez sur **Restaurer les alarmes par défaut**.

   Il peut s'écouler une minute avant que le changement prenne effet.
5. Pour poursuivre l'Assistant, cliquez sur **Enregistrer et continuer**.

Restaurer la sauvegarde de l'appliance OpenManage Integration pour VMware vCenter ne permet pas de restaurer tous les paramètres d'alarme. Cependant, dans l'interface utilisateur graphique (GUI) OpenManage Integration pour VMware, le champ **Alarmes et événements** affiche les paramètres restaurés. Pour résoudre ce problème, dans l'nterface graphique GUI d'OpenManage Integration pour VMware, dans l'onglet **Gérer** → **Paramètres** , modifiez manuellement les paramètres de la zone Événements et alarmes.

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

Configuration d'un serveur proxy [Assistant]

Configurez le serveur proxy dans l'Assistant Configuration ou plus tard avec la page **Paramètres** → **Proxy** de Dell Management Center.
Pour configurer un serveur proxy :

1. Dans la fenêtre **Configurer un proxy HTTP**, procédez comme suit :
   - Pour ne pas utiliser un serveur proxy, cliquez sur **Enregistrer et continuer**.
   - Pour utiliser un serveur proxy, sous **Paramètres** entrez une **adresse de serveur proxy**.
2. Entrez le **numéro de port proxy**.
3. Sélectionnez la case **Références requises** le cas échéant.
4. Si vous avez sélectionné **Références requises**, procédez comme suit :
   a. Dans la zone de texte **Nom d'utilisateur proxy**, entrez le nom d'utilisateur proxy.
   b. Dans la zone de texte **Mot de passe proxy**, entrez le mot de passe proxy.
   c. Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe proxy.
5. Sous **Proxy**, cochez la case **Utiliser le proxy**.

6. Pour enregistrer ces options et continuer, cliquez sur **Enregistrer et continuer**.

Planification des tâches d'inventaire [Assistant]

La configuration de la planification d'inventaire est similaire dans l'Assistant Configuration et l'option **Dell Management Center → Paramètres**. La seule différence est que l'Assistant donne l'option d'exécuter l'inventaire immédiatement si vous le souhaitez.

REMARQUE : Pour vous assurer que l'OpenManage Integration for VMware vCenter continue d'afficher des informations à jour, nous vous recommandons de planifier une tâche d'inventaire périodique. De telles tâches consomment un minimum de ressources et n'affectent pas les performances de l'hôte.

Pour planifier une tâche d'inventaire :

1. Dans l'Assistant **Configuration**, dans la fenêtre **Planification d'inventaire**, procédez ainsi :
   - Pour exécuter des planifications d'inventaire, cliquez sur **Les jours sélectionnés**.
   - Pour ne pas exécuter de planifications d'inventaire, sélectionnez **Ne pas exécuter d'inventaire sur les hôtes Dell**.
2. Si vous avez sélectionné **Les jours sélectionnés**, procédez ainsi :
   a. Cochez la case en regard de chaque jour de la semaine pendant lequel vous voulez exécuter l'inventaire.
   b. Dans la zone de texte, entrez l'heure au format HH:MM.

      L'heure entrée est votre heure locale. Par conséquent, si vous voulez exécuter l'inventaire dans le fuseau horaire de l'appliance virtuelle, calculez le décalage horaire entre votre fuseau horaire local et celui de l'appliance virtuelle, puis entrez l'heure de manière appropriée.
3. Pour appliquer les modifications et continuer, cliquez sur **Enregistrer et continuer**.

Exécution d'une tâche de récupération de la garantie [Assistant]

La configuration de la tâche de récupération de la garantie est similaire qu'elle soit effectuée à l'aide de l'Assistant ou à partir de l'option **Dell Management Center → Paramètres**. De plus, vous pouvez maintenant exécuter la tâche de récupération de la garantie depuis la file d'attente des tâches.

Pour exécuter une tâche de récupération de la garantie :

1. Dans l'**Assistant Configuration**, dans la fenêtre **Planification de garantie**, procédez ainsi :
   - Pour exécuter des planifications de garantie, cliquez sur **Les jours sélectionnés**.
   - Pour ne pas exécuter de planifications de garantie, sélectionnez **Ne pas récupérer les données de garantie**.
2. Si vous avez sélectionné **Les jours sélectionnés**, procédez ainsi :
   a. Cochez la case en regard de chaque jour de la semaine où vous voulez exécuter les tâches de garantie.
   b. Dans la zone de texte, entrez l'heure au format HH:MM.

      L'heure entrée est votre heure locale. Par conséquent, si vous voulez exécuter l'inventaire au fuseau horaire de l'appliance virtuelle, calculez le décalage horaire entre votre fuseau horaire local et celui de l'appliance virtuelle, puis entrez l'heure de manière appropriée.
3. Pour appliquer les modifications et continuer, cliquez sur **Enregistrer et continuer**.

Configuration des références de déploiement [Assistant]

Les références de déploiement servent à communiquer en toute sécurité avec un système sans système d'exploitation qui a été découvert à l'aide de l'auto-détection. Pour la sécurisation de la communication, il utilise l'iDRAC, depuis la découverte initiale jusqu'à la fin du processus de déploiement. Une fois le déploiement terminé, les références sont remplacées par celles qui se trouvent dans le profil de connexion correspondant au système sans système d'exploitation à partir de l'Assistant Déploiement. Si les références de déploiement sont modifiées, tous les systèmes

nouvellement découverts à partir de ce stade sont configurés avec les nouvelles références. Cependant, les références qui se trouvent sur les serveurs découverts avant la modification ne sont pas affectées.

REMARQUE : OpenManage Integration for VMware vCenter fonctionne comme un serveur de provisionnement. Les références de déploiement sont définies sur l'iDRAC qui utilise le plug-in comme serveur de provisionnement au cours du processus de découverte automatique.

Pour configurer les références de déploiement :

1. Dans la fenêtre **Références de déploiement**, vous pouvez afficher ou modifier les références. Le serveur sans système d'exploitation passe de ces références à celles spécifiées dans le profil de connexion.
2. Pour modifier ces références, sous **Références du déploiement de serveur sans système d'exploitation**, procédez ainsi :
   a. Dans la zone de texte **Nom d'utilisateur**, modifiez le nom d'utilisateur.
   b. Dans la zone de texte **Mot de passe**, modifiez le mot de passe.
   c. Dans la zone de texte **Vérifier le mot de passe**, confirmez le mot de passe.
3. Pour enregistrer les références spécifiées et continuer l'Assistant Configuration, cliquez sur **Enregistrer et continuer**.

Configuration de l'espace de stockage de mise à jour du micrologiciel par défaut [Assistant]

Les paramètres de l'espace de stockage du micrologiciel contiennent l'emplacement du catalogue du micrologiciel utilisé pour mettre à jour les serveurs déployés. Vous pouvez configurer l'espace de stockage du micrologiciel ici dans l'Assistant ou plus tard à l'aide de l'option **Dell Management Center → Paramètres**. Par ailleurs, vous pourrez exécuter la mise à jour plus tard à partir de l'onglet OpenManage Integration.

Pour configurer l'espace de stockage de mise à jour du micrologiciel par défaut :

1. Dans l'**Assistant Configuration**, sur la page **Espace de stockage du micrologiciel**, pour choisir l'espace de stockage par défaut pour les mises à jour du micrologiciel, sélectionnez l'une des options suivantes :

   - Dell Online

     Espace de stockage du micrologiciel par défaut (ftp.dell.com) avec un dossier d'organisation. L'OpenManage Integration for VMware vCenter télécharge les mises à jour du micrologiciel sélectionnées et les stocke dans le dossier d'organisation. Elles sont ensuite appliquées selon les besoins.

   - Répertoire local/partagé :

     Ces espaces de stockage sont créés avec l'application Dell Repository Manager. Ces espaces de stockage locaux doivent se trouver sur des partages de fichiers Windows.

2. Si vous avez sélectionné **Dossier local/partagé**, procédez ainsi :
   a. Entrez l'**Emplacement du fichier de catalogue** sous le format suivant :

      - Partage NFS pour fichier xml : host:/partage/nom de fichier.xml
      - Partage NFS pour le fichier gz : hôte/partage/nom de fichier.gz
      - Partage CIFS pour fichier xml : \\hôte\partage\nom de fichier.xml
      - Partage CIFS pour fichier gz : \\hôte\partage\nom de fichier.gz

   b. Si vous utilisez un partage CIFS, entrez le **Nom d'utilisateur**, le **Mot de passe** et **Vérifiez le mot de passe**. Les mots de passe doivent concorder. Ces champs ne sont actifs que lorsque vous entrez un partage CIFS.

      REMARQUE : Le caractère @ n'est pas accepté dans les champs Nom d'utilisateur et Mot de passe des dossiers réseau partagés.

   c. Pour valider vos entrées cliquez sur **Démarrer le test**.

3. Pour enregistrer cette sélection et poursuivre l'**Assistant Configuration**, cliquez sur **Enregistrer et continuer**.

Activation du lien OMSA [Assistant]

Préalablement à l'ouverture d'OMSA (OpenManage Server Administrator) dans l'appliance virtuelle OpenManage Integration for VMware vCenter, le serveur Web OMSA doit être installé et configuré. Voir le *Guide d'installation d'OpenManage Server Administrator* pour en savoir plus sur l'installation et la configuration du serveur Web.

REMARQUE : OMSA est requis uniquement sur les serveurs Dell antérieurs aux serveurs Dell PowerEdge 12G.

Vous pouvez utiliser OMSA pour :

- Gérer les éléments vCenter (informations détaillées sur l'intégrité au niveau capteur/composant).
- Effacer les journaux de commandes et les journaux des événements système (System Event Logs — SEL).
- Obtenir des statistiques sur les cartes réseau.
- Assurez-vous que OpenManage Integration for VMware vCenter capture les événements d'un hôte sélectionné.

1. Dans l'**Assistant Configuration**, sur la page **OpenManage Server Admin**, utilisez la zone de texte **URL du serveur Web OMSA** pour entrer l'URL OMSA. Vous devez inclure l'URL complète avec HTTPS et numéro de port. Par exemple,

   https:\\ <OMSA_Serveur_IP_ou_nom d'hôte> : 1311.
2. Pour enregistrer cette URL et terminer l'Assistant Configuration, cliquez sur **Terminer**.

Configuration de partages NFS

Pour utiliser des partages NFS avec OpenManage Integration for VMware vCenter comme dossier intermédiaire et pour effectuer des opérations de sauvegarde et restauration et des mises à jour du micrologiciel, vous devez renseigner certains éléments de configuration. Les partages CIFS ne nécessitent pas de configuration supplémentaire.

Pour configurer des partages NFS :

1. Sur la machine à système d'exploitation Linux ou Unix qui héberge les partages NFS, modifiez **/etc/exports** pour ajouter : **/share/path <IP de l'appliance> (rw) *(ro)**.

   Cela donne à l'appliance virtuelle un accès complet en lecture et écriture au partage, mais limite tous les autres utilisateurs à un accès en lecture seule.
2. Démarrez les services nfs :

   ```
   service portmap start service nfs start service nfslock status
   ```

   REMARQUE : Les étapes ci-dessus peuvent varier en fonction de la distribution Linux utilisée.
3. Si l'un des services était déjà en cours d'exécution :

   ```
   exportfs -ra
   ```

Présentation des paramètres

Vous pouvez effectuer les tâches suivantes à partir de la section Paramètres :

- Général : configure l'URL OMSA qui s'affiche sur l'onglet Hôtes Dell dans vCenter. Vous pouvez aussi activer ou désactiver Gestion proactive des systèmes ou Notification d'expiration de la garantie.
- Événements et alarmes : active ou désactive toutes les alarmes matérielles (l'état d'alerte actuel est affiché sur l'onglet Alarmes). Configure également le filtrage des événements et alertes entrants.
- Proxy HTTP : active ou désactive l'utilisation de proxy durant la communication avec des sites Internet.
- Planification de l'inventaire : configure la planification de l'inventaire d'hôte vCenter.

- Planification de la garantie : configure la planification de la récupération des informations de garantie des hôtes Dell à partir de Dell Online.
- Références de déploiement : configure les Références à utiliser pour la communication avec les serveurs Dell durant la découverte initiale et le déploiement de serveurs métal nu.
- Espace de stockage du micrologiciel : vous permet de modifier le lieu de stockage des mises à jour du micrologiciel.
- Sécurité : fournit une liste blanche de serveurs qui limite les serveurs déployés.

Présentation des paramètres généraux

Les paramètres généraux servent à :

- Définir l'URL d'OpenManage Server Administrator (OMSA).
- Activer ou désactiver la notification d'expiration de la garantie.

Le logiciel OMSA peut servir à :

- Gérer les éléments vCenter (informations détaillées sur l'intégrité au niveau capteur/composant).
- Effacer les journaux de commandes et les journaux des événements système (System Event Logs — SEL).
- Obtenir des statistiques sur les cartes réseau.
- Assurez-vous que OpenManage Integration for VMware vCenter capture les événements d'un hôte sélectionné.

REMARQUE : Le logiciel OMSA est requis uniquement sur les serveurs Dell antérieurs aux serveurs Dell PowerEdge 12G.

La notification de l'expiration de la garantie peut être utilisée pour :

- Surveiller la date d'expiration de la garantie.
- Définir un seuil de nombre minimum de jours de garantie restants au delà duquel une alerte d'avertissement ou critique est générée. L'alerte apparaît sous forme d'icône sur l'onglet OpenManage Integration de l'hôte.

Tâches connexes :

- Activation du lien OMSA
- Activation ou désactivation de la notification d'expiration de la garantie.

Activation du lien OMSA en dehors de l'Assistant Configuration

Pour lancer OMSA (OpenManage Server Administrator) dans l'appliance virtuelle OpenManage Integration for VMware vCenter, le serveur Web OMSA doit être installé et configuré. Voir le *Guide d'installation de Dell OpenManage Server Administrator* correspondant à la version d'OMSA utilisée pour en savoir plus sur l'installation et la configuration du serveur Web.

REMARQUE : OMSA est requis uniquement sur les serveurs Dell antérieurs aux serveurs Dell PowerEdge 12G.

Pour activer le lien OMSA :

1. Dans le **Dell Management Center**, **Paramètres** → **Général** sous Programme de lancement d'OMSA, cliquez sur **Modifier**.
2. Utilisez la zone de texte **URL du serveur Web OMSA** pour entrer l'URL d'OMSA. Vous devez spécifier l'URL complète avec HTTPS et le numéro de port 1311.
3. Pour enregistrer l'URL, cliquez sur **Appliquer**.

   Pour plus d'informations sur la configuration d'une destination d'interruption OMSA, voir Configuration d'une destination d'interruption OMSA.

Activation ou désactivation de la notification 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 configurant l'alerte Seuil d'alerte minimum en jours. Utilisez cette page pour activer ou désactiver les notifications d'expiration de la garantie du serveur pour les hôtes et clusters. Configurez ou modifiez cette fonctionnalité dans Dell Management Center sur la page Paramètres/Général.

Pour activer ou désactiver la notification d'expiration de la garantie :

1. Dans **Dell Management Center**, cliquez sur **Paramètres → Général.**
2. Sur la page **Général**, pour activer les notifications, cochez la case **Activer les notifications de l'état de la garantie**.
3. Pour configurer l'option **Seuil d'alerte minimum en jours**, procédez ainsi :
   a. Pour configurer des avertissements, dans la liste déroulante **Avertissement**, sélectionnez le nombre de jours correspondant aux avertissements à propos de l'état de la garantie du serveur.
   b. Pour configurer l'état de licence critique, dans la liste déroulante **Critique** configurez le nombre de jours correspondant à l'avertissement d'état critique de la garantie du serveur.
4. Pour appliquer les modifications, cliquez sur **Appliquer**.

Création d'un nouveau profil de connexion

Un profil de connexion stocke les références que l'appliance virtuelle utilise pour communiquer avec les serveurs Dell. Chaque serveur Dell doit être associé à un seul profil de connexion qui sera géré par l'OpenManage Integration for VMware vCenter. Vous pouvez attribuer plusieurs serveurs à un profil de connexion unique. La création du profil de connexion est similaire dans l'Assistant Configuration et à partir de l'option **Dell Management Center → Paramètres**. Vous pouvez exécuter l'Assistant Configuration la première fois que vous accédez à la Dell Management Console, ou ultérieurement dans la fenêtre Paramètres.

REMARQUE : Avec les installations sur des hôtes de serveurs Dell PowerEdge de12e génération ou de générations ultérieures, l'installation de l'agent OMSA n'est pas requise. Pour les installations sur des serveurs Dell PowerEdge de 11e génération, l'agent OMSA est désormais installé automatiquement au cours du processus de déploiement.

REMARQUE : Pour en savoir plus sur les licences, voir À propos des licences OpenManage Integration for VMware vCenter.

REMARQUE : Il est interdit de créer un profil de connexion si le nombre d'hôtes ajoutés excède la limite de licences.

Pour créer un nouveau profil de connexion :

1. Dans l' **OpenManage Integration for VMware vCenter** , dans le volet de gauche, cliquez sur **Profils de connexion**.
2. Dans le volet **Nom et description du profil**, entrez le **Nom du profil de connexion** et une **Description du profile de connexion** facultative (ce nom et cette description servent à gérer les profils de connexion personnalisés).
3. Dans la page **Hôtes associés**, sélectionnez les hôtes associés au profil de connexion, puis cliquez sur **Suivant**.
4. Lisez les informations offertes par la page **Informations d'identification**, puis cliquez sur **Suivant**.
5. Dans la page iDRAC, sous Informations d'identification, effectuez l'une des tâches suivantes :

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

   - Dans le cas des iDRACs déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; autrement, configurez les informations d'identification iDRAC plus bas.
     – Entrez le nom de l'utilisateur dans la zone de texte **Nom d'utilisateur Active Directory**. Pour ce faire, utilisez l'un des formats suivants : domaine\nom d'utilisateur ou domaine/nom d'utilisateur ou encore nom

d'utilisateur@domaine. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la documentation Microsoft Active Directory pour connaître les conventions de nom d'utilisateur.

– Entrez le mot de passe dans la zone de texte **Mot de passe Active Directory**. Celui-ci ne doit pas comporter plus de 127 caractères.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat iDRAC et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat, sélectionnez **Désactivé**.

- Pour configurer les références iDRAC sans Active Directory, effectuez les opérations suivantes :

– Dans la zone de texte **Nom d'utilisateur**, entrez le nom de l'utilisateur. Celui-ci ne doit pas comporter plus de 16 caractères. Pour en savoir plus sur les restrictions de nom d'utilisateur de votre version d'iDRAC, reportez-vous à la documentation iDRAC.

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

– Entrez le mot de passe dans la zone de texte **Mot de passe**. Celui-ci ne doit pas comporter plus de 20 caractères.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat iDRAC et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat, sélectionnez **Désactivé**.

6. Cliquez sur **Suivant**.
7. Dans la page Informations d'identification d'hôte, sous Informations d'identification, effectuez l'une des tâches suivantes :

- Dans le cas des hôtes déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; autrement, configurez les références iDRAC plus bas.

– Entrez le nom de l'utilisateur dans la zone de texte **Nom d'utilisateur Active Directory**. Pour ce faire, utilisez l'un des formats suivants : domaine\nom d'utilisateur ou domaine/nom d'utilisateur ou encore nom d'utilisateur@domaine. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la documentation Microsoft Active Directory pour connaître les conventions de nom d'utilisateur.

– Entrez le mot de passe dans la zone de texte **Mot de passe Active Directory**. Celui-ci ne doit pas comporter plus de 127 caractères.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat de l'hôte, sélectionnez **Désactivé**.

- Pour configurer les informations d'identification de l'hôte sans Active Directory, effectuez les opérations suivantes :

– Dans la zone de texte **Nom d'utilisateur**, entrez le nom de l'utilisateur. Le nom d'utilisateur par défaut en lecture seule est root (racine). Si vous sélectionnez l'option **Utiliser Active Directory,** le nom d'utilisateur peut être différent du nom root(racine).

– Entrez le mot de passe dans la zone de texte **Mot de passe**. Celui-ci ne doit pas comporter plus de 127 caractères.

REMARQUE : Les références OMSA sont les mêmes que celles utilisées pour les hôtes ESX et ESXi.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat de l'hôte, sélectionnez **Désactivé**.

8. Cliquez sur **Suivant**.
9. Le lien **Test de connexion** est utilisé pour valider l'iDRAC et les informations d'identification de l'hôte pour les serveurs sélectionnés. Effectuez l'une des opérations suivantes :

   - Pour commencer le test, cliquez sur **Tester sélectionné**. Les autres options sont inactives.
   - Pour arrêter les tests, cliquez sur **Interrompre tous les tests**.

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

10. Pour enregistrer le profil, cliquez sur **Enregistrer**.

    Pour gérer les profils de connexion, voir Gestion des profils de connexion.

Configuration des événements et alarmes

Dell Management Center, sous l'onglet « Événements et alarmes » dans l'option Paramètres active ou désactive toutes les alarmes matérielles. L'état actuel des alertes est affiché dans l'onglet Alarmes vCenter. Un événement critique indique un dysfonctionnement du système ou une perte de données réelle ou imminente. Un événement d'avertissement n'est pas forcément significatif, mais peut indiquer un problème futur éventuel. Les événements et alarmes peuvent également être activés à l'aide de VMware Alarm Manager. Les événements sont affichés dans l'onglet Tâches et événements vCenter de la vue Hôtes et clusters.

REMARQUE : Sur les hôtes antérieurs à Dell PowerEdge de 12e génération, cette fonction exige que l'appliance virtuelle soit configurée comme destination d'interruption dans OMSA afin d'afficher les événements d'hôte dans vCenter. Pour plus d'informations sur OMSA, voir Configuration d'une destination d'interruption OMSA.

Configurez les événements et alarmes à l'aide de l'Assistant Configuration ou depuis Dell Management Center, sous l'onglet "Événements et alarmes" dans l'option "Paramètres" :
Pour configurer les événements et alarmes :

1. Dans **Dell Management Center**, sous **Paramètres** → **Événements et alarmes**, cliquez sur **Modifier**.
2. Sous **Niveaux de publication des événements**, sélectionnez l'une des options suivantes :

   - Ne publier aucun événement : bloquer les événements matériels.
   - Publier tous les événements : publier tous les événements matériels.
   - Publier uniquement les événements critiques et d'avertissement : publier uniquement les événements matériels de niveau critique et d'avertissement.
   - Publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation : publier uniquement les événements critiques et d'avertissement relatifs à la virtualisation ; c'est le niveau de publication d'événement par défaut.

3. Pour activer tous les événements et alarmes matériels, cochez la case **Activer les alarmes d'hôtes Dell**.

   REMARQUE : Les hôtes Dell pour lesquels les alarmes sont activées répondent aux événements critiques en entrant en mode de maintenance.

4. Dans la boîte de dialogue qui s'affiche, cliquez sur **Continuer** pour accepter cette modification ou cliquez sur **Annuler**.
5. Pour restaurer les paramètres d'alarmes vCenter par défaut pour tous les serveurs Dell gérés, cliquez sur **Restaurer les alarmes par défaut**.

   Il peut s'écouler une minute avant que le changement prenne effet.
6. Pour enregistrer, cliquez sur **Enregistrer**.

À propos de la configuration du proxy

Les paramètres du proxy définissent le proxy HTTP et les références requises utilisées pour récupérer des informations à partir du Web (y compris de Dell Online), telles que :

- Activer ou désactiver le serveur proxy
- Entrer le serveur proxy et le numéro de port requis
- Définir les références requises : nom d'utilisateur et mot de passe

Tâches connexes :

- Configuration d'un serveur proxy
- Utilisation du proxy HTTP pour récupérer des données Web
- Configuration du proxy HTTP à l'aide d'Administration Console

Configuration d'un serveur proxy

Configurez le serveur proxy dans l'Assistant Configuration ou plus tard avec l'option Paramètres, Proxy.

REMARQUE : Les mots de passe de proxy ne peuvent pas dépasser 31 caractères.

Pour configurer un serveur proxy :

1. Dans Dell Management Center, sélectionnez **Paramètres** → **Proxy**, puis cliquez sur **Modifier**.
2. Dans la fenêtre **Proxy HTTP**, procédez comme suit :
   - Pour ne pas utiliser un serveur proxy, cliquez sur **Enregistrer et continuer**.
   - Pour utiliser un serveur proxy, sous **Paramètres** entrez une **adresse de serveur proxy**.
3. Entrez le **numéro de port proxy**.
4. Sélectionnez la case **Références requises** le cas échéant.
5. Si vous avez sélectionné **Références requises**, procédez comme suit :
   a. Dans la zone de texte **Nom d'utilisateur proxy**, entrez le nom d'utilisateur proxy.
   b. Dans la zone de texte **Mot de passe proxy**, entrez le mot de passe proxy.
   c. Dans la zone de texte **Vérifier le mot de passe proxy**, entrez à nouveau le mot de passe proxy.
6. Sous **Proxy**, cochez la case **Utiliser le proxy**.
7. Pour enregistrer ces options, cliquez sur **Enregistrer**.

Utilisation du proxy HTTP pour récupérer des données Web

Pour utiliser le proxy HTTP pour récupérer des données Web :

1. Dans le **Dell Management Center**, sélectionnez **Paramètres** → **Proxy HTTP**, puis cliquez sur **Modifier**.
2. Cochez la case **Utiliser Proxy**.

3. Cliquez sur **Appliquer**.
4. Pour valider les paramètres, cliquez sur **Tester la connectivité**.

Exécution de tâches d'inventaire

Pour exécuter une tâche d'inventaire :

1. À la fin de l'**Assistant Configuration**, cliquez sur **File d'attente des tâches → Inventaire → Exécuter maintenant**pour exécuter immédiatement une tâche d'inventaire.
2. Pour afficher l'état de la tâche d'inventaire, cliquez sur **Actualiser**.
3. Accédez à la vue **Hôtes et clusters** , cliquez sur un **hôte Dell**, puis cliquez sur l'onglet **OpenManage Integration**. Les infos suivantes devraient être disponibles :

   - Page Vue générale
   - Journal des événements système
   - Inventaire matériel
   - Stockage
   - Micrologiciel
   - Surveillance de l'alimentation
   - État de la garantie

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

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

   - Faire clignoter le voyant
   - Exécuter l'Assistant Mise à jour du micrologiciel
   - Lancer Remote Access
   - Lancer OMSA
   - Lancer CMC

Exécution d'une tâche de récupération de la garantie

La configuration de la tâche de récupération de garantie est similaire dans l'Assistant et à partir de l'option **Dell Mangement Center → Paramètres**. Après avoir exécuté l'Assistant, vous pouvez effectuer des modifications à tout moment à partir de la page **Dell Management Center → Settings → Planification de la garantie**. Vous pouvez exécuter la tâche de récupération de garantie dès maintenant à partir de la page **File d'attente des tâches → Historique de garantie**.

Pour planifier une tâche de récupération de la garantie :

1. Dans le **Dell Management Center**, sélectionnez **Paramètres → Planification de la garantie.**
2. Dans la fenêtre **Planification de la garantie**, cliquez sur **Modifier**.
3. Pour configurer la planification, procédez ainsi :
   a. Pour exécuter des planifications de garantie, cliquez sur **Les jours sélectionnés**.
   b. Pour ne pas exécuter de planifications de garantie, sélectionnez **Ne pas exécuter d'inventaire sur les hôtes Dell**.
4. Si vous avez sélectionné **Les jours sélectionnés**, procédez ainsi :
   a. Cochez la case en regard de chaque jour de la semaine où vous voulez exécuter les tâches de garantie.
   b. Dans la zone de texte, entrez l'heure au format HH:MM.

L'heure entrée est votre heure locale. Calculez la différence d'heure requise pour exécuter les tâches de garantie à l'heure voulue.

5. Pour exécuter les tâches de garantie maintenant, allez à **File d'attente des tâches** → **Historique de la garantie**, puis cliquez sur **Exécuter maintenant**.

Afficher ou modifier les références de déploiement

Dans Dell Management Center, vous pouvez modifier les références de déploiement. Les références de déploiement sont utilisées pour communiquer de manière sécurisée avec un système sans système d'exploitation en utilisant l'iDRAC de la découverte initiale, jusqu'à la fin du processus de déploiement. Une fois le déploiement terminé, les références sont remplacées par celles du profil de connexion correspondant au système sans système d'exploitation de l'Assistant de déploiement. Si les références de déploiement sont modifiées, tous les systèmes nouvellement découverts à partir de ce moment-là seront dotés des nouvelles références ; les références sur les serveurs découverts avant le changement des références ne sont pas touchées par ce changement. Le nom d'utilisateur doit comporter 16 caractères maximum (uniquement des caractères ASCII imprimables). Le mot de passe doit comporter 20 caractères maximum (uniquement des caractères ASCII imprimables).
Pour modifier les références de déploiement :

1. Dans **Dell Management Center** → **Paramètres** → **Références de déploiement**, cliquez sur **Modifier**.
2. Dans **Références de déploiement de serveur sans système d'exploitation**, sous **Références**, procédez ainsi :
   - Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
     Le nom d'utilisateur doit comporter 16 caractères maximum (uniquement des caractères ASCII imprimables)
   - Dans la zone de texte **Mot de passe**, entrez le mot de passe.
     Le mot de passe doit comporter 20 caractères maximum (uniquement des caractères ASCII imprimables)
   - Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe.
     Les mots de passe doivent concorder.
3. Cliquez sur **Appliquer**.

Configuration de l'espace de stockage du micrologiciel

Pour configurer les références et l'espace de stockage du micrologiciel :

1. Dans l' **OpenManage Integration for VMware vCenter** , sélectionnez **Paramètres** → **Espace de stockage du micrologiciel** puis cliquez sur **Modifier**.
2. Sur la page **Espace de stockage du micrologiciel**, pour choisir l'espace de stockage par défaut pour les mises à jour du micrologiciel, sélectionnez l'une des options suivantes :
   - **Dell Online**
     Cette option utilise l'espace de stockage de mise à jour du micrologiciel par défaut de Dell en ligne (ftp.dell.com) avec un dossier intermédiaire requis. L'OpenManage Integration for VMware vCenter télécharge les mises à jour du micrologiciel sélectionnées et les stocke dans le dossier intermédiaire, en attendant leur application.
   - **Dossier de réseau partagé**
     Les hôtes utilisant le Lifecycle Controller peuvent effectuer des mises à jour à partir d'un espace de stockage personnalisé qui est hébergé sur un dossier réseau partagé accessible. Pour créer un espace de stockage personnalisé, Dell recommande l'utilisation du Dell Repository Manager. Celui-ci vous permet de le créer, puis de l'enregistrer à un emplacement partagé auquel les hôtes et OpenManage Integration peuvent accéder. Indiquez l'emplacement du fichier de catalogue de l'espace de stockage ci-dessous.
3. Si vous avez sélectionné **Dossier de réseau partagé** entrez l'intégralité de la section du fichier de catalogue dans le champ **Emplacement du fichier de catalogue**

4. Cliquez sur **Lancer le test**.
5. Cliquez sur **Appliquer**.

Paramètres de sécurité des serveurs de déploiement

Vous pouvez restreindre l'ensemble de serveurs déployables en utilisant une liste blanche. Si un serveur est dans la liste blanche, il est doté de références au cours du processus de découverte automatique et d'établissement d'une liaison et est affiché dans la liste des serveurs utilisés pour le déploiement. La liste blanche est maintenue manuellement en ajoutant les numéros de service de serveur, supprimant les numéros de service, ou important une liste de numéros de service à partir d'un fichier CSV.

REMARQUE : Utilisez un fichier CSV pour importer des serveurs. Celui-ci contient des enregistrements multiples sur des lignes différentes, où chaque enregistrement a un ou plusieurs numéros de service séparés par des virgules.

Pour configurer et gérer des listes blanches, choisissez l'une des options suivantes :

- Activation d'une liste blanche de serveurs
- Ajout de serveurs à une liste blanche
- Suppression de serveurs d'une liste blanche

Activation d'une liste blanche de serveurs déployables

Pour plus d'informations à propos des paramètres de sécurité des serveurs déployables, voir Paramètres de sécurité de déploiement.

Pour activer une liste blanche de serveurs :

1. Dans **Dell Management Center**, dans le volet gauche, sélectionnez **Paramètres**.
2. Dans le volet droit, sélectionnez **Sécurité**.
3. Dans la fenêtre **Sécurité**, cliquez sur **Modifier**.
4. Pour utiliser la liste blanche pour restreindre le déploiement de serveurs, sélectionnez la case **Utiliser la liste blanche de serveurs**.
5. Cliquez sur **Appliquer** et le paramètre de la liste blanche de serveurs passe à ACTIVÉ.

Ajout de serveurs déployables à une liste blanche

Pour plus d'informations sur les paramètres de sécurité des serveurs déployables, consultez Paramètres de sécurité serveur pour le déploiement. Lorsque ces paramètres sont appliqués, seuls les serveurs Dell qui figurent sur la liste blanche des serveurs sont disponibles pour le déploiement à l'aide de l'OpenManage Integration for VMware vCenter. Vous pouvez ajouter manuellement des serveurs déployables à une liste blanche ou les importer à l'aide d'une liste.

Pour ajouter des serveurs déployables à une liste blanche :

1. Dans **Dell Management Center**, dans le volet gauche, sélectionnez **Paramètres** → **Sécurité**.
2. Dans la fenêtre **Liste blanche des serveurs**, cliquez sur **Modifier**, puis procédez ainsi :
   - Pour ajouter manuellement des serveurs à la liste blanche, cliquez sur **Ajouter un serveur.**
     - Dans la boîte de dialogue **Ajouter des numéros de service**, entrez les numéros de service.
     - Pour ajouter les numéros, cliquez sur **Continuer**.
   - Pour importer une liste de numéros de service, cliquez sur **Importer une liste blanche**.
     - À l'affichage de la boîte de dialogue **Sélectionner le fichier à charger**, accédez au fichier CSV et cliquez sur **Ouvrir**.

       Pour un exemple de liste blanche :

       ASDFG12

SDCNRD0

TESCVD3

AS243AS, ASWERF3, FGVCSD9

– À l'affichage de la boîte de dialogue **Nous avons trouvé ces numéros de service dans votre fichier**, cliquez sur **Appliquer**.

Les numéros de service sont maintenant affichés dans la liste Numéros de service.

Suppression des serveurs déployables d'une liste blanche

Pour plus d'informations à propos des paramètres de sécurité des serveurs déployables, voir Paramètres de sécurité de déploiement.

Pour supprimer des serveurs déployables d'une liste blanche :

1. Dans **Dell Management Center**, dans le volet gauche, sélectionnez **Paramètres**.
2. Dans le volet droit, sélectionnez **Sécurité**.
3. Dans la fenêtre **Sécurité** , cliquez sur **Modifier**.
4. Effectuez l'une des opérations suivantes :
   - Pour supprimer un serveur particulier, cochez la case **Numéro de service**, puis cliquez sur **Supprimer les éléments sélectionnés**.
   - Pour supprimer un serveur particulier, cochez la case **Numéro de service**, puis cliquez sur **Supprimer les éléments sélectionnés**.
5. À l'affichage de la boîte de dialogue **Voulez-vous vraiment supprimer les numéros de service sélectionnés ?**, cliquez sur **Appliquer** ou cliquez sur **Annuler** pour annuler.
6. Pour appliquer les modifications, cliquez sur **Appliquer**.

À propos des problèmes de conformité d'hôte, serveur sans système d'exploitation et iDRAC

Pour gérer les hôtes, serveurs sans système d'exploitation et iDRAC avec le OpenManage Integration for VMware vCenter ceux-ci doivent satisfaire certains critères minimum. S'ils ne sont pas conformes, ils ne sont pas gérés correctement par le OpenManage Integration for VMware vCenter. Utilisez les liens Corriger la conformité des hôtes, Serveur sans système d'exploitation et conformité de l'iDRAC pour afficher les éléments de votre configuration qui ne sont pas conformes et les corriger. Cet Assistant affiche les hôtes, serveurs sans système d'exploitation et iDRAC répondant aux cas suivants :

- Les hôtes n'ont pas été associés à un profil de connexion.

  Si un profil de connexion n'est pas attribué à un hôte, une boîte de dialogue se propose de vous conduire à l'écran Profil de connexion. Cette configuration se situe en dehors de l'Assistant. Revenez ultérieurement pour exécuter cet Assistant.
- Collecte de l'inventaire du système au redémarrage (CSIOR) est désactivé ou n'a pas été exécuté, ce qui nécessite un redémarrage manuel.
- L'agent OMSA (Informations d'identification de racine hôte) n'est pas installé, est obsolète ou n'est pas correctement configuré.
- Les serveurs sans système d'exploitation ont des versions périmées du micrologiciel d'Integrated Dell Remote Access Controller (iDRAC), du micrologiciel de Lifecycle Controller (LC) ou du BIOS.

PRÉCAUTION : Les hôtes en mode verrouillage n'apparaissent pas dans les contrôles de conformité, même s'ils ne sont pas conformes. Ils ne s'affichent pas parce que leur état de conformité ne peut pas être déterminé. Vérifiez la conformité de ces systèmes manuellement. Le cas échéant, un avertissement s'affiche.

Dans chaque cas, vous devez corriger les problèmes de conformité en exécutant une des opérations suivantes :

- Pour corriger les problèmes de conformité des hôtes vSphere, voir Exécution de l'Assistant Correction des hôtes vSphere non conformes.
- Pour corriger les problèmes de conformité des serveurs sans système d'exploitation, voir Exécution de l'Assistant Correction des serveurs sans système d'exploitation non conformes.
- Pour corriger les problèmes de conformité des iDRAC : Conformité de licence iDRAC.

Informations connexes :

- Revérification de la conformité des serveurs sans système d'exploitation
- Téléchargement d'un ISO pour les mises à jour manuelles du micrologiciel

Exécution de l'Assistant Correction des hôtes vSphere non conformes

Exécutez l'Assistant Correction des hôtes vSphere non conformes pour corriger les hôtes non conformes. Pour plus d'informations sur la conformité, voir À propos des problèmes de conformité des hôtes et des serveurs sans système d'exploitation. Certains hôtes ESXi non conformes exigent un redémarrage. Le redémarrage d'un hôte ESXi est requis si OMSA (OpenMange Server Administrator) doit être installé ou mis à jour. De plus, un redémarrage est requis sur tout hôte qui n'a jamais exécuté CSIOR. Si vous choisissez de redémarrer automatiquement un hôte ESXi, les actions suivantes sont effectuées :

- Pour une correction de l'état CSIOR :

  Si la fonction CSIOR n'est pas activée sur l'hôte, CSIOR est configuré sur *ON* sur l'hôte, et l'hôte est configuré en mode de maintenance et redémarré.

- Pour une correction de l'état OMSA :

  a. OMSA est installé sur l'hôte.
  b. L'hôte est configuré en mode de maintenance et redémarré.
  c. À la fin du redémarrage, OMSA est configuré pour que les modifications s'appliquent.
  d. L'hôte sort du mode de maintenance.
  e. L'inventaire est exécuté pour actualiser les données.

Pour exécuter l'Assistant Correction des hôtes vSphere non conformes :

1. Dans **Dell Management Center**, dans le volet gauche, cliquez sur **Conformité** → **Hôtes vSphere**.
2. Dans la fenêtre **Conformité des hôtes vSphere**, examinez les hôtes non conformes, puis cliquez sur **Corriger les hôtes vSphere non conformes**.
3. Dans l'Assistant **Correction des hôtes vSphere non conformes**, sélectionnez les cases correspondant aux hôtes à corriger.
4. Cliquez sur **Suivant**.
5. Si un serveur n'a pas de profil de connexion, vous avez la possibilité de quitter l'Assistant et de corriger ces systèmes depuis la page **Profil de connexion** ou de continuer cet Assistant. Voir Création d'un nouveau profil de connexion. Une fois terminé, retournez à cet Assistant.
6. Dans la fenêtre **Activer CSIOR**, sélectionnez les cases pour activer **CSIOR** pour les hôtes sélectionnés.
7. Cliquez sur **Suivant**.
8. Dans la fenêtre **Corriger OMSA**, cochez les cases pour corriger **OMSA** pour les hôtes sélectionnés.
9. Cliquez sur **Suivant**.
10. Dans la fenêtre **Redémarrer les hôtes**, examinez les hôtes ESXi à redémarrer. Le redémarrage d'un hôte ESXi est requis si OMSA doit être installé ou mis à jour. De plus, un redémarrage est requis sur tout hôte qui n'a jamais exécuté CSIOR. Procédez ainsi :

    - Si vous voulez mettre automatiquement les hôtes en mode de maintenance et les redémarrer au besoin, sélectionnez la case **Mettre automatiquement les hôtes en mode de maintenance et les redémarrer au besoin**.

- Si vous voulez redémarrer manuellement, vous devez procéder ainsi :
    1. Lorsque la tâche *Installer OMSA* est terminée pour un hôte, redémarrez l'hôte.
    2. Lorsque l'hôte est redémarré, si OMSA n'est pas configuré, configurez OMSA manuellement ou utilisez l'Assistant Conformité.
    3. Réexécutez l'inventaire. Voir Exécution de tâches d'inventaire.

11. Cliquez sur **Suivant**.
12. Dans la fenêtre **Récapitulatif**, examinez les actions qui ont lieu sur les hôtes non conformes. Des redémarrages manuels sont requis pour qu'elles s'appliquent.
13. Cliquez sur **Terminer**.

Exécution de l'Assistant Correction des serveurs sans système d'exploitation non conformes

Exécutez l'Assistant Correction des serveurs sans système d'exploitation non conformes pour corriger les serveurs sans système d'exploitation non conformes. Pour plus d'informations sur la conformité, voir À propos des problèmes de conformité des hôtes et des serveurs sans système d'exploitation.

Exécution de l'Assistant Correction des serveurs sans système d'exploitation non conformes

1. Dans **Dell Management Center**, dans le volet gauche, cliquez sur **Conformité → Serveurs sans système d'exploitation**.
2. Dans la fenêtre **Serveurs sans système d'exploitation**, examinez les hôtes non conformes, puis cliquez sur **Corriger les serveurs sans système d'exploitation non conformes**.
3. Dans l'Assistant **Correction des serveurs sans système d'exploitation non conformes**, sélectionnez les cases correspondant aux hôtes à corriger.
4. Cliquez sur **Suivant**.
5. Dans la fenêtre **Récapitulatif**, examinez les actions qui ont lieu sur les serveurs sans système d'exploitation non conformes
6. Cliquez sur **Terminer**.

Revérification de la conformité des serveurs sans système d'exploitation

Pour les serveurs que vous avez corrigés en dehors de l'OpenManage Integration for VMware vCenter, vous devez exécuter cette revérification manuelle de la conformité des serveurs. Elle se trouve sur la page Dell Management Center, Conformité, Serveurs sans système d'exploitation.

Pour revérifier la conformité des serveurs sans système d'exploitation :

1. Sur la page **Dell Management Center → Conformité → Serveurs sans système d'exploitation**, cliquez sur **Revérifier la conformité**.
2. Dans la fenêtre **Serveurs non conformes**, pour actualiser la liste, cliquez sur **Actualiser**.
3. Pour exécuter la revérification, cliquez sur **Vérifier la conformité**.
4. Pour abandonner la revérification, cliquez sur **Interrompre tous les tests**.
5. Si vous avez réussi à corriger le système, la liste est actualisée et le système est supprimé de la liste. Sinon, le système non conforme reste sur la liste.
6. Après avoir terminé, cliquez sur **Terminé**.

Téléchargement d'un ISO pour les mises à jour manuelles du micrologiciel

Le OpenManage Integration for VMware vCenter corrige automatiquement la plupart des problèmes de conformité. Une installation ISO manuelle est parfois requise. Vous pouvez télécharger l'ISO nécessaire pour corriger la conformité manuellement en suivant les étapes ci-après :

1. Sur la page **Dell Management Center** → **Conformité** → **Serveurs sans système d'exploitation**, pour télécharger une image ISO, cliquez sur **Télécharger une image ISO**.
2. Dans la boîte de dialogue **Télécharger une image ISO**, pour trouver l'emplacement de l'ISO, cliquez sur **Télécharger**.

   REMARQUE : Le navigateur externe peut s'ouvrir derrière cette fenêtre d'application.
3. Allez jusqu'au fichier ISO requis pour que votre serveur sans système d'exploitation soit conforme.
4. Gravez ce fichier ISO, démarrez l'hôte par l'intermédiaire de ce fichier ISO, puis mettez à jour les composants micrologiciels au niveau requis.

Conformité à la licence iDRAC

Lorsque vous sélectionnez la page Conformité de licence iDRAC, un test de conformité est effectué. Ce test dure quelques minutes. Les hôtes vSphere et serveurs sans système d'exploitation figurant sur cette page ne sont pas conformes, car ils n'ont pas de licence iDRAC compatible. Le tableau affiche l'état de la licence iDRAC. Sur cette page vous pouvez voir le nombre de jours restants sur votre licence et effectuer une mise à jour au besoin. Si le lien *Exécuter une tâche d'inventaire* est désactivé, cela signifie qu'aucun hôte vSphere n'est pas conforme en raison de la licence iDRAC. Si le lien *Revérifier la conformité des serveurs sans système d'exploitation* est désactivé, cela signifie qu'aucun serveur sans système d'exploitation n'est pas conforme en raison de la licence iDRAC.

1. Dans le volet gauche de **Dell Management Center**, cliquez sur **Conformité**.
2. Développez **Conformité**, puis cliquez sur **Licence iDRAC**.

   Lorsque vous arrivez sur cette page, le test de conformité est exécuté. Il s'agit du test qui est exécuté lorsque vous cliquez sur **Actualiser**.
3. Si votre licence est périmée, cliquez sur **Acheter/Renouveler une licence iDRAC**.
4. Connectez-vous à la page **Gestion de licences Dell** et mettez à jour ou achetez une nouvelle licence iDRAC.

   Utilisez les informations sur cette page pour identifier et mettre à jour votre iDRAC.
5. Après avoir installé une licence iDRAC, exécutez une tâche d'inventaire pour les hôtes vSphere et revenez sur cette page à la fin de celui-ci. Pour les serveurs sans système d'exploitation, revérifiez la conformité des serveurs sans système d'exploitation sous licence.

Mise à niveau de l'OpenManage Integration for VMware vCenter

Ce qui suit est le scénario de mise à niveau de l' OpenManage Integration for VMware vCenter :

- Mise à niveau d'une version d'évaluation à une version complète du produit

REMARQUE : Effectuez une sauvegarde de l'appliance avant de commencer la mise à niveau. Voir Exécution d'une sauvegarde immédiate.

Mise à niveau d'une version d'évaluation à une version complète du produit

Pour effectuer une mise à niveau d'une version d'évaluation à la version complète du produit :

1. Allez sur le **site Web Dell** et achetez la version complète du produit.

Vous pouvez également accéder au site Web de Dell à l'aide de OpenManage Integration for VMware vCenter à l'aide de l'un des liens **Acheter maintenant** , tels que celui qui se trouve dans la fenêtre d'administration sur le portail **de licences**. Ceci s'applique uniquement lorsque vous utilisez des licences d'évaluation.

2. Le téléchargement inclut la nouvelle version complète du produit et un nouveau fichier de licence.
3. Ouvrez une fenêtre de navigateur et entrez l'**URL de l'Administration Console** affiché dans l'**onglet vSphere vCenter Console** de la machine virtuelle que vous voulez configurer ou utilisez le lien de la page **Dell Management Console → Paramètres**. L'URL se conforme au format suivant et est sensible à la casse : **https://<Adresse IP de l'appliance>**
4. Dans la **fenêtre de connexion d'Administration Console**, entrez le mot de passe et cliquez sur **Connexion**.
5. Pour charger le fichier de licence, cliquez sur **Charger**.
6. Dans la fenêtre **Télécharger une licence**, cliquez sur **Parcourir** pour accéder au fichier de licence.
7. Sélectionnez le fichier de licence et cliquez sur **Téléverser**.

À propos des licences OpenManage Integration for VMware vCenter

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

Licence d'évaluation	La version d'essai contient une licence d'évaluation pour cinq hôtes (serveurs) gérés par l'OpenManage Integration for VMware vCenter. Ceci ne s'applique qu'aux serveurs de 11e génération et de générations ultérieures. Il s'agit d'une licence par défaut valide uniquement pendant la période d'essai de 90 jours.
Licence standard	La version complète du produit contient une licence standard pour jusqu'à dix vCenters et vous pouvez acheter n'importe quel nombre de connexions hôtes gérées par l'OpenManage Integration for VMware vCenter.

Lorsque vous effectuez une mise à niveau d'une licence d'évaluation à une licence standard complète, un nouveau fichier XML de licence ainsi que le fichier Zip contenant le fichier de licence à télécharger vous sont envoyés par courrier électronique. Enregistrez ce fichier sur votre système local et chargez le fichier de la nouvelle licence à l'aide de l'Administration Console. Les licences offrent les informations suivantes :

- Licences de connexions vCenter maximales : jusqu'à trois connexions vCenter enregistrées et utilisées sont autorisées.
- Licences de connexions hôte maximales : nombre de connexions hôte achetées.
- En cours d'utilisation : le nombre de connexions vCenter ou connexions hôte utilisées. Pour les connexions hôte, ce nombre représente le nombre d'hôtes (ou serveurs) découverts et inventoriés.
- Disponibles : le nombre de licences de connexions vCenter ou connexions hôte disponibles pour un usage ultérieur.
- Hôtes hors licence : le nombre de connexions hôtes qui dépassent la quantité sous licence. L'OpenManage Integration for VMware vCenter continue à fonctionner normalement, mais une nouvelle licence doit être achetée et installée pour résoudre cet avertissement.

4

Gestion matérielle de bout en bout

L'objectif de la gestion matérielle de bout en bout est de fournir l'état d'intégrité du système et des informations actualisées sur l'infrastructure dont l'administrateur a besoin pour répondre à des événements matériels critiques sans quitter le Dell Management Center ou vCenter. La gestion matérielle de bout en bout dans l'OpenManage Integration for VMware vCenter comprend quatre parties :

- Surveillance
- Inventaire
- Gestion d'hôte avancée
- Récupération de la garantie

Surveillance du Datacenter et du système hôte

Le contrôle des données et du système hôte, permet à l'administrateur de surveiller l'intégrité de l'infrastructure en affichant le matériel (serveurs et stockage) et les événements relatifs à la virtualisation dans l'onglet Tâches et événements de vCenter. En outre, les alertes matérielles peuvent déclencher les alarmes d'OpenManage Integration for VMware vCenter. Peu d'alarmes définies pour les événements relatifs à la virtualisation peuvent faire basculer le système hôte en mode de maintenance.

Pour exécuter la surveillance :

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

Comprendre les événements et alarmes

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

Il existe quatre niveaux de publication d'événement.

Tableau 1. Description des niveaux de publication d'événement

Événement	Description
Ne pas publier d'événement	Ne faites pas en sorte que l'OpenManage Integration for VMware vCenter transfère les événements ou alertes dans les vCenters associés.
Publier tous les événements	Publier tous les événements, notamment les événements non formels, que l'OpenManage Integration for VMware

	vCenter reçoit des hôtes Dell gérés dans les vCenters associés.
Publier uniquement les événements critiques et d'avertissement	Publier uniquement les événements de criticité 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.

Vous pouvez activer vos événements et alarmes lorsque vous les configurez. Lorsqu'elles sont activées, les alarmes matérielles critiques peuvent amener OpenManage Integration for VMware vCenter à mettre le système hôte en mode de maintenance, et dans certains cas, migrer les machines virtuelles vers un autre système hôte. L'OpenManage Integration for VMware vCenter transmet les événements reçus des hôtes Dell gérés et crée des alarmes pour ces événements. Utilisez ces alarmes pour déclencher des actions depuis le vCenter, comme un redémarrage, un mode de maintenance ou une migration. Par exemple, quand un double bloc d'alimentation tombe en panne et qu'une alarme est créée, l'action qui en résulte consiste à migrer la machine virtuelle sur cette machine vers une nouvelle machine.

Un hôte entre ou quitte le mode de maintenance seulement lorsque vous le demandez. Si l'hôte est dans un cluster lorsqu'il entre en mode de maintenance, vous avez la possibilité d'évacuer les machines virtuelles hors tension. Si cette option est sélectionnée, chaque machine virtuelle hors tension est migrée vers un autre hôte, à moins qu'il n'existe aucun hôte compatible disponible pour la machine virtuelle dans le cluster. En mode de maintenance, l'hôte ne permet pas le déploiement ou la *mise sous tension* d'une machine virtuelle. Les machines virtuelles qui s'exécutent sur un hôte entrant en mode de maintenance doivent être migrées vers un autre hôte ou arrêtées, manuellement ou automatiquement par VMware Distributed Resource Scheduling (DRS).

Les hôtes situés en dehors de clusters, ou dans des clusters où VMware Distributed Resource Scheduling (DRS) n'est pas activé, pourraient voir les machines virtuelles arrêtées en raison d'un événement critique. DRS surveille en permanence l'utilisation dans un pool de ressources et répartit intelligemment les ressources disponibles entre les machines virtuelles en fonction des besoins commerciaux. Utilisez les clusters avec DRS configuré en conjonction avec les alarmes Dell afin de vous assurer que les machines virtuelles sont automatiquement migrées en cas d'événements matériels critiques. Dans les détails du message à l'écran apparaissent les clusters sur cette instance vCenter qui pourraient être touchés. Confirmez que les clusters sont touchés avant d'activer événements et alarmes.

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

REMARQUE : Pour recevoir des événements Dell, vous devez activer les événements.

REMARQUE : L'OpenManage Integration for VMware vCenter pré-sélectionne les événements relatifs à la virtualisation qui sont essentiels pour que les hôtes exécutent avec succès des machines virtuelles. Les alarmes d'hôtes Dell sont désactivées par défaut. Si les alarmes Dell sont activées, les clusters doivent utiliser VMware Distributed Resource Scheduler pour que les machines virtuelles qui envoient des événements critiques soient automatiquement migrées.

Comprendre l'agent OMSA sur les hôtes Dell PowerEdge de11e génération

Sur les serveurs PowerEdge antérieurs aux serveurs de 12e génération, vous devez installer OMSA pour pouvoir utiliser le OpenManage Integration for VMware vCenter. L'agent OMSA est installé automatiquement sur les hôtes Dell PowerEdge de11e génération lors du déploiement mais vous pouvez également l'installer manuellement si vous le souhaitez.

REMARQUE : Lors du déploiement de l'agent OMSA, le OpenManage Integration for VMware vCenter démarre le service httpClient et active le port 8080 (pour les versions ultérieures à ESXi 5.0) pour télécharger le VIB OMSA et l'installer. Une fois l'installation d'OMSA terminée, le service s'arrête automatiquement et le port se ferme.

Pour configurer OMSA sur les serveurs Dell PowerEdge 11e génération, choisissez l'une des opérations suivantes :

- Déploiement d'un agent OMSA sur un système ESXi
- Déploiement d'un agent OMSA sur un système ESX
- Configuration d'une destination d'interruption OMSA

Déploiement de l'agent OMSA sur un système ESX

Installez le fichier tar.gz OMSA sur un système ESX pour rassembler les informations d'inventaire et d'alerte des systèmes.

REMARQUE : Des agents OpenManage doivent être installés sur les hôtes Dell antérieurs aux serveurs Dell PowerEdge de 12e génération. Installez OMSA à l'aide d'OpenManage Integration for VMware vCenter ou installez-le manuellement sur les hôtes avant d'installer l'OpenManage Integration for VMware vCenter. Vous trouverez des informations détaillées sur l'installation manuelle des agents à l'adresse **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

Pour déployer le fichier tar.gz de l'agent OMSA sur un système ESX avec le paramètre d'activation à distance requis (-c) :

1. Exécutez le script d'installation de l'agent OMSA :
   ```
   srvadmin-install.sh -x -c
   ```
2. Démarrez les services OMSA :
   ```
   srvadmin-services.sh start
   ```
3. Si l'agent OMSA est déjà installé, assurez-vous qu'il possède une option d'activation à distance (-c) ; sinon, l'installation de l'OpenManage Integration for VMware vCenter échouera. Réinstallez-le avec l'option -c et redémarrez le service :
   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

Déploiement d'un agent OMSA sur un système ESXi

Installez le VIB OMSA sur un système ESXi pour rassembler les informations d'inventaire et d'alerte des systèmes.

REMARQUE : Des agents OpenManage doivent être installés sur les hôtes Dell antérieurs aux serveurs Dell PowerEdge de 12e génération. Installez OMSA à l'aide d'OpenManage Integration for VMware vCenter ou installez-le manuellement sur les hôtes avant d'installer l'OpenManage Integration for VMware vCenter. Vous trouverez des informations détaillées sur l'installation manuelle des agents à l'adresse **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. S'il n'est pas installé, installez l'outil de ligne de commande vSphere (vSphere CLI) depuis **http://www.vmware.com**.
2. Entrez la commande suivante :
   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
   ```

   REMARQUE : L'installation d'OMSA peut prendre quelques minutes. Cette commande exige le redémarrage de l'hôte lorsqu'elle est terminée.

Configuration d'une destination d'interruption OMSA

L'agent OMSA doit être configuré sur tous les hôtes de 11e génération.

REMARQUE : OMSA est requis uniquement sur les serveurs Dell antérieurs aux serveurs Dell PowerEdge 12G.

Pour configurer une destination d'interruption OMSA :

1. Utilisez le lien vers l'interface utilisateur OMSA qui se trouve dans **Paramètres** → **Général**, ou naviguez vers l'agent OMSA depuis un navigateur Web (**https://<IP de l'hôte>:1311/**).
2. Connectez-vous à l'interface, et sélectionnez l'onglet **Gestion des alertes** .
3. Sélectionnez **Actions d'alerte** et vérifiez que tous les événements à surveiller ont l'option **Message à diffuser** configurée, pour que les événements soient envoyés.
4. Sélectionnez l'option **Événements de plate-forme** en haut de l'onglet.
5. Cliquez sur le bouton gris **Configurer les destinations**, puis cliquez sur le lien **Destination**.
6. Cochez la case **Activer la destination**.
7. Entrez l'adresse IP de l'appliance OpenManage Integration for VMware vCenter dans le champ **Adresse IP de destination** .
8. Cliquez sur **Appliquer les changements**.
9. Répétez les étapes 1 à 8 pour configurer d'autres événements.

Affichage des événements

Pour afficher les événements, procédez comme suit :

- Naviguez vers la machine virtuelle et cliquez droit pour afficher l'onglet **vCenter** → **Tâches et événements** et cliquez sur **Événements** pour afficher le niveau d'événement sélectionné.
- Cliquez sur le nœud parent (cluster ou centre de données) de l'hôte ou le dossier racine du vCenter.

Les événements apparaissent uniquement sur ces nœuds dans l'arborescence vSphere.

Présentation de vSphere Client Host

Cette présentation fournit des informations sur les principaux attributs du serveur hôte, y compris des informations sur l'intégrité de ses composants individuels, l'identification, l'hyperviseur et le micrologiciel.

INTÉGRITÉ DES COMPOSANTS MATÉRIELS

L'intégrité des composants est une représentation graphique de l'état de tous les principaux composants du serveur hôte : châssis du système, bloc d'alimentation, température, ventilateurs, tension, processeurs, batteries, intrusion, journal matériel, gestion de l'alimentation, et mémoire. Les états possibles sont les suivants :

- 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

L'état d'intégrité général est affiché sur la barre d'en-tête en haut à droite.

INFORMATIONS SUR LE SERVEUR

Les informations sur le serveur fournissent les références d'identification, d'hyperviseur et de micrologiciel, telles que :

- Nom d'hôte, état d'alimentation, IP d'iDRAC, IP de console, profil de connexion utilisé, modèle, numéro de service et numéro d'inventaire, nombre de jours restants sous garantie, et date de la dernière analyse d'inventaire.
- Versions d'hyperviseur, de micrologiciel BIOS et de micrologiciel iDRAC.
- Les dix dernières entrées du journal des événements système. Cliquez sur Détails pour ouvrir la fenêtre Journal des événements système qui affiche des détails supplémentaires du journal.

Informations sur l'hôte

Dans le volet gauche de présentation de l'hôte, vous pouvez trouver les liens vers les types d'informations sur l'hôte suivants :

- Journal des événements système

  Affiche les informations du journal des événements système matériels. Voir Comprendre les journaux des événements système.
- Inventaire matériel

  Affiche des informations sur les périphériques matériels suivants :

  – Les unités remplaçables sur site (Field Replaceable Unit — FRU) telles que modules DIMM, planaire système, blocs d'alimentation, fonds de panier, cartes contrôleur, etc.
  – Mémoire : nombre d'emplacements disponibles et utilisés, capacité maximale et quantité de mémoire utilisée, et détails sur les modules DIMM individuels.
  – NIC (Cartes réseau) : nombre de cartes installées et détails sur les cartes individuelles.
  – Emplacements PCI : nombre total d'emplacements disponibles et utilisés, et détails sur les emplacements individuels.
  – Blocs d'alimentation : nombre actuel et détails sur les blocs d'alimentation individuels.
  – Processeurs : nombre actuel et détails sur les processeurs individuels.
  – RAC (Carte d'accès à distance) : adresse IP, type de RAC et URL d'interface Web.

  Voir À propos des tâches d'inventaire.
- Stockage

  Le stockage du système hôte fournit une vue graphique et détaillée de la capacité et du type de stockage physique et logique pour le stockage connecté à un contrôleur de stockage hôte, y compris :

  – Stockage total du système hôte, non configuré, configuré, et capacité de disques de secours globaux et dédiés
  – Liste du nombre de chaque composant de stockage présent dans la table de données des composants du système qui contient des informations détaillées sur ce composant
- Micrologiciel

  Exécution de l'Assistant Mise à jour du micrologiciel ou affichage de votre version du micrologiciel. Voir Mises à jour du micrologiciel.
- Surveillance de l'alimentation

  La surveillance de l'alimentation du système hôte fournit des informations générales sur l'alimentation, des statistiques sur l'énergie, et des informations sur l'alimentation de réserve, y compris :

  – Budget de puissance actuel, profil, seuils d'avertissement et de panne
  – Statistiques sur la consommation d'énergie, la puissance de crête du système, et l'ampérage
  – Alimentation de réserve et capacité de crête de réserve

    REMARQUE : Certains blocs d'alimentation ne prennent pas en charge cette fonction et les blocs d'alimentation de boîtier lame ne sont pas pris en charge.
- La garantie

  La récupération de la garantie fournit les informations suivantes pour les serveurs Dell :

  – Informations mises à jour sur la garantie de service, en transmettant seulement le numéro de service hôte
  – Informations de garantie mises à jour à intervalles réguliers
  – Transmission sécurisée en utilisant un serveur proxy et les références
  – Informations par le biais d'une connexion testée et sécurisée

  Voir Récupération de la garantie.

Actions de l'hôte

Les actions de l'hôte sont les commandes que vous avez effectuées sur le serveur hôte actuel, telles que :

- Utilisez l'indicateur de clignotement pour faire clignoter le voyant de l'écran LCD avant. Voir Configuration des voyants avant de serveur physique.
- Utilisez l'Assistant Exécuter la mise à jour du micrologiciel pour afficher l'Assistant Mise à jour du micrologiciel et mettre à jour le micrologiciel du serveur hôte. Voir Exécution de l'Assistant Mise à jour du micrologiciel.
- Utilisez l'option Réinitialisation d'iDRAC pour réinitialiser l'iDRAC sans redémarrer l'hôte. Voir Réinitialisation d'iDRAC.

Consoles de gestion

Les consoles de gestion sont utilisées pour lancer des consoles de gestion de systèmes externes, telles que :

- Cliquez sur Console d'accès à distance pour lancer l'interface utilisateur Web d'iDRAC (Integrated Dell Remote Access Controller).
- Cliquez sur OMSA Console pour lancer l'interface utilisateur d'OpenManage Server Administrator (OMSA) si elle est configurée. Voir Activation du lien OMSA
- Cliquez sur Console de châssis lame pour lancer l'interface utilisateur Web de Chassis Management Controller (CMC).

Dell Online Services

Réinitialisation de l'iDRAC

Parfois, l'iDRAC peut ne pas répondre aux demandes, ce qui provoque un comportement inattendu au sein de l'OpenManage Integration for VMware vCenter. La seule façon d'effectuer une restauration depuis cet état est de réinitialiser l'iDRAC. Une réinitialisation d'iDRAC effectue un redémarrage normal de l'iDRAC. Ce redémarrage ne redémarre pas l'hôte. Suite à la réinitialisation, il faut 1 à 2 minutes à l'iDRAC pour redevenir utilisable.

Lors de la réinitialisation de l'iDRAC, vous verrez peut-être :

- Un certain délai ou une erreur de communication alors que l'OpenManage Integration for VMware vCenter obtient son état d'intégrité.
- La fermeture de toutes les sessions ouvertes avec l'iDRAC.
- L'adresse DHCP de l'iDRAC peut changer. Si l'iDRAC utilise DHCP pour son adresse IP, il y a des chances que l'adresse IP change. Dans ce cas, exécutez de nouveau la tâche d'inventaire de l'hôte pour capturer l'IP de l'iDRAC dans les données d'inventaire

REMARQUE : Une réinitialisation logicielle de l'iDRAC peut ne pas réussir à le rendre de nouveau utilisable. Vous aurez peut-être besoin d'effectuer une réinitialisation matérielle. Pour réaliser un redémarrage à froid, sur le serveur, mettez hors tension le serveur, retirez le câble d'alimentation pendant 2 minutes et rebranchez-le. Pour plus d'informations sur la réinitialisation de l'iDRAC, reportez-vous à votre version du Guide d'utilisation de l'iDRAC.

REMARQUE : Dell vous recommande de placer l'hôte en mode Maintenance avant de réinitialiser l'iDRAC.

1. Dans **vSphere Client**, sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, sélectionnez le système hôte dans l'arborescence, puis sélectionnez l'onglet **OpenManage Integration**.
3. Sous **Actions d'hôte**, sélectionnez **Réinitialisation d'iDRAC**.
4. Dans la boîte de dialogue Réinitialisation d'iDRAC, sélectionnez **Poursuivre la réinitialisation d'iDRAC**, puis cliquez sur **OK**.

À propos de la planification d'inventaire

La planification d'inventaire définit l'heure / le jour d'exécution de tâches d'inventaire, telles que :

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

La plupart des fonctions d'OpenManage Integration for VMware vCenterexigent la création préalable d'un inventaire pour recueillir les données requises. Un inventaire de tous les systèmes hôtes doit être dressé pour afficher ces informations. Pour effectuer un inventaire sur les systèmes hôtes, créez un profil de connexion qui fournit des informations de communication et d'authentification. Une fois l'inventaire créé, vous pouvez afficher les résultats d'inventaire de la totalité d'un centre de données ou d'un système hôte individuel.

REMARQUE : Pour assurer que l'inventaire contienne des informations à jour, planifiez la tâche d'inventaire pour qu'elle soit exécutée au moins une fois par semaine. Le travail d'inventaire consomme un minimum de ressources et ne dégrade pas les performances de l'hôte.

Tâches connexes :

- Exécution de tâches d'inventaire
- Modification d'une planification de tâche d'inventaire
- Affichage de l'inventaire d'un système hôte particulier
- Affichage de la configuration et de l'état matériels du centre de données

Modification d'une planification de tâche d'inventaire

La planification d'inventaire définit l'heure / le jour d'exécution de travaux d'inventaire, tels que :

- De manière hebdomadaire, à une heure précise et certains jours.
- À un intervalle de temps défini, un inventaire complet est nécessaire pour rassembler les données nécessaires à la majorité des fonctionnalités de l'OpenManage Integration for VMware vCenter.

REMARQUE : Pour s'assurer que l'inventaire contient des informations à jour, le travail d'inventaire doit être exécuté au moins une fois par semaine. Le travail d'inventaire consomme un minimum de ressources et ne dégrade pas les performances de l'hôte.

Pour modifier la planification du travail d'inventaire :

1. Dans Dell Management Center, sélectionnez**Paramètres** → **Planification d'inventaire**.
2. Pour modifier la planification actuelle, cliquez sur **Modifier**.
3. Sélectionnez l'option **Les jours sélectionnés**, puis cochez la case du jour de la semaine et entrez l'heure. Cliquez sur **Effacer** pour effacer les entrées.
4. Pour modifier la planification d'inventaire, cliquez sur **Appliquer**, ou pour annuler la planification d'inventaire, cliquez sur **Annuler**.
5. Pour exécuter le travail maintenant, dans Management Center, sélectionnez **File d'attente de travaux** et l'onglet **Historique d'inventaire**.
6. Cliquez sur **Exécuter maintenant**.
7. Pour mettre à jour les **Détails du dernier travail d'inventaire,** cliquez sur **Rafraîchir**.

Affichage de l'inventaire d'un système hôte particulier dans vCenter

Pour aficher l'inventaire d'un système hôte particulier :

1. Depuis le **vSphere Client**, sous le titre **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, dans le volet gauche, sélectionnez le système hôte, puis l'onglet **OpenManage Integration**.
3. Une présentation de l'hôte sélectionné est affichée.

   Cette présentation fournit des informations sur les principaux attributs du serveur hôte, y compris des informations sur l'intégrité de ses composants individuels, l'identification, l'hyperviseur et le micrologiciel.

- Intégrité des composants matériels est une représentation graphique de l'état de tous les principaux composants du serveur hôte : châssis du système, alimentation, température, ventilateurs, tension, transformateurs, batteries, intrusion, journal matériel, gestion de l'alimentation et mémoire. Les états possibles sont les suivants :

  – 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

  L'état d'intégrité général est affiché sur la barre d'en-tête en haut à droite.
- Informations sur le serveur fournit les informations d'identification, d'hyperviseur et de micrologiciel, telles que :

  – Nom d'hôte, état d'alimentation, adresse IP d'iDRAC, adresse IP de console, profil de connexion utilisé, modèle, numéro de service et numéro d'inventaire, nombre de jours restants sous garantie, et date de la dernière analyse d'inventaire.
  – Versions d'hyperviseur, de micrologiciel BIOS et de micrologiciel iDRAC.
  – FRM (Fault Resilient Memory - Mémoire résistante aux pannes) : ceci est un attribut du BIOS activé dans celui-ci lors de la configuration initiale du serveur. Cet attribut affiche le mode opérationnel du serveur. Vous devez redémarrer le système lorsque vous modifiez la valeur du mode opérationnel de la mémoire. Ceci s'applique aux serveurs R620, R720, T620, M620 et aux serveurs de 13e génération dotés d'une version ESXi 5.5 ou ultérieure. Les quatre différentes valeurs 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.
    * Enabled (Activé) et non protégé : Cette valeur indique que le mode de fonctionnement de la mémoire dans le BIOS est défini sur FRM, mais que le système d'exploitation ne dispose pas de prise en charge de cette fonction.
    * Désactivé : cette valeur indique que les systèmes valides dotés de 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.
- L'option Entrées récentes du journal système fournit les 10 dernières entrées du journal des événements système. Pour ouvrir la fenêtre **Journal des événements système** qui affiche des détails supplémentaires du journal, cliquez sur **Détails**.

4. Sous **Informations sur l'hôte**, cliquez sur **Inventaire matériel** pour afficher une liste et d'autres détails sur tous les composants installés sur le système hôte, y compris :

   - FRU (Unités remplaçables sur site) : modules DIMM, carte mère, blocs d'alimentation, fonds de panier, cartes contrôleur, etc
   - Mémoire : nombre d'emplacements disponibles et utilisés, capacité maximale et quantité de mémoire utilisée, et détails sur les modules DIMM individuels.
   - NIC (Cartes réseau) : nombre de cartes installées et détails sur les cartes individuelles.
   - Emplacements PCI : nombre total d'emplacements disponibles et utilisés, et détails sur les emplacements individuels.
   - Blocs d'alimentation : nombre actuel et détails sur les blocs d'alimentation individuels.
   - Processeurs : nombre actuel et détails sur les processeurs individuels.
   - RAC (Carte d'accès à distance) : adresse IP, type de RAC et URL d'interface Web.

5. Sous **Informations sur l'hôte**, cliquez sur **Stockage** pour afficher une vue graphique et détaillée de la capacité et du type de stockage physique et virtuel, y compris :
   - Stockage total du système hôte, non configuré, configuré, et capacité de disques de rechange globaux.
   - Liste du nombre de chaque composant de stockage présent sur le système.
   - Table de données des composants qui contient des informations détaillées sur ce composant.
6. Sous **Informations sur l'hôte**, cliquez sur **Micrologiciel** pour afficher toutes les informations du micrologiciel de Dell Lifecycle Controller, y compris :
   - Nom de mise à jour : BIOS, Dell Lifecycle Controller, bloc d'alimentation, etc.
   - Type de mise à jour : BIOS, micrologiciel ou application.
   - Détails d'une mise à jour particulière : version, heure d'installation, si une mise à jour est en cours ou l'état de la mise à jour et la version de la mise à jour. L'état et la version de la mise à jour ont des données uniquement si une mise à jour est planifiée, et la version de la mise à jour est la version du micrologiciel à laquelle le système sera mis à jour.
7. Sous **Informations sur l'hôte**, cliquez sur **Surveillance de l'alimentation** pour afficher des informations générales sur l'alimentation, des statistiques sur l'énergie, et des informations sur l'alimentation de réserve, y compris :
   - Budget de puissance actuel, profil, seuils d'avertissement et de panne.
   - Statistiques sur la consommation d'énergie, la puissance de crête du système, et l'ampérage.
   - Alimentation de réserve et capacité de crête de réserve.
8. Sous **Informations sur l'hôte**, cliquez sur **Garantie** pour afficher des informations sur la garantie du système, y compris :
   - Nom du fournisseur de la garantie et description de la garantie.
   - Dates de début et de fin et nombre de jours restants sous garantie.
   - État de la garantie (active ou expirée) et date de la dernière mise à jour des informations de garantie.

Inventaire et licences

Si les données du serveur ne peuvent pas être récupérées et affichées, il y a plusieurs causes possibles :

- Le serveur n'est pas associé à un profil de connexion, donc une tâche d'inventaire ne peut pas être exécutée.
- Une tâche d'inventaire n'a pas été exécutée sur le serveur pour collecter les données, donc il n'y a rien à afficher.
- Le nombre de licences hôte est dépassé, et vous devez disposer de licences supplémentaires pour exécuter la tâche d'inventaire.
- Le serveur n'a pas la licence iDRAC correcte, requise pour les serveurs de 12e génération et de générations ultérieures . Vous devez acheter la licence iDRAC adéquate.

Le lien Acheter maintenant sert à l'achat initial du produit et non aux mises à niveau. Le lien Acheter maintenant apparaît uniquement si vous utilisez une licence d'évaluation.

Tâches connexes :

- Affichage et modification d'un profil de connexion existant
- Modification d'une planification de tâche d'inventaire

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

- Licence d'évaluation : la version d'essai contient une licence de démonstration pour cinq hôtes (serveurs) gérés par l'OpenManage Integration for VMware vCenter.
- Licence standard : la version complète du produit contient une licence de produit pour dix vCenter et le nombre de connexions hôte achetées gérées par l'OpenManage Integration for VMware vCenter.

Tâches connexes :

- À propos des licences OpenManage Integration for VMware vCenter
- Chargement d'une licence OpenManage Integration for VMware vCenter sur l'Administration Console

Affichage de l'inventaire du stockage

Le stockage du système hôte fournit une vue graphique et détaillée de la capacité et du type de stockage physique et logique pour le stockage connecté à un contrôleur de stockage hôte, y compris :

- Stockage total du système hôte, non configuré, configuré, et capacité de disques de secours globaux.
- Liste du nombre de chaque composant de stockage présent sur le système.
- Table de données des composants qui contient des informations détaillées sur ce composant.

Pour afficher les données sur le stockage :

1. Dans **vSphere Client**, sélectionnez un hôte, puis l'onglet **OpenManage Integration**.
2. Sur la page **Présentation de l'hôte**, dans le volet gauche, cliquez sur **Stockage**.
3. Sur la page **Stockage**, examinez le résumé graphique ou utilisez le tableau et les listes déroulantes **Afficher** et **Filtre** pour trier les informations d'inventaire.

Affichage de la surveillance de l'alimentation hôte

La surveillance de l'alimentation du système hôte fournit des informations générales sur l'alimentation, des statistiques sur l'énergie, et des informations sur l'alimentation de réserve, y compris :

- Budget de puissance actuel, profil, seuils d'avertissement et de panne
- Statistiques sur la consommation d'énergie, la puissance de crête du système, et l'ampérage
- Alimentation de réserve et capacité de crête de réserve

Pour afficher la surveillance de l'alimentation hôte :

1. Dans **vSphere Client**, sélectionnez votre hôte, puis l'onglet **OpenManage Integration.**
2. Dans le volet gauche, sous **Informations sur l'hôte**, cliquez sur **Surveillance de l'alimentation**.
3. Dans la page **Surveillance de l'alimentation**, vous pouvez voir l'alimentation de cet hôte.

Affichage de la configuration et de l'état matériels de tout le centre de données

Vous devez effectuer un travail d'inventaire avant d'afficher la configuration et l'état matériels de tout le centre de données. Après avoir exécuté l'inventaire, vous pouvez afficher les éléments suivants :

- Matériel : unités remplaçables sur site
- Matériel : processeurs
- Matériel : blocs d'alimentation
- Matériel : mémoire
- Matériel : cartes réseau
- Matériel : emplacements PCI
- Matériel : carte d'accès à distance
- Stockage : disques physiques
- Stockage : disques virtuels

- Micrologiciel
- Surveillance de l'alimentation
- La garantie

Pour afficher la configuration et l'état matériels de tout le centre de données :

1. Depuis **vSphere Client** , sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, sélectionnez un centre de données dans l'arborescence puis l'onglet **OpenManage Integration**.
3. Une vue générale de tous les hôtes du centre de données est affichée. Utilisez la liste déroulante **Afficher** pour afficher une catégorie d'inventaire.
4. Utilisez la zone de texte **Filtre** pour entrer un filtre des données d'inventaire.
5. Pour actualiser l'inventaire affiché, cliquez sur **Rafraîchir**.
6. Dans la fenêtre **emplacement de téléchargement**, accédez à l'emplacement où enregistrer l'inventaire et cliquez sur **Enregistrer**.

Gestion des profils de connexion

Les profils de connexion associent les informations d'identification d'accès et de déploiement à un ensemble de systèmes hôte et contiennent en général :

- Nom de profil et description unique (pour aider à la gestion des profils)
- Une liste des hôtes associés au profil de connexion
- Informations d'identification iDRAC
- Informations d'identification de l'hôte
- Date de création
- Date de modification
- Dernière modification de l'utilisateur

Après avoir exécuté l'**Assistant Configuration**, vous gérez les profils d'informations d'identification à partir de l'OpenManage Integration for VMware vCenter **OpenManage Integration for VMware vCenter** → **Modèles et profils** à l'aide des opérations suivantes :

- Création d'un profil de connexion
- Affichage et modification d'un profil de connexion existant
- Suppression d'un profil de connexion
- Test d'un profil de connexion
- Actualisation d'un profil de connexion

Affichage et modification d'un profil de connexion existant

Après avoir configuré un profil de connexion, vous pouvez modifier le nom du profil, la description, les hôtes associées, et les informations d'identification d'agent OMSA et iDRAC.
Pour afficher ou modifier un profil de connexion existant :

1. Dans l'OpenManage Integration for VMware vCenter, sélectionnez **Profils de connexion**.
2. Sous **Profils disponibles**, sélectionnez le profil à afficher ou modifier, puis cliquez sur **Afficher/Modifier**.
3. Dans le volet **Nom et description du profil**, entrez le **Nom du profil de connexion** et une **Description du profile de connexion** facultative (ce nom et cette description servent à gérer les profils de connexion personnalisés).
4. Dans la page **Hôtes associés**, sélectionnez les hôtes associés au profil de connexion, puis cliquez sur **Suivant**.

5. Lisez les informations offertes par la page **Informations d'identification**, puis cliquez sur **Suivant**.
6. Dans la page iDRAC, sous Informations d'identification, effectuez l'une des tâches suivantes :

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

   - Dans le cas des iDRACs déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; autrement, configurez les informations d'identification iDRAC plus bas.

     – Entrez le nom de l'utilisateur dans la zone de texte **Nom d'utilisateur Active Directory**. Pour ce faire, utilisez l'un des formats suivants : domaine\nom d'utilisateur ou domaine/nom d'utilisateur ou encore nom d'utilisateur@domaine. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la documentation Microsoft Active Directory pour connaître les conventions de nom d'utilisateur.

     – Entrez le mot de passe dans la zone de texte **Mot de passe Active Directory**. Celui-ci ne doit pas comporter plus de 127 caractères.

     – Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

     – Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

       * Pour télécharger et stocker le certificat iDRAC et le valider lors de connexions futures, sélectionnez **Activer** .
       * Pour ne pas effectuer de vérification et ne pas stocker le certificat, sélectionnez **Désactivé**.

   - Pour configurer les références iDRAC sans Active Directory, effectuez les opérations suivantes :

     – Dans la zone de texte **Nom d'utilisateur**, entrez le nom de l'utilisateur. Celui-ci ne doit pas comporter plus de 16 caractères. Pour en savoir plus sur les restrictions de nom d'utilisateur de votre version d'iDRAC, reportez-vous à la documentation iDRAC.

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

     – Entrez le mot de passe dans la zone de texte **Mot de passe**. Celui-ci ne doit pas comporter plus de 20 caractères.

     – Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

     – Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

       * Pour télécharger et stocker le certificat iDRAC et le valider lors de connexions futures, sélectionnez **Activer** .
       * Pour ne pas effectuer de vérification et ne pas stocker le certificat, sélectionnez **Désactivé**.
7. Cliquez sur **Suivant**.
8. Dans la page Informations d'identification d'hôte, sous Informations d'identification, effectuez l'une des tâches suivantes :

   - Dans le cas des hôtes déjà configurés et activés pour Active Directory sur lesquels vous souhaitez utiliser Active Directory, cochez la case **Utiliser Active Directory** ; autrement, configurez les références iDRAC plus bas.

     – Entrez le nom de l'utilisateur dans la zone de texte **Nom d'utilisateur Active Directory**. Pour ce faire, utilisez l'un des formats suivants : domaine\nom d'utilisateur ou domaine/nom d'utilisateur ou encore nom d'utilisateur@domaine. Le nom d'utilisateur ne doit pas comporter plus de 256 caractères. Reportez-vous à la documentation Microsoft Active Directory pour connaître les conventions de nom d'utilisateur.

– Entrez le mot de passe dans la zone de texte **Mot de passe Active Directory**. Celui-ci ne doit pas comporter plus de 127 caractères.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat de l'hôte, sélectionnez **Désactivé**.

- Pour configurer les informations d'identification de l'hôte sans Active Directory, effectuez les opérations suivantes :

– Entrez le nom de l'utilisateur dans la zone de texte **Nom d'utilisateur**. Ce nom doit être root (racine).

– Entrez le mot de passe dans la zone de texte **Mot de passe**. Celui-ci ne doit pas comporter plus de 127 caractères.

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

REMARQUE : Les références OMSA sont les mêmes que celles utilisées pour les hôtes ESX et ESXi.

– Entrez à nouveau le mot de passe dans la zone de texte **Vérifier le mot de passe**, .

– Dans la liste déroulante Vérification de certificat, sélectionnez une des opérations suivantes :

* Pour télécharger et stocker le certificat de l'hôte et le valider lors de connexions futures, sélectionnez **Activer** .

* Pour ne pas effectuer de vérification et ne pas stocker le certificat de l'hôte, sélectionnez **Désactivé**.

9. Cliquez sur **Enregistrer**.
10. Pour fermer la fenêtre, cliquez sur **X** (en haut à droite).

Suppression d'un profil de connexion

Vous pouvez supprimer un profil de connexion à partir de l'OpenManage Integration for VMware vCenter.
Pour supprimer un profil de connexion :

1. Dans l' **OpenManage Integration for VMware vCenter** , cliquez sur **Profils de connexion**.
2. Sous **Profils disponibles**, sélectionnez le profil à supprimer, puis cliquez sur **Supprimer**.
3. Lorsque le message s'affiche, pour supprimer le profil, cliquez sur **Supprimer**, ou cliquez sur **Annuler** pour annuler la suppression.

Test d'un profil de connexion

Pour tester un profil de connexion :

1. Dans l'**OpenManage Integration for VMware vCenter** , sélectionnez **Profils de connexion**.
2. Sous **Profils disponibles**, pour tester les informations d'identification iDRAC et de racine hôte entrées sur les serveurs sélectionnés, sélectionnez le profil de connexion et cliquez sur **Tester la connexion**.
3. Utilisez les cases pour sélectionner les hôtes à tester, puis cliquez sur **Tester sélectionnés**.
4. Pour abandonner tous les tests sélectionnés et annuler les tests, cliquez sur **Annuler tous les tests**.
5. Pour quitter, cliquez sur **Terminé**.

Actualisation d'un profil de connexion

Pour actualiser un profil de connexion :

Cliquez sur **Rafraîchir**.

REMARQUE : Si un hôte est supprimé de vCenter, il est supprimé du profil de connexion.

Comprendre les journaux des événements système dans la Vue d'hôte de vSphere Client

Le journal des événements système fournit des informations sur l'état du matériel découvert par l' OpenManage Integration for VMware vCenter.

Les journaux des événements système fournissent des informations basées sur les critères suivants :

Condition	Il existe plusieurs icônes d'état : Informations (point d'exclamation bleu), Avertissement (triangle jaune avec point d'exclamation), Erreur (X rouge).
Heure (Heure du serveur)	Indique l'heure et la date de l'événement.
Rechercher dans cette page	Affiche le message, les noms de serveur, les paramètres de configuration, etc.spécifiques.

Les niveaux de gravité sont définis de la manière suivante :

Informatif	L'opération OpenManage Integration for VMware vCenter a été réalisée avec succès.
Avertissement	L'opération OpenManage Integration for VMware vCenter a partiellement échoué et partiellement réussi.
Erreur	L'opération OpenManage Integration for VMware vCenter a échoué.
Sécurité	Contient des informations sur la sécurité du système.

Vous pouvez enregistrer le journal dans un fichier CSV externe.

Informations connexes :

- Affichage des journaux des événements système d'un hôte particulier

Affichage des journaux dans Dell Management Center

Les journaux de Dell Management Center comprennent des informations sur l'état du matériel découvert et un historique des actions des utilisateurs.
Pour afficher les journaux dans Dell Management Center :

1. Depuis **Dell Management Center**, dans le volet gauche, sélectionnez **Journal**.
2. Pour mettre à jour le journal avec les données les plus récentes, cliquez sur **Rafraîchir**.
3. Pour sélectionner une catégorie de gravité pour filtrer les données du journal, dans la liste déroulante **Toutes les catégoriess**, sélectionnez l'une des options suivantes : Toutes les catégories, Info, Avertissement, Erreur ou Sécurité.
4. Pour sélectionner une plage de dates pour filtrer les données du journal, cliquez sur la liste déroulante **Semaine dernièrek** et sélectionnez l'une des options suivantes : Semaine dernière, Mois dernier, Année dernière ou Plage personnalisée.

   Si Plage personnalisée est sélectionné, les listes déroulantes **Date de début** et **Date de fin** s'affichent.

5. Si vous avez sélectionné une plage de dates personnalisée :
   a. Cliquez sur le calendrier pour renseigner la date de **Début**.
   b. Cliquez sur le calendrier pour renseigner la date de **Fin**.
   c. Pour enregistrer la configuration, cliquez sur **Appliquer**.
6. Pour contrôler l'affichage du journal, utilisez les commandes d'affichage pour configurer **Enregistrements par écran**, allez à la **Page** souhaitée, et utilisez les commandes Page suivante et Page précèdente.
7. Pour exporter le contenu du journal vers un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter**.
8. Dans la fenêtre emplacement de téléchargement, accédez à l'emplacement où enregistrer le journal et cliquez sur **Enregistrer**.

Affichage des journaux des événements d'un hôte particulier

La fonctionnalité Journaux des événements matériels système fournit des informations basées sur les critères suivants :

- Condition

  Il existe plusieurs icônes d'état : Informations (point d'exclamation bleu), Avertissement (triangle jaune avec point d'exclamation), Erreur (X rouge).
- Heure (Heure du serveur)

  Affiche l'heure et la date de l'événement.
- Rechercher dans cette page

  Affiche le message, les noms de serveur, les paramètres de configuration, etc.spécifiques.

Pour afficher le journal des événements système d'un hôte particulier :

1. Depuis **vSphere Client** , sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans l'arborescence, sélectionnez le système hôte.
3. Sélectionnez l'onglet **OpenManage Integration**.
4. Dans **Entrées récentes du journal système**, pour ouvrir la fenêtre **Journal des événements système** , cliquez sur **Détails**.
5. Pour mettre à jour le **Journal des événements système**, cliquez sur **Rafraîchir le journal**.
6. Pour limiter (filtrer) le nombre d'entrées du journal des événements, choisissez l'une des options suivantes :
   - Dans la zone de texte du filtre de recherche, entrez une chaîne de texte pour filtrer dynamiquement les entrées du journal.
   - Pour effacer la zone de texte du filtre, cliquez sur **X** et toutes les entrées du journal des événements s'affichent.
7. Pour effacer toutes les entrées du journal des événements, cliquez sur **Effacer le journal**. Un message s'affiche indiquant que toutes les entrées du journal sont supprimées après avoir été effacées. Sélectionnez l'une des opérations suivantes :
   - Pour accepter d'effacer les entrées du journal, cliquez sur **OK**.
   - Pour annuler, cliquez sur **Annuler**.
8. Pour exporter le journal des événements vers un fichier CSV file, cliquez sur **Exporter**.
9. Accédez à l'emplacement où enregistrer le journal des événements système et cliquez sur **Enregistrer**.

À propos des mises à jour du micrologiciel

L'emplacement auquel les serveurs reçoivent les mises à jour de micrologiciel est un paramètre global disponible dans l'OpenManage Integration for VMware vCenter sur l'onglet Paramètres.

Les paramètres de l'espace de stockage du micrologiciel comprennent l'emplacement du catalogue du micrologiciel utilisé pour mettre à jour les serveurs déployés. Il existe deux types d'emplacement :

Dell (ftp.dell.com)	Utilise l'espace de stockage de mise à jour du micrologiciel Dell (**ftp.dell.com**). L'OpenManage Integration for VMware vCenter télécharge de l'espace de stockage Dell les mises à jour du micrologiciel sélectionnées.
Dossier de réseau partagé	Créés avec Dell Repository Manager™, ces espaces de stockage locaux sont situés sur le partage de fichier CIFS ou NFS.

REMARQUE : Une fois l'espace de stockage créé, enregistrez-le à un emplacement accessible aux hôtes enregistrés. Les mots de passe d'espace de stockage ne peuvent pas dépasser 31 caractères. N'utilisez pas les caractères suivants dans un mot de passe : @, &, %, ', ", , (virgule), <>

L'Assistant Mise à jour du micrologiciel vérifie toujours les niveaux minimum du micrologiciel d'iDRAC, BIOS, et Lifecycle Controller, et tente de les mettre à jour aux versions minimales requises. Lorsque les versions du micrologiciel d'iDRAC, BIOS, et Lifecycle Controller satisfont les conditions minimales, l'Assistant Mise à jour du micrologiciel permet d'effectuer les mises à jour de tous les micrologiciels, y compris : iDRAC, Lifecycle Controller, RAID, carte réseau/LOM, bloc d'alimentation, BIOS, etc.

REMARQUE : Pour les serveurs de 9e et 10e générations, les versions du micrologiciel du BIOS / BMC / DRAC sont visibles uniquement au niveau Vue de cluster dans vCenter ou sur la page Présentation de la vue d'un hôte particulier. Les informations de version du micrologiciel ne sont pas actives dans la vue d'un hôte particulier sous Micrologiciel et les mises à jour à distance du micrologiciel ne sont pas disponibles.

Versions du micrologiciel ultérieures au 14 octobre 2010

Pour le micrologiciel mis à jour le ou après le 14 octobre 2010, l'Assistant Mise à jour du micrologiciel s'exécute.

Versions du micrologiciel ultérieures au 29 juillet 2009 et antérieures au 14 octobre 2010

Si votre micrologiciel a été mis à jour le ou après le 29 juillet 2009 et avant le 14 octobre 2010, vous ne verrez toujours pas l'Assistant Mise à jour du micrologiciel, mais vous recevrez un groupe ISO pour mettre à jour le micrologiciel. Après cette mise à jour, il se peut que vous n'ayez pas la dernière version du micrologiciel. Après avoir exécuté le groupe, il est recommandé d'exécuter à nouveau la mise à jour.

Versions du micrologiciel antérieures au 29 juillet 2009

Si votre micrologiciel est antérieur au 29 juillet 2009, vous devrez peut-être télécharger et exécuter le fichier ISO pour mettre à jour vos machines. Après avoir exécuté l'ISO, il est recommandé d'exécuter à nouveau l'Assistant Mise à jour du micrologiciel.

Informations connexes :

- Configuration de l'espace de stockage du micrologiciel

Exécution de l'Assistant Firmware Update (Mise à jour de micrologiciel)

Cette fonctionnalité n'est disponible que pour les serveurs Dell de 11e génération et de générations ultérieures dotés d'une carte iDRAC Express ou Enterprise. Si votre micrologiciel a été installé le 14 octobre 2010 ou après cette date, vous pouvez automatiquement mettre à jour vos versions du micrologiciel à l'aide de l'Assistant Mise à jour de micrologiciel.

REMARQUE : Comme précaution contre les problèmes de délai d'expiration de navigateurs, définissez le délai d'expiration par défaut sur 30 secondes. Pour savoir comment modifier le paramètre de délai d'expiration par défaut, voir la section « Pourquoi un message d'erreur s'affiche-t-il lorsque je clique sur le lien Mise à jour de micrologiciel » dans la section Dépannage du *Guide d'utilisation*.

REMARQUE : Vous pouvez utiliser l'Assistant Micrologiciel pour la licence d'essai/évaluation tant que la licence n'a pas expiré.

Pour exécuter l'Assistant Mise à jour du micrologiciel :

1. Dans le **vSphere Client → onglet OpenManage Integration → Informations sur l'hôte**, cliquez sur **Micrologiciel → Exécuter l'Assistant Mise à niveau de micrologiciel.**
2. Pour utiliser l'option **Charger une seule mise à jour de micrologiciel depuis un fichier** :
   a. Entrez le chemin d'accès dans le format suivant :
   ```
   CIFS: \\<host accessible share path>\<FileName>.exe or NFS: host:/share/filename.exe
   ```
   b. Si vous possédez NFS, passez à l'étape 7. Autrement, entrez le **Nom d'utilisateur** et **Mot de passe** dans un format de domaine accessible au lecteur partagé.
   c. Passez à l'étape 7.

   Alternativement, pour utiliser l'option **Mettre à jour à partir du référentiel**:
   a. Sélectionnez **Mettre à jour à partir de l'espace de stockage**.
   b. Assurez-vous d'avoir une connexion réseau à **ftp.dell.com**.
   c. Cliquez sur **Suivant**.
3. Sélectionnez l'ensemble correspondant à votre hôte, puis cliquez sur **Suivant**.
4. Sélectionnez les mises à jour de micrologiciel souhaitées, puis cliquez sur **Suivant**. Les composants rétrogradés, déjà mis à jour, ou qui ont actuellement une mise à jour planifiée ne sont pas sélectionnables. Si vous sélectionnez la case à cocher **Autoriser les Composants à rétrograder**, sélectionnez les options énumérées sur la liste des Rétrogradations. Cette option n'est recommandée qu'aux utilisateurs expérimentés qui comprennent les implications de la rétrogradation de micrologiciel.
5. Sélectionnez l'option de redémarrage souhaitée.
   - **Entrez dans le mode maintenance, appliquez les mises à jour, puis redémarrez.**
     L'hôte passe en mode maintenance. Si l'hôte ne peut passer en mode maintenance, l'hôte n'est pas redémarré et la mise à jour est appliquée lors du prochain redémarrage. Cochez la case **Quitter le mode maintenance après exécution complète de la mise à jour du micrologiciel**, pour quitter le mode maintenance après la mise à jour.
   - **Appliquer les mises à jour lors du prochain redémarrage.**
     Pour éviter une interruption de service, il est recommandé que l'hôte passe en mode Maintenance avant le redémarrage.
   - **Appliquer les mises à jour et forcer le redémarrage sans passer en mode Maintenance.**
     Les mises à jour sont appliquées, et le redémarrage s'effectue même si l'hôte n'est pas en mode maintenance. Cette méthode n'est pas recommandée.
6. Cliquez sur **Terminer**.
7. Pour vérifier que la mise à jour a bien fonctionné, dans Dell Management Center, sélectionnez **File d'attente des tâches → Historique d'inventaire → Exécuter maintenant**, puis pour afficher les nouvelles versions, accédez à**vSphere Client → onglet OpenManage Integration**et cliquez sur**Micrologiciel**.

Mise à jour d'anciennes versions du micrologiciel

Le micrologiciel doit être à un niveau minimum pour exécuter l'Assistant Mise à jour du micrologiciel. Sinon, vous disposez d'options pour vous aider à mettre à jour votre micrologiciel, avant d'exécuter l'Assistant Mise à jour du micrologiciel. En général, si le micrologiciel a été installé avant le 29 juillet 2009, vous devez télécharger et exécuter un fichier ISO, voir Mises à jour du micrologiciel. Si le micrologiciel a été installé entre le 29 juillet 2009 et le 14 octobre 2010, vous disposez d'un lot ISO pour une installation automatique depuis le OpenManage Integration for VMware vCenter. Le micrologiciel mis à jour après le 14 octobre 2010 exécute l'Assistant Mise à jour du micrologiciel. Les mises à jour du micrologiciel sont exécutées depuis vSphere Client sur l'onglet OpenManage Integration de l'hôte. Pour configurer le référentiel, voir Configuration du référentiel du micrologiciel.

Pour mettre à jour d'anciennes versions du micrologiciel :

1. Dans **vSphere Client**, sur l'onglet **OpenManage Integration**, sous **Actions de l'hôte**, cliquez sur **Exécuter l'Assistant Mise à jour du micrologiciel**.

   La boîte de dialogue Mise à jour requise s'affiche lorsque votre hôte est à un niveau de micrologiciel inférieur à celui pris en charge par l'Assistant. Vous serez invité à télécharger et exécuter un fichier ISO ou recevrez un lot de mises à jour à exécuter.
2. Dans la boîte de dialogue **Mise à jour requise**, procédez comme suit :

   - Pour sortir automatiquement du mode de maintenance après la mise à jour du micrologiciel, sélectionnez la case **Quitter le mode de maintenance après la mise à jour du micrologiciel**.
   - Pour entrer en mode de maintenance pour examiner et/ou tester la machine avant de la rajouter au cluster, ne cochez pas la case.
3. Cliquez sur **Mettre à jour**.
4. La boîte de dialogue **Réussite** vous informe qu'une mise à jour est en cours.

   Si vous choisissez l'option **Quitter le mode de maintenance après la mise à jour du micrologiciel**, la mise à jour du micrologiciel met l'hôte en mode de maintenance puis il redémarre automatiquement. Sinon, il reste en mode de maintenance.
5. Reportez-vous à la zone**Tâches récentes** de vSphere Client pour voir la progression de la mise à jour.

   Après cette procédure, exécutez à nouveau l'Assistant Mise à jour du micrologiciel pour vous assurer que le micrologiciel est totalement à jour.

Exécution de l'Assistant Mise à jour de micrologiciel pour les clusters et centres de données

Cette fonctionnalité est disponible uniquement sur les serveurs Dell de 11e génération et de générations ultérieures dotés d'une carte iDRAC Express ou Enterprise. Si votre micrologiciel a été installé le 14 octobre 2010 ou plus tard, vous pouvez automatiquement mettre à jour vos versions micrologicielles à l'aide de l'Assistant Mise à jour de micrologiciel. Cet Assistant met à jour uniquement les hôtes faisant partie d'un profil de connexion et conformes en termes de micrologiciel, d'état CSIOR, d'hyperviseur et d'état OMSA (serveurs de 11e génération uniquement). Si votre hôte n'est pas répertorié, exécutez l'Assistant Conformité pour les hôtes vSphere depuis l'OpenManage Integration for VMware vCenter ou sélectionnez l'hôte qui ne s'affiche pas depuis la vue Hôtes et Clusters, puis utilisez l'Assistant Mise à jour de micrologiciel. La mise à jour des composants micrologiciels de chaque hôte dure de 30 à 60 minutes. Activez DRS sur un cluster pour que les machines virtuelles puissent êtres migrées lorsqu'un hôte passe en mode Maintenance ou sort de ce mode lors du processus de mise à jour de micrologiciel. Vous ne pouvez planifier ou exécuter qu'une tâche de mise à jour de micrologiciel à la fois.

Si vous effectuez une exportation depuis l'Assistant, utilisez le bouton Exporter vers CSV. Utilisez la recherche pour localiser un cluster, centre de données, hôte ou élément de rubrique spécifique de la grille de données, sauf l'élément Date d'application.

REMARQUE : Veillez à toujours mettre à jour le micrologiciel dans le cadre du groupe de référentiels : BIOS, iDRAC et Lifecycle Controller.

REMARQUE : Pour savoir comment modifier le paramètre de délai d'expiration par défaut, voir « Pourquoi un message d'erreur s'affiche-t-il lorsque je clique sur le lien Mise à jour de micrologiciel » dans la section Dépannage du *Guide d'utilisation*.

Vous pouvez afficher l'état et gérer les tâches de mise à jour de micrologiciel depuis la page File d'attente des tâches. Voir Affichage de l'état de mise à jour de micrologiciel pour les clusters et centres de données.

1. Depuis **vSphere Client** , sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, dans la vue d'arborescence, sélectionnez un centre de données ou un cluster, puis sélectionnez l'onglet **OpenManage Integration**.

3. Cliquez sur **Mettre à jour le micrologiciel**.

   Si ce lien n'est pas activé ou si un message pop-up s'affiche lorsque vous cliquez sur cette option, une tâche de mise à jour de micrologiciel est en cours ou est planifiée. Fermez la boîte de dialogue. Patientez un moment, puis relancez l'opération. Affichez l'état de toutes les tâches dans l'onglet Tâches de mise à jour de micrologiciel sous Files d'attente de tâches.
4. Dans la page d'accueil, lisez les informations sur la mise à jour avant de lancer l'Assistant.
5. Cliquez sur **Suivant**.
6. Dans la page Inventaire du micrologiciel, vérifiez les composants déjà installés sur le système.
7. Cliquez sur **Suivant**.
8. Dans la page Sélectionner des groupes mis à jour, sélectionnez les groupes de mises à jour en cochant les cases.
9. Cliquez sur **Suivant**.
10. Dans la page Sélectionner les systèmes/composants à mettre à jour, cochez les cases en regard des composants à mettre à niveau ou à rétrograder. Si vous souhaitez rétrograder, cochez la case **Autoriser la rétrogradation des composants**.

    REMARQUE : Si vous sélectionnez tous les composants et certains d'entre eux ne sont pas sélectionnés, cela veut dire qu'aucune mise à niveau n'existe pour ces composants-là. Vous pouvez sélectionner ces composants pour les rétrograder.
11. Cliquez sur **Suivant**.
12. Dans la page Informations sur la mise à jour de micrologiciel, vérifiez les composants que vous avez sélectionnés pour une mise à niveau ou une rétrogradation.
13. Cliquez sur **Suivant**.
14. Dans la page Planifier des mises à jour de micrologiciel, sous Nom de tâche, faites ce qui suit :
    a. Dans la zone de texte Nom de tâche de mise à jour de micrologiciel, saisissez le **nom de tâche de mise à jour de micrologiciel**.

       Ce champ est obligatoire. S'il n'est pas rempli, la mise à niveau est bloquée. N'utilisez pas un nom déjà utilisé. Si vous supprimez ce nom, vous pouvez le réutiliser.
    b. Dans la Description de mise à jour de micrologiciel, saisissez la **description**.
15. Sous Planification de tâche, effectuez l'une des actions suivantes :

    REMARQUE : La sélection d'une option n'est pas obligatoire. Si une option n'est pas sélectionnée, la mise à niveau est bloquée.

    - Si vous souhaitez exécuter la tâche de mise à jour maintenant, cliquez sur **Mettre à jour maintenant**, puis cliquez sur **Terminer**.
    - Si vous souhaitez exécuter la tâche de mise à jour ultérieurement, cliquez sur **Planifier une mise à jour**, puis effectuez l'une des actions suivantes :

      1. Dans la zone Calendrier, sélectionnez les **mois et jour**.
      2. Dans la zone de texte Heure, saisissez l'**heure** en HH:MM, puis cliquez sur **Terminer**.

         REMARQUE : L'heure est le fuseau horaire local de l'emplacement de votre client. Si vous saisissez des valeurs d'heure non valides, la mise à jour est bloquée.

Affichage de l'état de mise à jour de micrologiciel pour les clusters et centres de données

Pour afficher des informations sur cette page, exécutez une mise à jour de micrologiciel pour un cluster ou un centre de données. Cette page affiche uniquement des informations sur les mises à jour des clusters et des centres de données. Voir Exécution de l'Assistant Mise à jour de micrologiciel pour les clusters et centres de données.

Utilisez cette page pour actualiser, supprimer ou annuler vos tâches de mise à jour de micrologiciel.

1. Dans Dell Management Center, sélectionnez **File d'attente des tâches → Tâches de mise à jour de micrologiciel**.
2. Pour afficher les informations les plus récentes, cliquez sur **Actualiser/Rafraîchir**.
3. Affichez l'état dans la grille de données. Cette grille fournit les informations suivantes sur les tâches de mise à jour de micrologiciel :
   - Condition
   - Heure planifiée
   - Nom
   - Description
   - Taille de la collection

     La taille de la collection est le nombre de serveurs dans cette tâche d'inventaire de micrologiciel.
   - Récapitulatif d'avancement

     Le récapitulatif d'avancement affiche les détails d'avancement de cette mise à jour de micrologiciel.
4. Pour afficher davantage de détails sur une tâche spécifique, cliquez sur **Détails** dans la grille de données d'une tâche spécifique.

   Vous trouverez ci-dessous les détails suivants :
   - Numéro de service
   - IP iDRAC
   - Condition
   - Avertissements
   - Détails de tâche de mise à jour de micrologiciel
   - Heure de début
   - Heure de fin
5. Si vous souhaitez annuler une mise à jour de micrologiciel planifiée qui ne s'exécute pas, cliquez sur **Annuler** sur la ligne de la tâche que vous souhaitez annuler.
6. Si vous souhaitez supprimer des mises à jour de micrologiciel planifiées, cliquez sur **Purger la file d'attente**.

   Vous ne pouvez supprimer que les tâches terminées ou planifiées.
7. Sélectionnez **Plus anciennes que la date et l'état de tâche**, puis cliquez sur **Appliquer**. Les tâches sélectionnées sont alors supprimées de la file d'attente.

Gestion d'hôte avancée à l'aide du vCenter

Les tâches de gestion d'hôte avancée sont des actions système qui permettent à un administrateur d'identifier un serveur physique dans l'environnement du centre de données, de lancer des outils de gestion serveur et d'afficher les informations de garantie du serveur. Toutes ces actions sont lancées à partir de l'onglet OpenManage Integration dans le vCenter ou par un clic droit sur l'hôte dans la vue *Hôte et clusters* d'un système hôte particulier.

Configuration du voyant avant d'un serveur physique

Pour aider à localiser un serveur physique dans un environnement de grand centre de données, vous pouvez configurer le voyant avant pour qu'il clignote durant une période spécifiée.

Pour configurer le voyant avant d'un serveur physique :

1. Dans **vSphere Client**, sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, sélectionnez le système hôte dans l'arborescence et sélectionnez l'onglet **OpenManage Integration**.
3. Sous **Actions de l'hôte**, sélectionnez **Faire clignoter le voyant**
4. Choisissez l'une des options suivantes :

   - Pour activer le clignotement et spécifier la période, dans la boîte de dialogue **Voyant**, cliquez sur **Clignotement activé** et utilisez la liste déroulante Délai d'expiration pour sélectionner l'incrément du délai d'expiration, puis cliquez sur **OK**.
   - Pour désactiver le clignotement, dans la boîte de dialogue **Voyant**, cliquez sur **Clignotement désactivé**, puis cliquez sur **OK**.

Outils de gestion basés sur le serveur

Il y a deux outils de gestion basés sur le serveur, iDRAC et OMSA, que l'on peut lancer depuis l'onglet **vSphere Client** → **OpenManage Integration**. Sous le lien Management Consoles (Consoles de gestion) dans le volet gauche, vous pouvez accéder à :

- Lancer l'accès à distance.
  Utiliser cette option pour lancer l'interface utilisateur iDRAC
- Lancer OMSA
  Utiliser cette option pour lancer l'URL de l'interface utilisateur d'OpenManage Server Administrator qui a été entrée dans le centre de gestion durant l'Assistant Configuration initial ou avec**Paramètres** → **Général**. Vous devez installer l'URL du serveur Web OMSA sur une station de gestion Windows.
- Si vous êtes sur un système lame, lancez CMC pour lancer l'interface utilisateur de Chassis Management Controller. Si vous n'êtes pas sur un système lame, cela ne s'affiche pas.

Récupération de la garantie

La récupération de la garantie fournit les informations suivantes pour les serveurs Dell :

- Informations mises à jour sur la garantie de service, en transmettant seulement le numéro de service hôte
- Informations de garantie mises à jour à intervalles réguliers
- Transmission sécurisée en utilisant un serveur proxy et les références

REMARQUE : Dell ne stocke pas les informations de numéro de service transmises.

Tâches connexes :

- Exécution d'une tâche de récupération de la garantie
- Affichage des informations de garantie serveur d'un hôte particulier
- Affichage des informations de garantie de tout un centre de données

Affichage des informations de garantie de tout un centre de données

À la fin de la tâche de garantie, vous pouvez afficher les informations de garantie dans vSphere Client, sur la page Vue de centre de données.

Pour afficher les informations de garantie de tout un centre de données :

1. Depuis **vSphere Client** , sous l'en-tête **Inventaire**, sélectionnez Hôtes et clusters.
2. Dans **Hôtes et clusters**, sélectionnez le centre de données dans l'arborescence et sélectionnez l'onglet **OpenManage Integration**.

3. Une vue générale de tous les hôtes du centre de données s'affiche. Dans la liste déroulante Afficher, sélectionnez **Garantie**.
4. Dans la zone de texte **Filtre**, entrez un filtre pour les données de garantie.
5. Pour actualiser l'inventaire affiché, cliquez sur **Rafraîchir**.
6. Pour exporter l'inventaire vers un fichier CSV, cliquez sur **Exporter**. Dans la fenêtre Emplacement de téléchargement, accédez à l'emplacement où enregistrer l'inventaire et cliquez sur **Enregistrer**.

Affichage des informations de garantie serveur d'un hôte particulier

Après la fin d'une tâche de garantie, vous pouvez afficher les informations de garantie d'un hôte particulier dans vSphere Client sur la page Vue Hôtes).

Pour afficher les informations de garantie d'un hôte particulier :

1. Depuis vSphere Client , sous l'en-tête **Inventaire**, sélectionnez **Hôtes et clusters**.
2. Dans **Hôtes et clusters**, sélectionnez le système hôte dans l'arborescence et sélectionnez l'onglet **OpenManage Integration**.
3. Pour afficher les informations de garantie, sélectionnez **Garantie**. Les informations sur la page État de la garantie comprennent :
    - Nom du fournisseur de la garantie et description de la garantie
    - Dates de début et de fin et nombre de jours restants sous garantie
    - État de la garantie (active ou inactive) et date de la dernière mise à jour des informations de garantie

5

Gestion du matériel

Prérequis :

Pour réaliser avec succès l'allocation et le déploiement du matériel, les serveurs physiques doivent figurer dans l'Assistant Déploiement. Tous les serveurs physiques doivent satisfaire les conditions préalables suivantes :

- Reportez-vous aux *OpenManage Integration for VMware vCenterd'OpenManage pour VMware vCenter* pour obtenir des informations spécifiques sur le matériel pris en charge.
- Le serveur doit posséder les versions minimales prises en charge du micrologiciel iDRAC, de Lifecycle Controller et du BIOS. Reportez-vous aux *OpenManage Integration for VMware vCenterd'OpenManage Integration pour VMWare vCenter* afin d'obtenir des informations spécifiques sur le matériel pris en charge.

  REMARQUE : Si les versions du micrologiciel sont périmées, un processus de mise à niveau en deux étapes peut être nécessaire. Consultez la documentation du micrologiciel pour obtenir des instructions détaillées sur la mise à niveau.
- L'OpenManage Integration for VMware vCenter prend en charge le déploiement à l'aide uniquement des LOM embarqués / intégrés. Vous pouvez configurer manuellement les cartes réseau dans les emplacements PCI après le déploiement. Si vous utilisez des cartes réseau d'extension, les LOM hôte doivent être activés sur le système.
- L'OpenManage Integration for VMware vCenter permet d'effectuer un déploiement sur un double module SD interne (hyperviseur uniquement) ou des disques durs locaux. Le double module SD interne doit être activé à partir du BIOS avant le déploiement de l'hyperviseur avec le OpenManage Integration for VMware vCenter. Vous pouvez changer manuellement la carte réseau de gestion et ajouter le système au vCenter.

  REMARQUE : Pour le double module SD pris en charge, reportez-vous à la documentation du serveur respectif.
- Si l'iDRAC est en mode dédié, sa carte réseau doit être activée pour communiquer avec l'OpenManage Integration for VMware vCenter.
- CSIOR doit être activé. En outre, avant de lancer la découverte automatique, afin de s'assurer que les données récupérées sont à jour, le système doit être mis complètement hors tension puis remis sous tension (redémarrage matériel).
- Les serveurs Dell peuvent être commandés avec les options de découverte automatique et les options d'établissement de liaison (« handshake ») pré-configurées en usine. Si un serveur n'est pas pré-configuré avec ces options, vous devez entrer manuellement l'adresse IP d'OpenManage Integration for VMware vCenter ou configurer votre réseau local pour fournir cette information.
- Si l'OpenManage Integration for VMware vCenter n'est pas utilisé pour la configuration matérielle, vérifiez que les conditions suivantes sont remplies avant de lancer le déploiement de l'hyperviseur :
  - Activez l'indicateur VT (Virtualization Technology — Technologie de virtualisation) dans le BIOS.
  - Configurez la séquence de démarrage du système sur un disque virtuel amorçable ou un double module SD interne pour l'installation du système d'exploitation.
- Si l'OpenManage Integration for VMware vCenter est utilisé pour la configuration matérielle, les paramètres du BIOS pour VT sont automatiquement activés, même si la configuration du BIOS ne fait pas partie du profil matériel. La configuration RAID Express / Clone est requise si un disque virtuel n'est pas déjà présent sur le système cible.
- Si vos serveurs sont de versions antérieures à Dell PowerEdge 12G, le processus de déploiement installe le progiciel OpenManage Server Administrator sur le système cible et configure automatiquement la destination d'interruption SNMP pour pointer vers l'OpenManage Integration for VMware vCenter .
- Les images ESXi personnalisées qui contiennent *tous* les lecteurs Dell sont requises pour le déploiement. Vous trouverez les images correctes à la page Lecteurs et téléchargements Dell et en enregistrant les images personnalisées dans un emplacement auquel vous aurez accès lors du processus de déploiement. Pour une liste à jour des versions ESXi prises en charges de cette version, voir les Notes de mise à jour.

- *OpenManage Integration for VMware vCenter* prend uniquement en charge le mode BIOS pour déployer automatiquement l'hyperviseur sur le serveur cible. Assurez-vous que le mode BIOS est sélectionné dans le profil matériel de référence avant d'appliquer le profil d'hyperviseur. S'il n'existe pas de profil matériel sélectionné, assurez-vous de configurer manuellement le mode d'amorçage BIOS et redémarrez le serveur avant d'appliquer le profil d'hyperviseur.

REMARQUE : Le déploiement du système d'exploitation à partir d'OpenManage Integration pour VMware et vCenter (OMIVV) échoue si le mode d'amorçage (BOOT) de la machine cible est défini sur UEFI.

Présentation de l'allocation

À la fin de l'inventaire physique du datacenter, tous les systèmes métal nu découverts automatiquement sont mis à la disposition de l'OpenManage Integration for VMware vCenter pour effectuer le déploiement d'hyperviseur et l'allocation matérielle sans intervention. Pour préparer l'allocation et le déploiement, vous devez :

Créer un profil matériel	Contient les paramètres matériels rassemblés à partir d'un serveur de référence utilisé pour déployer de nouveaux serveurs. Voir Création d'un nouveau profil matériel.
Créer un profil d'hyperviseur	Contient les informations d'installation d'hyperviseur nécessaires au déploiement ESX/ESXi. Voir Création d'un nouveau profil d'hyperviseur.
Créer un modèle de déploiement	Contient un profil matériel et / ou un profil d'hyperviseur. Vous pouvez enregistrer et réutiliser ces profils pour tous les serveurs du centre de données disponibles. Voir Construction de modèles de déploiement.

Après avoir créé le modèle de déploiement, utilisez l'Assistant Déploiement pour rassembler les informations nécessaires pour créer un travail planifié qui alloue le matériel serveur et déploie de nouveaux hôtes dans vCenter. Pour plus d'informations sur l'exécution de l'Assistant Deployment (Déploiement), voir Exécution de l'Assistant Déploiement. Enfin, utilisez File d'attente des tâches pour afficher l'état des tâches et effectuer des changements sur les tâches de déploiement en attente.

REMARQUE : Pas plus de deux tâches de déploiement doivent être planifiées pour s'exécuter consécutivement. Les tâches multiples doivent utiliser la fonction de planification pour échelonner l'exécution du déploiement.

Comprendre les heures de tâches de déploiement

L'allocation et le déploiement de serveurs métal nu peuvent prendre de 30 minutes à plusieurs heures, en fonction de certains 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 à l'allocation et au déploiement varie en fonction du type de déploiement, de la complexité et du nombre de tâches de déploiement exécutées simultanément. Le tableau ci-dessous donne des indications sur la durée approximative d'une tâche de déploiement. Les tâches de déploiement sont exécutées par lots de jusqu'à cinq serveurs simultanés, afin de raccourcir la durée totale de la tâche de déploiement. Le nombre exact de tâches simultanées dépend des ressources disponibles.

Tableau 2. Scénarios de durée approximative de déploiement

Type de déploiement	Durée approximative par déploiement
Hyperviseur uniquement	De 30 à 130 minutes
Matériel uniquement	Jusqu'à 2 heures en fonction de la complexité et des options RAID, BIOS et de démarrage à configurer
Profils matériel et hyperviseur	De 1 à 4 heures

États du serveur dans la séquence de déploiement

Quand un travail d'inventaire est exécuté, les systèmes métal nu découverts automatiquement sont classés dans différents états pour aider à déterminer si le serveur est nouveau dans le centre de données ou a une tâche de déploiement en attente prévue. Les administrateurs peuvent utiliser ces états afin de déterminer si un serveur doit être inclus dans un travail de déploiement. Les états sont :

Non configuré	Le serveur a contacté le OpenManage Integration for VMware vCenter et attend d'être configuré. Voir Comprendre les heures de tâches de déploiement.
Configuré	Le serveur est configuré avec toutes les informations matérielles requises pour réussir le déploiement de l'hyperviseur.

Téléchargement d'images ISO Dell personnalisées

Les images ESXi personnalisées qui contiennent *tous* les lecteurs Dell sont requises pour le déploiement. Dell ne peut pas produire des images ESX 4.1 personnalisées. Pour que les déploiements fonctionnent, *tous* les pilotes doivent être présents nativement dans les produits VMware ISO. Pour une liste à jour des versions ESXi prises en charge de cette version, voir les Notes de mise à jour.

REMARQUE : L'ISO du OpenManage Integration for VMware vCenter ne contient pas les images ISO ESXi requises pour le déploiement. Vous devez télécharger ces images à un emplacement accessible durant le déploiement, sinon celui-ci pourra échouer.

1. Accédez à **support.dell.com**.
2. Allez sur la page **Pilotes et téléchargements** dans votre langue, puis procédez comme suit :
   - Pour sélectionner les pilotes avec le numéro de service ou le code de service express, sous **Oui** dans la zone de texte, entrez le numéro de service ou le code de service express, puis cliquez sur **Envoyer**.
   - Pour sélectionner les pilotes avec une autre méthode, sous **Non**, sélectionnez l'une des options suivantes :
     - Automatically detect my Service Tag for me (Détecter automatiquement le numéro de service)
     - Choose from My Products and Services List (Choisir dans la liste Mes produits et services)
     - Choose from a list of all Dell products (Choisir dans la liste de tous les produits Dell)

     Ensuite, cliquez sur **Continuer** et suivez les instructions correspondant à l'option choisie.
3. Sur la page du serveur sélectionné, défilez vers le bas jusqu'à **Affiner les résultats** et sous **Système d'exploitation**, utilisez la liste déroulante pour sélectionner le système ESX ou ESXi désiré.
4. Cliquez sur **Solutions d'entreprise**.
5. Dans la liste **Solutions Enterprise**, sélectionnez la version d'ISO requise, puis cliquez sur **Télécharger le fichier**.

   REMARQUE : Les ISO intégrés sont utilisés pour les installations d'hyperviseur sur doubles modules SD internes. Les ISO installables sont pour les installations sur disques durs.
6. Dans la boîte de dialogue, sélectionnez **Pour un téléchargement de fichier unique via le navigateur**, puis cliquez sur **Télécharger maintenant**.
7. Dans la boîte de dialogue, allez à l'emplacement de stockage des images ISO pour le déploiement.

Comprendre la manière de configurer un profil matériel

Pour configurer les paramètres matériels d'un serveur, vous devez créer un profil matériel. Un profil matériel est un modèle de configuration que vous pouvez appliquer aux composants de l'infrastructure nouvellement découverts ; il nécessite les informations suivantes :

Séquence de démarrage	La séquence de démarrage est la séquence de périphérique de démarrage et séquence de disque dur, que vous pouvez modifier uniquement si le mode de démarrage est sur BIOS.
Paramètres du BIOS	Les paramètres du BIOS comprennent : mémoire, processeur, SATA, périphériques intégrés, communications série, gestion de serveur intégrée, gestion de l'alimentation, sécurité système, et divers paramètres.
iDRAC Settings (Paramètres iDRAC)	Les paramètres iDRAC comprennent : réseau, liste d'utilisateurs et configuration d'utilisateurs (privilèges IPMI/iDRAC). **REMARQUE :** Pour les systèmes dotés d'iDRAC Express, la configuration iDRAC ne peut pas être extraite ; le serveur ne doit donc pas être utilisé comme serveur de référence. S'il est utilisé comme système cible, aucune configuration iDRAC du serveur de référence n'est appliquée.
Configuration RAID	La configuration RAID affiche la topologie RAID actuelle sur le serveur de référence server au moment où le profil matériel a été extrait. **REMARQUE :** Deux options de configuration RAID sont configurées dans le Profil matériel : 1. *Appliquez RAID1 et créez un disque de secours dédié, applicable*. Utilisez l'option si vous souhaitez appliquer les paramètres de configuration RAID par défaut au serveur cible. La tâche de configuration RAID passe à RAID1 par défaut sur les deux premiers lecteurs du contrôleur intégré qui prennent en charge RAID1. De plus, un disque de secours dédié est créé pour la matrice RAID1 si un disque candidat répondant aux critères existe. 2. *Clonez la configuration RAID depuis le serveur de référence, tel qu'indiqué ci-dessous*. Utilisez cette option si vous souhaitez cloner le paramètre du serveur de référence. Voir Création d'un nouveau Profil matériel. **REMARQUE :** Le OpenManage Integration for VMware vCenter active certains paramètres du BIOS dans le groupe Processeur dans le BIOS sur tous les serveurs déployés, quels que soient les paramètres sur le serveur de référence. Pour que vous puissiez utiliser un serveur de référence pour créer un nouveau profil matériel, le paramètre Collecte de l'inventaire du système au redémarrage (CSIOR) doit être activé et un redémarrage doit être effectué pour fournir des informations d'inventaire et de configuration exactes.

Les tâches de création de profils matériels comprennent :

- Activation de CSIOR sur un serveur de référence
- Création d'un nouveau profil matériel
- Clonage d'un nouveau profil matériel
- À propos de la gestion des profils matériels

Création d'un nouveau profil matériel

Pour créer un nouveau profil matériel :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils matériels.**.
2. Cliquez sur **Créer nouveau**.
3. Sur la page **Nouveau profil matériel**, procédez ainsi :
    - Dans la zone de texte **Nom de profil**, entrez le nom du profil
    - Dans la zone de texte **Description**, entrez une description optionnelle.

4. Cliquez sur **Enregistrer**.
5. Pour continuer, dans le volet gauche, cliquez sur **Serveur de référence**.
6. Dans la fenêtre Serveur de référence, cliquez sur **Modifier**.
7. Pour trouver un serveur de référence compatible, géré par vCenter et correctement inventorié par l'OpenManage Integration for VMware vCenter, cliquez sur **Parcourir**.
8. Dans la boîte de dialogue **Serveurs**, défilez vers le bas de la liste pour trouver le bon serveur de référence, puis cliquez sur **Sélectionner**.
9. Pour personnaliser les paramètres du serveur de référence comme valeurs par défaut, cliquez sur **Personnaliser les paramètres du serveur de référence**) puis cliquez sur **Enregistrer**.
10. Une boîte de dialogue vous informant que l'extraction des paramètres prend quelques minutes est affichée. Pour renseigner les paramètres, cliquez sur **Continuer**. Le nom, l'adresse IP iDRAC et le numéro de service du serveur sélectionné sont affichés dans la fenêtre **Serveur de référence**.
11. Dans le volet gauche, sélectionnez **Séquence de démarrage**. Pour inclure des informations sur la séquence de démarrage dans le profil, cochez la case **Inclure la séquence de démarrage dans ce profil matériel**.
12. Pour afficher les options de séquence de démarrage, développez **Séquence de démarrage** puis cliquez sur **Modifier** pour effectuer des mises à jour :

    REMARQUE : Pour les serveurs PowerEdge Dell de 13e génération, seules les informations relatives au mode de démarrage actuel sont affichés pour les profils matériels.

    REMARQUE : Le déploiement du système d'exploitation à partir d'OpenManage Integration pour VMware et vCenter échoue si le mode d'amorçage (BOOT) de la machine cible est défini sur UEFI.

    a. Dans la liste déroulante **Mode de démarrage**, sélectionnez BIOS ou UEFI.
    b. Dans la liste déroulante **Afficher/Configurer**, sous **Séquence de périphériques de démarrage**, pour apporter des changements à la séquence de périphériques de démarrage affichée, sélectionnez le périphérique, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
    c. Dans la liste déroulante **Retentative de séquence de démarrage**, sélectionnez **Activé** pour que le serveur retente automatiquement la séquence de démarrage, ou sélectionnez **Désactivé** pour ne pas retenter la séquence.
    d. Cliquez sur **Enregistrer** pour enregistrer les modifications ou sur **Annuler** pour annuler les modifications.
13. Si **Mode de démarrage du BIOS** a été sélectionné, vous pouvez développer **Séquence de disques durs** pour afficher les options de séquence de disques durs, puis cliquez sur **Modifier** pour effectuer des mises à jour :

    - Pour modifier la séquence de disques durs affichée, sélectionnez le périphérique et cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
    - Cliquez sur **Enregistrer** pour enregistrer les modifications ou sur **Annuler** pour annuler les modifications.
14. Dans le volet gauche, sélectionnez **Paramètres BIOS**. Pour inclure les informations de paramètres BIOS dans le profil, sélectionnez la case **Inclure les paramètres BIOS dans ce profil matériel**. Développez une catégorie pour afficher les options de paramètres, et cliquez sur **Modifier** pour effectuer des mises à jour des paramètres suivants :

    - Memory Settings (Paramètres de mémoire)
    - Processor Settings (Paramètres du processeur)
    - Paramètres SATA
    - Integrated Devices (Périphériques intégrés)
    - Serial Communication (Communications série)
    - Gestion de serveur intégrée
    - Power Management (Gestion de l'alimentation)
    - System Security (Sécurité du système)
    - Miscellaneous Settings (Paramètres divers)

Après avoir effectué toutes les mises à jour d'une catégorie, cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Annuler** pour annuler les modifications.

REMARQUE : Pour obtenir des informations détaillées sur le BIOS, y compris les options et explications des paramètres, reportez-vous au *Manuel du propriétaire du matériel* du serveur sélectionné.

15. Dans le volet gauche, sélectionnez **Paramètres iDRAC**, puis sélectionnez **Réseau**.
16. Pour inclure les informations de paramètres réseau dans le profil, sélectionnez la case **Inclure les paramètres réseau dans ce profil matériel**. Développez une catégorie pour afficher les options de paramètres, et cliquez sur **Modifier** pour effectuer des mises à jour des paramètres suivants :

    - Réseau
    - Paramètres réseau
    - Média virtuel

    Après avoir effectué toutes les mises à jour d'une catégorie, cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Annuler** pour annuler les modifications.

    REMARQUE : Pour obtenir des informations détaillées sur le BIOS, y compris les options et explications des paramètres, reportez-vous au *Manuel du propriétaire iDRAC* du serveur sélectionné.
17. Dans le volet gauche, sélectionnez **Paramètres iDRAC → Liste d'utilisateurs**. Pour inclure les informations de liste d'utilisateurs dans le profil, cochez la case **Inclure la liste d'utilisateurs dans ce profil matériel**. Sous Liste d'utilisateurs iDRAC locale, procédez ainsi :
    a. **Ajouter un utilisateur** : entrez manuellement un utilisateur iDRAC et les informations requises. Lorsque vous avez terminé, cliquez sur **Enregistrer** pour enregistrer les modifications ou **Annuler** pour annuler.
    b. **Supprimer un utilisateur** : supprimez l'utilisateur sélectionné. Sélectionnez la case de l'utilisateur et cliquez sur **Supprimer** ou cliquez sur **Annuler** pour annuler.
    c. **Modifier un utilisateur** : modifiez manuellement les informations d'un utilisateur iDRAC. Lorsque vous avez terminé, cliquez sur **Enregistrer** pour enregistrer les modifications ou **Annuler** pour annuler.

    REMARQUE : Pour obtenir des informations détaillées sur le BIOS, y compris les options et explications des paramètres, reportez-vous au *Manuel du propriétaire iDRAC* du serveur sélectionné.
18. Dans le volet gauche, sélectionnez **Configuration RAID**. Pour inclure les informations de configuration RAID dans le profil, sélectionnez la case **Inclure la configuration RAID dans ce profil matériel**. La fenêtre est mise à jour avec toutes les informations RAID.

    - Appliquez RAID1 et créez un disque de secours dédié, applicable.

      Utilisez l'option si vous souhaitez appliquer les paramètres de configuration RAID par défaut au serveur cible. La tâche de configuration RAID passe à RAID1 par défaut sur les deux premiers lecteurs du contrôleur intégré qui prennent en charge RAID1. De plus, un disque de secours dédié est créé pour la matrice RAID1 si un disque candidate répondant aux critères existe.
    - Clonez la configuration RAID depuis le serveur de référence, tel qu'indiqué ci-dessous.

      Utilisez cette option si vous souhaitez cloner le paramètre du serveur de référence.

    Le profil est enregistré et s'affiche dans la fenêtre **Profils matériels** sous **Profils disponibles**.

Activation de CSIOR sur un serveur de référence

Avant de créer un profil matériel à l'aide d'un serveur de référence, activez le paramètre Collect System Inventory On Reboot (CSIOR) (Collecte de l'inventaire du système au redémarrage) et redémarrez le serveur pour fournir des informations d'inventaire et de configuration exactes. Il y a deux méthodes pour activer CSIOR :

Localement	Cette méthode utilise un hôte individuel utilisant l'interface utilisateur Dell Lifecycle Controller United Server Configurator (USC).

À distance	Cette méthode utilise un script WS-Man. POur plus d'informations sur les scripts de cette fonctionnalité, voir *Centre technique Dell* et *Profil de gestion DCIM Lifecycle Controller Manager*.

Pour activer CSIOR localement sur un serveur de référence :

1. Mettez le système sous tension, et durant le POST appuyez sur **<F10>** pour lancer USC.
2. Sélectionnez **Configuration matériellen → Configuration de remplacement de pièce**.
3. Activez le paramètre **Collecte de l'inventaire du système au redémarrage** et quittez USC.

Clonage d'un profil matériel

Pour cloner un nouveau profil matériel :

1. Dans le Dell Management Center, sélectionnez **Déploiement → Modèles de déploiement → Profils matériels**.
2. Cliquez sur **Créer nouveau**.
3. Sur la page **Nouveau profil matériel**, procédez ainsi :
   - Dans la zone de texte **Nom de profil**, entrez le nom du profil
   - Dans la zone de texte **Description**, entrez une description optionnelle.
4. Cliquez sur **Enregistrer**.
5. Dans le volet gauche, cliquez sur **Serveur de référence**.
6. Dans la fenêtre **Serveur de référence**, cliquez sur **Modifier**.
7. Pour extraire tous les paramètres matériels du serveur de référence, cliquez sur l'option **Cloner les paramètres du serveur de référence**.
8. Cliquez sur **Enregistrer**.
9. Une boîte de dialogue vous informant que l'extraction des paramètres prend quelques minutes est affichée. Cliquez sur **Continuer**. Les paramètres sont renseignés, et le nom, l'adresse IP iDRAC et le numéro de service du serveur sélectionné sont affichés dans la fenêtre Serveur de référence.

   Le profil est enregistré et s'affiche dans la fenêtre **Profils matériels** sous **Profils disponibles**.

À propos de la gestion des profils matériels

Les profils matériels définissent la configuration matérielle d'un serveur à partir d'un serveur de référence. Dans le Dell Management Center, il existe plusieurs actions de gestion que vous pouvez effectuer sur les profils matériels existants, y compris :

- Afficher ou modifier un profil matériel
- Dupliquer des profils matériels
- Renommer un profil matériel
- Supprimer un profil matériel
- Actualiser des profils matériels

Afficher ou modifier un profil matériel

Pour afficher ou modifier un profil matériel :

1. Dans le Dell Management Center, sélectionnez **Déploiement → Modèles de déploiement → Profils matériels**.
2. Sélectionnez un profil et cliquez sur **Afficher/Modifier**.
3. Dans la fenêtre **Profil matériel**, pour effectuer des modifications, cliquez sur **Modifier**.

4. Cliquez sur **Enregistrer** pour appliquer les modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Duplication d'un profil matériel

Pour dupliquer un profil matériel :

1. Dans Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils matériels**.
2. Sur la page **Profil matériel**, sélectionnez un profil et cliquez sur **Dupliquer**.
3. Dans la boîte de dialogue **Dupliquer**. entrez un nom de profil matériel unique.
4. Cliquez sur **Appliquer** pour créer une copie du profil avec le nouveau nom, ou cliquez sur **Annuler** pour annuler.

Renommer un profil matériel

Pour renommer un profil matériel :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils matériels**.
2. Sur la page **Profil matériel**, sélectionnez un profil et cliquez sur **Renommer**.
3. Dans la boîte de dialogue **Renommer**, entrez un nom de profil matériel unique.
4. Cliquez sur **Appliquer** pour utiliser le nouveau nom ou cliquez sur **Annuler** pour annuler.

Supprimer un profil matériel

Pour supprimer un profil matériel :

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

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils matériels.**.
2. Sélectionnez unprofil et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de message, pour supprimer le profil, cliquez sur **Supprimer**, ou cliquez sur **Annuler** pour annuler.

Actualisation d'un profil matériel mis à jour

Pour actualiser un profil matériel mis à jour :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils matériels.**.
2. Cliquez sur **Rafraîchir**.

   Les informations du profil matériel mis à jour s'affichent.

Création d'un nouveau profil d'hyperviseur

Pour déployer et configurer ESX/ESXi sur un serveur, un profil d'hyperviseur doit être créé. Un profil d'hyperviseur exige les informations suivantes :

- L'emplacement du support logiciel ISO de référence scriptable sur un partage NFS ou CIFS
- L'instance vCenter qui gère les hôtes déployés, plus un profil d'hôte facultatif
- Le centre de données ou cluster de destination où le plug-in déploie les serveurs dans vCenter

REMARQUE : Utilisez l'une des conventions de désignation suivantes pour le nom du fichier ISO de référence :

```
NFS format: host:/share/hypervisor_image.iso

CIFS format: \\host\share\hypervisor.iso
```

REMARQUE : Un déploiement réussi nécessite un ISO ESX doté des bons pilotes. Le déploiement sur les nouveaux systèmes Dell peut nécessiter l'utilisation d'images ISO personnalisées Dell qui contiennent tous les pilotes Dell nécessaires. ESX 4.1 peut ne pas fonctionner sur les nouveaux systèmes Dell et peut ne pas avoir d'ISO personnalisé disponible auprès de Dell.

Pour créer un nouveau profil d'hyperviseur :

1. Dans **Dell Management Center**, sélectionnez**Déploiement** → **Modèles de déploiement** → **Profil d'hyperviseu**.
2. Sur la page **Profils d'hyperviseur**, cliquez sur **Créer nouveau**.
3. Sur la page **Nouveau profil d'hyperviseur**, procédez ainsi :
   - Dans la zone de texte **Nom de profil**, entrez le nom du profil
   - Dans la zone de texte **Description**, entrez une description optionnelle.
4. Dans le volet gauche, cliquez sur **ISO de référence**, puis cliquez sur **Modifier**, et dans la boîte de dialogue **Source d'installation de l'hyperviseur**, entrez les informations suivantes :
   - Dans la zone de texte **IISO de source d'installation** , entrez le chemin de l'emplacement de partage de l'hyperviseur. Une copie de cette image d'hyperviseur est modifiée pour permettre une installation par script. L'emplacement de l'ISO de référence doit adopter l'un des formats suivants :

     Format NFS : host:/share/hypervisor_image.iso

     Format CIFS : \\host\share\hypervisor.iso
   - Dans la liste déroulante **Sélectionner une version**, sélectionnez une version ESX ou ESXi.

   Tous les serveurs déployés avec ce profil d'hyperviseur auront cette image, et si les serveurs sont d'une version antérieure à 12G, la dernière version recommandée d'OpenManage Server Administrator est installée.
5. Si vous utilisez un partage CIFS, entrez le **Nom d'utilisateur**, le **Mot de passe** et **Vérifiez le mot de passe**. Les mots de passe doivent concorder.
6. Pour ajouter les paramètres au profil, cliquez sur **Enregistrer**.
7. Dans le panneau gauche, cliquez sur **Paramètres vCenter**, puis apportez des modifications là où nécessaire :
   - **Instance vCenter** : affiche l'instance de serveur qui gère un hôte après le déploiement.
   - **Version vCenter** : affiche la version actuelle.
   - **Conteneur de destinations vCenter** : centre de données ou cluster qui héberge les nouveaux serveurs physiques ; cliquez sur **Parcourir** pour rechercher les destinations vCenter
   - **Profil d'hôte vCenter** : un profil qui englobe la configuration de l'hôte et aide à gérer la configuration de l'hôte
8. Pour ajouter les informations au profil, cliquez sur **Enregistrer**.

Pour plus d'informations sur la gestion des profils d'hyperviseur, voir Gestion des profils d'hyperviseur.

Gestion des profils d'hyperviseur

Il y a plusieurs actions de gestion que vous pouvez effectuer sur les profils d'hyperviseur existants, y compris :

- Comprendre la prise en charge VLAN
- Affichage ou modification des profils d'hyperviseur
- Dupliquer des profils d'hyperviseur
- Renommer des profils d'hyperviseur

- Suppression d'un profil d'hyperviseur
- Actualisation de profils d'hyperviseur

Prise en charge VLAN

Le OpenManage Integration for VMware vCenter prend en charge le déploiement d'hyperviseur vers un VLAN routable. Configurez la prise en charge VLAN dans l'Assistant Déploiement. Dans cette section de l'Assistant Déploiement, vous avez l'option de spécifier l'utilisation des VLAN et de spécifier un ID VLAN. Lorsqu'un ID VLAN est fourni, il est appliqué à l'interface de gestion de l'hyperviseur lors du déploiement et marque tout le trafic doté de l'ID VLAN.

Assurez-vous que le VLAN fourni lors du déploiement communique avec l'appliance virtuelle et le serveur vCenter. Le déploiement d'un hyperviseur vers un VLAN qui ne peut pas communiquer vers une des/les deux destinations provoque l'échec du déploiement.

Si vous avez sélectionné plusieurs serveurs sans système d'exploitation dans une tâche de déploiement unique et que vous souhaitez appliquer le même ID VLAN à tous les serveurs, utilisez le bouton *Appliquer les paramètres à tous les serveurs sélectionnés*, qui se trouve sous Paramètres par défaut dans la section Identification de serveur de l'Assistant Déploiement. Cette option vous permet d'appliquer le même ID VLAN ainsi que d'autres paramètres réseau à tous les serveurs de cette tâche de déploiement.

REMARQUE : Le OpenManage Integration for VMware vCenter ne prend pas en charge une configuration multiconnexions. L'ajout d'une deuxième interface réseau à l'appliance pour une communication avec un deuxième réseau entraîne des problèmes pour les flux de travail reliés au déploiement d'hyperviseur, à la conformité du serveur et aux mises à jour de micrologiciel.

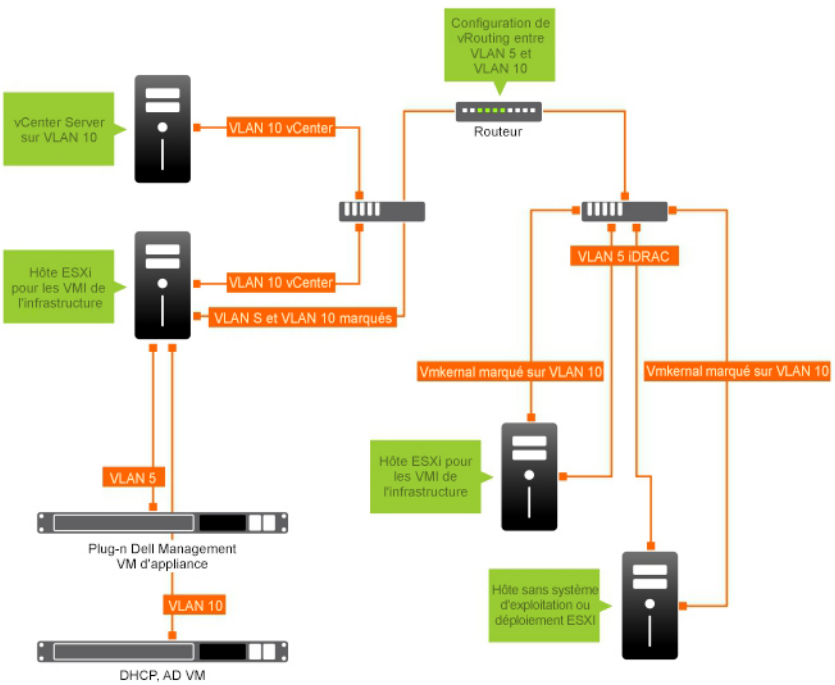

Figure 4. Exemple de réseau VLAN.

Dans cet exemple de réseau, le OpenManage Integration for VMware vCenter est sur VLAN 5, alors que le vCenter et le VMkernal des hôtes ESXi en cours de déploiement sont sur VLAN 10. Comme le OpenManage Integration for VMware vCenter ne prend pas en charge la connexion de plusieurs VLAN, VLAN 5 doit se router vers VLAN 10 pour que tous les systèmes communiquent entre eux correctement. Si le routage n'est pas activé entre ces VLAN, le déploiement échoue.

Affichage ou modification des profils d'hyperviseur

Pour afficher ou modifier les profils d'hyperviseur :

1. Dans le Dell Management Center, sélectionnez la fenêtre **Déploiement** → **Modèles de déploiement** → **Profils d'hyperviseur**.
2. Sélectionnez un profil et cliquez sur **Afficher/Modifier**.
3. Dans la fenêtre **Profils d'hyperviseur : nom du profil**, sélectionnez la section de profil à afficher ou modifier et effectuez les modifications nécessaires.
4. Cliquez sur **Enregistrer** pour appliquer les modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Duplication d'un profil d'hyperviseur

Pour dupliquer un profil d'hyperviseur :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils d'hyperviseur**.
2. Sur la page **Profils d'hyperviseur**, sélectionnez un profil et cliquez sur **Dupliquer**.
3. Dans la boîte de dialogue **Dupliquer**, entrez un nom de profil d'hyperviseur unique.
4. Cliquez sur **Appliquer** pour créer une copie du profil avec le nouveau nom, ou cliquez sur **Annuler** pour annuler.

Renommer un profil d'hyperviseur

Pour renommer un profil d'hyperviseur :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiemen** → **Profils d'hyperviseur.**
2. Sur la page **Profils d'hyperviseur**, sélectionnez un profil et cliquez sur **Renommer**.
3. Dans la boîte de dialogue **Renommer**, entrez un nom de profil d'hyperviseur unique.
4. Cliquez sur **Appliquer** pour utiliser le nouveau nom ou cliquez sur **Annuler** pour annuler.

Suppression d'un profil d'hyperviseur

Pour supprimer un profil d'hyperviseur :

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

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils d'hyperviseur**.
2. Sélectionnez unprofil et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de message, cliquez sur **Supprimer** pour supprimer le profil, ou cliquez sur **Annuler** pour annuler.

Actualisation de profils d'hyperviseur

Pour actualiser un profil d'hyperviseur mis à jour :

1. Dans Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** → **Profils d'hyperviseur**.
2. Cliquez sur **Rafraîchir**.

   Les informations du profil d'hyperviseur mis à jour s'affichent.

Construction d'un nouveau modèle de déploiement

A modèle de déploiement contient un profil matériel et / ou un profil d'hyperviseur. L'Assistant Déploiement utilise ce modèle pour allouer le matériel de serveur et déployer les hôtes dans vCenter.

Pour contruire un nouveau modèle de déploiement :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement**.
2. Sous **Profils disponibles**, cliquez sur **Créer nouveau**.
3. Dans la fenêtre **Créer nouveau**, entrez un nom pour le modèle, puis cliquez sur **Enregistrer**.
4. Pour complèter le modèle, cliquez sur **Modifier**.
5. Dans le volet droit, dans la liste déroulante **Profil** , choisissez un profil, et procédez ainsi :
   - Pour afficher les paramètres de profil matériel/hyperviseur du profil sélectionné, cliquez sur **Afficher**.
   - Pour créer un nouveau profil matériel/hyperviseur, cliquez sur **Créer nouveau**.
6. Entrez une **Description** optionnelle pour le modèle de déploiement qui sera utile pour gérer le modèle.
7. Pour appliquer les sélections de profil et enregistrer les modifications, cliquez sur **Enregistrer**. Pour annuler, cliquez sur **Annuler**.

Gestion des modèles de déploiement

Dans Dell Management Center, vous pouvez effectuer plusieurs actions de gestion sur les modèles de déploiement existants, y compris :

- Construire des modèles de déploiement
- Dupliquer des modèles de déploiement
- Renommer des modèles de déploiement
- Supprimer un modèle de déploiement

Dupliquer des modèles de déploiement

Pour dupliquer un modèle de déploiement :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** .
2. Sur la page Modèles de déploiement, sélectionnez un modèle et cliquez sur **Dupliquer**.
3. Entrez le nouveau nom du modèle et cliquez sur **Appliquer**. Le modèle doit avoir un nom unique.

Supprimer un modèle de déploiement

Pour supprimer un modèle de déploiement :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement** .
2. Sur la page **Modèles de déploiement**, sélectionnez un modèle et cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer** sur la zone de message pour supprimer le modèle ou cliquez sur **Annuler** pour annuler.

Renommer un modèle de déploiement

Pour renommer un modèle de déploiement :

1. Dans le Dell Management Center, sélectionnez **Déploiement** → **Modèles de déploiement**.
2. Sur la page **Modèles de déploiement**, sélectionnez un modèle et cliquez sur **Renommer**.
3. Entrez le nouveau nom du modèle et cliquez sur **Appliquer**. Le modèle doit avoir un nom unique.

4. Pour afficher tous les modèles de déploiement, dans le **Dell Management Center**, sélectionnez **Déploiement** → **Modèles de déploiement** et cliquez sur **Rafraîchir**.

Exécution de l'Assistant Déploiement

L'Assistant Déploiement vous guide à travers le processus de déploiement de serveurs métal nu :

- Sélection de serveurs non déployés.

  Lorsque vous déployez l'hyperviseur, vous pouvez le déployer sur un double module SD interne doté d'un minimum de 1 Go de stockage. Le double module SD interne doit être activé dans le BIOS avant le déploiement de l'hyperviseur avec le OpenManage Integration for VMware vCenter.
- Utilisation d'un modèle de déploiement (combinaison de profils matériel et hyperviseur).
- Configuration des paramètres globaux. Cette page vous permet de choisir de déployer l'hyperviseur sur un disque dur ou un double module SD interne.
- Attribution d'une identification aux serveurs déployés.
- Mise en rapport d'un profil de connexion souhaité avec chaque serveur.
- Planification de l'exécution de travaux de déploiement de serveur.
- Affichage de la file d'attente où vous pouvez gérer les tâches de déploiement.

REMARQUE : Si vous déployez uniquement un profil matériel, les nouvelles pages Paramètres globaux, Identification du serveur et Profil de connexion sont ignorées et vous accédez directement à la page Planifier des travaux.

REMARQUE : Vous pouvez utiliser l'Assistant Déploiement pour la licence d'essai/évaluation tant que la licence n'a pas expiré.

Tâches connexes :

- Assistant Déploiement — Étape 1: sélection des serveurs
- Assistant Déploiement — Étape 2 : modèles de déploiement
- Assistant Déploiement — Étape 3 : paramètres globaux
- Assistant Déploiement — Étape 4 : identification du serveur
- Assistant Déploiement — Étape 5 : profil de connexion
- Assistant Déploiement — Étape 6 : planifier des tâches

Assistant Déploiement - Étape 1 : sélectionner des serveurs

Cette page couvre le déploiement de serveurs. Si vous souhaitez déployer l'hyperviseur sur un double module SD interne, cette page s'affiche si cette option est disponible ou non. Pour plus d'informations sur les doubles modules SD internes, voir Exécution de l'Assistant Déploiement. Si le serveur que vous souhaitez déployer n'apparaît pas dans la liste de l'étape 2, vous pouvez ajouter manuellement un serveur pour qu'il s'affiche dans la liste de cette étape ; voir Ajout manuel d'un serveur.
Pour sélectionner des serveurs :

1. Dans **Dell Management Center**, sélectionnez**Déploiement** → **Assistant Déploiemend**.
2. Dans la fenêtre **Sélectionner des serveurs**, pour attribuer des serveurs non déployés à cette tâche de déploiement, utilisez les cases pour sélectionner les **serveurs**.
3. Cliquez sur **Suivant**.

Pour passer à l'étape 2, cliquez sur Assistant Déploiement — Étape 2

Assistant Déploiement — Étape 2 : modèles de déploiement

Les déploiements sur un profil matériel diffèrent des déploiements d'hyperviseur. Si vous déployez sur un profil matériel, cliquez sur Assistant Déploiement — Étape 6.

REMARQUE : Un déploiement réussi nécessite un ISO ESX doté des bons pilotes. Le déploiement sur les nouveaux systèmes Dell peut nécessiter l'utilisation d'images ISO personnalisées Dell qui contiennent tous les pilotes Dell nécessaires. ESX 4.1 peut ne pas fonctionner sur les nouveaux systèmes Dell et peut ne pas avoir d'ISO personnalisé disponible auprès de Dell.

Pour sélectionner un modèle de déploiement :

1. La fonctionnalité Modèle de déploiement sélectionne/crée un modèle de déploiement de l'une des façons suivantes :
   - Sélectionnez un modèle de déploiement existant sous **Modèles disponibles**. Les informations du modèle sélectionné renseignent le volet droit.
   - Sélectionnez un modèle de déploiement existant, puis cliquez sur **Modifier** pour modifier un ou deux profils associés.
   - Cliquez sur **Créer nouveau** pour définir un nouveau modèle.
2. Sélectionnez l'une des options suivantes :
   - Si vous déployez sur un profil matériel, cliquez sur **Suivant**, ce qui vous amène à Assistant Déploiement — Étape 6.
   - Si vous déployez sur un profil d'hyperviseur, cliquez sur **Suivant**, ce qui vous amène à Assistant Déploiement — Étape 3.

Assistant Déploiement — Étape 3 : paramètres globaux

Vous pouvez déployer l'hyperviseur sur un disque dur ou un Internal Dual SD Module (double module interne SD). Si un Internal Dual SD Module est disponible sur au moins l'un des serveurs sélectionnés, l'option **double module interne SD** est activée par défaut. Si ce n'est pas le cas, aucune des options **disque dur** ou **double module interne SD** ne sont sélectionnées.

Pour le déploiement de l'hyperviseur, effectuez les opérations suivantes :

1. Dans la page Paramètres globaux, sélectionnez l'une des options suivantes :
   - **Disque dur** : déploie l'hyperviseur sur le lecteur de disque dur.
   - **Double module interne SD** : déploie l'hyperviseur sur un double module SD interne.
2. Si l'un des serveurs sélectionnés ne prend pas en charge un double module SD interne, ou si un double module SD interne n'est pas présent lors du déploiement, effectuez l'une des actions suivantes :
   - Cochez la case **Déployer l'hyperviseur sur le premier disque dur des serveurs qui ne disposent pas d'un double module SD interne** si vous souhaitez déployer l'hyperviseur sur le premier disque dur des serveurs.

     PRÉCAUTION : Si vous sélectionnez cette option et effectuez le déploiement de l'hyperviseur sur le premier disque dur des serveurs, toutes les données présentes sur le lecteur de disque seront effacées.
   - Décochez la case **Déployer l'hyperviseur sur le premier disque dur des serveurs qui ne disposent pas d'un double module SD interne** afin d'ignorer le déploiement sur ces serveurs et de continuer le déploiement de l'hyperviseur sur le serveur suivant.
3. Cliquez sur **Suivant**.

   Pour passer à l'étape 4, cliquez sur Assistant Déploiement — Étape 4 : identification du serveur.

Assistant Déploiement — Étape 4 : identification du serveur

L'identification du serveur peut être fournie de deux manières :

- Entrez les informations réseau (adresse IP, masque de sous-réseau et passerelle) ; un nom de domaine entièrement qualifié pour le nom d'hôte est obligatoire. L'utilisation de *localhost* pour le FQDN n'est pas prise en charge. Le FQDN est utilisé lors de l'ajout de l'hôte à vCenter.
- Utilisez le DHCP (Dynamic Host Configuration Protocol) pour configurer les adresses IP, le masque de sous-réseau, l'IP de passerelle, le nom d'hôte et les serveurs DNS préférés/de remplacement. Le DHCP attribué à l'adresse IP sera utilisé lors de l'ajout de l'hôte à vCenter. Lorsque vous utilisez DHCP, nous vous recommandons vivement d'utiliser une réservation IP pour les adresses MAC NIC sélectionnées.

REMARQUE : Utilisez un FQDN (Fully Qualified Domain Name) pour le nom d'hôte au lieu de l'hôte local. À partir d'ESXi 5.1, une valeur d'hôte local empêche le plug-in Dell Management de traiter des événements envoyés de l'hôte. Créer un enregistrement DNS qui résoud l'adresse IP au FQDN. Pour que les alertes SNMP dESXi 5.1 soient identifiées correctement, 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.

Cet écran offre l'option de spécifier un ID VLAN. Lorsqu'un ID VLAN est fournit, il est appliqué à l'interface de gestion de l'hyperviseur lors du déploiement et marque tout le trafic doté de l'ID VLAN.
Pour identifier le serveur :

1. La fonctionnalité Identification du serveur attribue de nouveaux noms et identification réseau aux serveurs déployés. Pour afficher une liste des serveurs qui ne satisfont pas les conditions minimum en matière de micrologiciel ou BIOS, ou qui ont d'autres problèmes, cliquez sur **Serveurs non conformes**.
2. Pour des informations supplémentaires, cliquez sur **Aide**.
3. Une fois les systèmes mis à jour, cliquez sur **Vérifier la conformité** pour retester et vérifier les corrections. Pour actualiser la liste, cliquez sur **Refraîchir**, et cliquez sur **Annuler tous les tests** pour annuler les tests.
4. Cliquez sur **^** pour développer et afficher les informations sur un serveur particulier.
5. Sous **Nom d'hôte et carte réseau**, entrez un **Nm de domaine pleinement qualifié** pour le serveur.
6. Dans la liste déroulante **Tâches de gestion de carte résea**, sélectionnez la carte réseau qui sera utilisée pour gérer le serveur.
7. Entrez les **adresses IP**, le **masque de sous-réseau** et d'autres informations réseau, ou sélectionnez la case **Obtenir avec DHCP**.
8. Lors d'un déploiement vers un réseau exigeant un ID VLAN, cochez la case VLAN et entrez l'ID VLAN.

   Pour l'ID VLAN, utilisez les numéros de 1 à 4094. L'ID VLAN 0 est réservé au marcage de la priorité des trames.
9. Répétez pour tous les serveurs à déployer, ou sélectionnez la case **Appliquer les paramètres à tous les serveurs sélectionnés**.
10. Cliquez sur **Suivant**.

    Pour passer à l'étape 5, cliquez sur Assistant Déploiement — Étape 5

Assistant Déploiement — Étape 5 : profil de connexion

Les profils de connexion sont utilisés pour établir les informations d'identification de connexion des hôtes en les associant aux informations d'identification de racine hôte ou iDRAC. La fenêtre Profils de connexion vous permet de :

- Afficher ou modifier un profil de connexion actuel
- Supprimer un profil de connexion :
- Rafraîchir le profil de connexion pour refléter les modifications apportées à l'hôte vCenter

Pour créer un nouveau profil de connexion :

1. La fonctionnalité Profil de connexion affecte automatiquement des serveurs aux profils de connexion une fois la tâche de déploiement terminée.

   Après avoir sélectionné un profil de connexion, cliquez sur **Suivant**.
2. Sélectionnez l'option **Affecter tous les serveurs au même profil de connexion**, et sélectionnez le profil de connexion dans la liste déroulante pour affecter tous les serveurs au même profil de connexion.
3. Pour créer un nouveau profil, cliquez sur **Nouveau** et pour afficher ou modifier le profil sélectionné, cliquez sur **Afficher/Modifier**.
4. Pour afficher les paramètres du profil de connexion sélectionné, cliquez sur **Afficher**.
5. Sélectionnez l'option **Sélectionner un profil de connexion pour chaque serveur**, puis sélectionnez un profil de connexion particulier pour chaque serveur de la liste déroulante.
6. Après avoir sélectionné un profil de connexion, cliquez sur **Suivant**.

   Pour passer à l'étape 6, cliquez sur Assistant Déploiement — Étape 6.

Assistant Déploiement — Étape 6 : planifier des travaux

La fonctionnalité Planification configure la planification de la tâche de déploiement. Celle-ci peut être exécutée immédiatement, à une date et une heure déterminées, manuellement ou mis en attente.

Pour configurer la planification :

1. Déterminez le moment d'exécution d'un travail de déploiement en entrant une date et une heure :
   a. Cliquez sur **Planifier les serveurs à déployer**.
   b. Servez-vous du calendrier pour sélectionner la date.
   c. Entrez l'heure du jour :

      - Immédiatement : cliquez sur **Déployer les serveurs maintenant**.
      - Reporter la tâche : cliquez sur **Créer une tâche de déploiement**.
      - Mise en attente : avec cette option, seule la planification peut être modifiée et toutes les autres options de travail de déploiement ne peuvent pas être changées.
2. Entrez **Nom de tâche** et **Description de tâche** .
3. Cliquez sur **Terminer**.
4. Vous avez maintenant terminé l'Assistant Déploiement et pouvez donc gérer les tâches de déploiement avec **File d'attente des tâches**.
5. Pour afficher une liste des serveurs non conformes qui doivent effectuer une mise à jour du micrologiciel avant de pouvoir terminer l'Assistant, cliquez sur **Serveurs non conformes**.

Tâches connexes :

- Gestion des tâches de déploiement avec la file d'attente des tâches de déploiement.

Comprendre la file d'attente des tâches

La file d'attente des tâches gère les tâches de récupération de la garantie et de déploiement de serveurs, tels que :

- Affichage des tâches de déploiement de serveurs soumis.
- Actualisation des files d'attente de tâche de déploiement ou d'historique d'inventaire / de garantie.
- Planification d'une tâche d'inventaire pour mettre à jour les attributs de serveur Dell trouvés dans le vCenter actuel.
- Purge des entrées de la file d'attente des tâches de déploiement.
- Gestion des mises à jour de micrologiciel pour les clusters et bases de données.

REMARQUE : Pour s'assurer que l'inventaire / la garantie contient des informations à jour, planifiez la tâche d'inventaire / de garantie pour qu'elle soit exécutée au moins une fois par semaine. La tâche d'inventaire / de garantie consomme un minimum de ressources et ne dégrade pas les performances de l'hôte.

Les tâches de cette page comprennent :

- Gestion des travaux de déploiement avec la file d'attente des tâche de déploiement.
- Exécution de tâches d'inventaire
- Modification d'une planification de tâche d'inventaire
- Affichage de l'état de mise à jour de micrologiciel pour les clusters et centres de données

Gestion des travaux de déploiement avec la file d'attente des travaux de déploiement

Pour gérer les travaux de déploiement avec la file d'attente des travaux de déploiement :

1. Dans **Dell Management Center**, sélectionnez **File d'attente des tâches → Tâches de déploiement**.
2. Pour mettre à jour les **Détails des tâches de déploiement**, cliquez sur **Rafraîchir**.
3. Pour afficher la boîte de dialogue Détails des tâches de déploiement, qui contient des informations détaillées sur les serveurs inclus dans la tâche de déploiement, cliquez sur **Détails**. Les détails suivants s'affichent :
   - Numéro de service
   - Adresse IP iDRAC
   - État du serveur
   - La production éventuelle d'avertissements
   - Détails du travail de déploiement
   - Heure de début et de fin

   Pour afficher des informations complètes sur chaque élément du tableau de la boîte de dialogue, survolez l'élément et un texte supplémentaire s'affiche.
4. Pour mettre un travail sélectionné en attente ou pour entrer une planification mise à jour, cliquez sur **Modifier**.
5. Cliquez sur **Annuler** pour abandonner la tâche de déploiement.
6. À l'affichage du message, cliquez sur **Annuler la tâche** pour abandonner la tâche, ou cliquez sur **Ne pas annuler la tâche** pour annuler.

   REMARQUE : Toute tâche de déploiement en cours ne peut pas être abandonnée.
7. Pour afficher la fenêtre Purger la file d'attente des tâches de déploiement) cliquez sur **Purger la file d'attente des tâches**. Sélectionnez **Antérieurs à date et État de tâche** et cliquez sur **Appliquer**. Les tâches sélectionnées sont alors effacées de la file d'attente.

Ajout manuel d'un serveur

Vous pouvez ajouter manuellement un serveur qui n'a pas été ajouté par le processus de découverte. Une fois ajouté, le serveur apparaît dans la liste des serveurs dans l'Assistant Déploiement.

1. Dans le Dell Management Center, cliquez sur .**Déploiement** puis sur **Assistant Déploiement**
2. Dans l'onglet **Sélectionner un serveur**, cliquez sur **Ajouter un serveur**.
3. Dans la boîte de dialogue **Ajouter un serveur**, procédez ainsi :
   a. Dans la boîte de dialogue **Adresse IP iDRAC**, entrez l'adresse IP iDRAC.
   b. Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
   c. Dans la zone de texte **Mot de passe**, entrez le mot de passe.
4. Cliquez sur **Ajouter le serveur**. Cela peut prendre plusieurs minutes.

Suppression d'un serveur métal nu

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

1. Dans le Dell Management Center, sous **Déploiement** cliquez sur **Assistant Déploiement**.
2. Dans l'onglet **Sélectionner des serveurs**, cliquez sur **Supprimer des serveurs**.
3. Dans la boîte de dialogue **Supprimer des serveurs**, cochez la case du serveur à supprimer.
4. Cliquez sur **Supprimer les serveurs sélectionés**.
5. Dans l'onglet **Sélectionner des serveurs**, examinez les serveurs affichés dans le tableau pour confirmer qu'il a été supprimé.

6

Administration de console

L'administration du OpenManage Integration for VMware vCenter et de son environnement virtuel s'effectue à l'aide de deux portails d'administration supplémentaires :

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

Grâce à ces deux portails, les paramètres globaux de gestion de vCenter, de sauvegarde et restauration de la base de données du OpenManage Integration for VMware vCenter, et les actions réinitialiser / redémarrer peuvent être saisis et utilisés par toutes les instances vCenter.

Administration Console Web

L'Administration Console Web fournit plusieurs fonctionnalités importantes : enregistrement et gestion de serveur vCenter, gestion d'appliance virtuelle, paramètres globaux d'alerte vCenter, et paramètres de sauvegarde et restauration.

Gestion des connexions de serveur vCenter

Depuis la fenêtre Enregistrement vCenter de l'Administration Console, vous pouvez enregistrer un serveur vCenter et charger ou acheter une licence. Si vous utilisez une licence de démonstration, utilisez le lien **Acheter maintenant** pour acheter une licence de version complète afin de gérer plusieurs hôtes. Dans cette section, vous pouvez aussi modifier, mettre à jour et désenregistrer un serveur.

Tâches connexes :

- Enregistrement d'un serveur vCenter
  - Modification de la connexion Administrateur vCenter
  - Mise à jour des certificats SSL des vCenter enregistrés
  - Désinstallation de OpenManage Integration for VMware vCenter depuis vCenter
- Chargement d'une licence OpenManage Integration for VMware vCenter à l'aide de l'Administration Console

Enregistrement d'un serveur vCenter

Vous pouvez enregistrer l'OpenManage Integration for VMware vCenter après l'installation d'OpenManage Integration for VMware vCenter. OpenManage Integration for VMware vCenter utilise un compte utilisateur admin pour les opérations vCenter. OpenManage Integration for VMware vCenter prend en charge 10 vCenters par appliance.

1. Dans l'OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Pour enregistrer un nouveau serveur, dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**, puis cliquez sur **Enregistrer un nouveau serveur vCenter**.

4. Dans la boîte de dialogue **Enregistrer un nouveau serveur vCenter**, sous **Nom vCenter** effectuez les tâches suivantes :
   a. Dans la zone de texte **Nom d'hôte ou IP du serveur vCenter**, entrez l'adresse IP du vCenter ou un FQDN de l'hôte.
   b. Dans la zone de texte **Description**, entrez une description optionnelle.
5. Sous **Compte utilisateur Admin**, procédez ainsi :
   a. Dans la zone de texte **Nom d'utilisateur Admin**, entrez le nom d'utilisateur de l'administrateur.
   b. Dans la zone de texte **Mot de passe**, entrez le mot de passe.
   c. Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe.
6. Cliquez sur **Enregistrer**.

Exigences d'OpenManage Integration for VMware vCenter

L'OpenManage Integration for VMware vCenter (OMIVV) requiert des informations émises par OpenManage sur les serveurs d'ancienne génération, et les plateformes plus récentes sont limitées au démarrage sous la version de vSphere qui comprend les jeux de puces plus récents. Pour cette raison, il existe des limites de la version de vSphere qu'une version donnée d'OMIVV prend en charge.

Versions d'ESXi qui doivent être prises en charge sur des hôtes gérés :

prise en charge des versions ESX/ ESXi	Prise en charge de la génération de plateformes				
	9G	10G	11G	12G	13G
v4.1 (ESX/ESXi)	0	0	0	N	N
v4.1 U1 (ESX/ESXi)	0	0	0	N	N
v4.1 U2 (ESX/ESXi)	0	0	0	0	N
v4.1 U3 (ESX/ESXi)	0	0	0	0	N
v5.0	0	0	0	0	N
v5.0 U1	0	0	0	0	N
v5.0 U2	0	0	0	0	N
v5.0 U3	0	0	0	0	N
v5.1	0	0	0	0	N
v5.1 U1	0	0	0	0	N
v5.1 U2	0	0	0	0	N
v5.5	N	y	0	0	N
v5.5 U1	N	N	N	N	0
v5.5 U2	N	N	N	0	0

sSupport vCenter

Actuellement, la prise en charge de la version 5.5 U1 n'est disponible qu'avec les serveurs de 12e génération au moyen d'iDRAC avec prise en charge du Lifecycle Controller. La prise en charge OpenManage de la version 5.5 U1 avec les serveurs d'anciennes générations est à paraître. vSphere v5.5 U1 n'est pas pris en charge avec le dernier jeu de puces, et donc n'est pas pris en charge sur les plateformes de 13e génération.

Prise en charge de vSphere v5.5 U2

Grâce à la prise en charge d'iDRAC avec le Lifecycle Controller, la version 5.5 U2 est prise en charge par vSphere pour les palteformes de 12e et 13e générations.

Versions de vCenter Server prises en charge par la version 2.3

L'OpenManage Integration for VMware vCenter fonctionne avec n'importe laquelle de ces versions du vCenter Server :

Version vCenter	Prise en charge du client de bureau	Prise en charge du client Web
v5.0 U3	O	N
v5.1 U2	O	N
v5.5	O	O
v5.5 U1	O	O
v5.5 U2	O	O

Avec n'importe quelle version de vCenter, les hôtes ESX/ESXi administrés doivent être de version égale ou inférieure. Un vCenter de version au moin 5.0 U3 est nécessaire pour administrer un environnement vSphere v4.1 ou v5.0 avec OMIVV.

Modification de la connexion vCenter Administrator

1. Dans l'OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**. Les vCenter enregistrés sont affichés dans le volet de droite. Pour afficher la fenêtre **Modifier le compte Admin**, sous **Informations d'identification**, cliquez sur **Modifier**.
4. Entrez les **Nom d'utilisateur** et **Mot de passe**, puis **Vérifiez le mot de passe** de vCenter Administrator. Les mots de passe doivent concorder.
5. Pour changer le mot de passe, cliquez sur **Appliquer** ; pour annuler le changement, cliquez sur **Annuler**.

Mise à jour des certificats SSL des serveurs vCenter enregistrés

Si le certificat SSL est modifié sur un serveur vCenter, suivez les étapes ci-après pour importer le nouveau certificat de l'OpenManage Integration for VMware vCenter. L'OpenManage Integration for VMware vCenter utilise ce certificat pour s'assurer que le serveur vCenter avec lequel il communique est le bon serveur vCenter et non un imitateur.

OpenManage Integration for VMware vCenter utilise l'API openssl pour créer la CSR (Certificate Signing Request - Demande de signature de certificat) à l'aide de la norme de cryptage RSA d'une longueur de clé de 2048 bits. La CSR générée par l'OpenManage Integration for VMware vCenter sert à obtenir d'une Autorité de certification de confiance un certificat signé numériquement. L'OpenManage Integration for VMware vCenter utilise ce certificat numérique pour activer SSL sur le serveur Web pour la communication sécurisée.

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>
2. Dans le volet de gauche, cliquez sur **ENREGISTREMENT VCENTER**. Les vCenter enregistrés sont affichés dans le volet de droite. Pour mettre à jour les certificats, cliquez sur **Mettre à jour**.

Désinstallation de l'OpenManage Integration for VMware vCenter de VMware vCenter

Pour être supprimé, l'OpenManage Integration for VMware vCenter doit être désenregistré du serveur vCenter à l'aide de l'Administration Console.

1. Lancez un navigateur web puis entrez https://<ApplianceIPAddress>
2. Dans la page **Enregistrement vCenter** , sous le tableau du serveur vCenter, désenregistrez l'OpenManage Integration for VMware vCenter en cliquant sur **Désenregistrer**.

   Vous pouvez avoir plusieurs vCenter, vérifiez donc que vous avez sélectionné le bon.

3. Dans la boîte de dialogue **Désenregistrer vCenter** qui vous demande si vous voulez vraiment désenregistrer ce serveur, cliquez sur **Désenregistrer**.

Chargement d'une licence OpenManage Integration for VMware vCentersur l'Administration Console

Pour charger une licence OpenManage Integration for VMware vCenter sur l'Administration Portal (Portail d'administration) :

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>
2. Dans le volet gauche, cliquez sur **ENREGISTREMENT VCENTER**. Les vCenter enregistrés sont affichés dans le volet de droite. Pour afficher la boîte de dialogue Charger une licence, cliquez sur **Charger une licence**.
3. Pour accéder au fichier de licence, cliquez sur **Parcourir** , puis cliquez sur **Charger**.

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

Gestion de l'appliance virtuelle

La gestion de d'appliance virtuelle inclut les informations de réseau OpenManage Integration for VMware vCenter, de version, NTP et HTTPS et permet à l'administrateur d'effectuer les tâches suivantes :

- Redémarrer l'appliance virtuelle
- Mettre à jour l'appliance virtuelle, et configurer un emplacement de référentiel de mise à jour
- Générer un lot de dépannage qui contient les informations des journaux de l'appliance.
- Entrer les paramètres NTP (Network Time Protocol)
- Charger et gérer les certificats HTTPS

Tâches connexes :

- Redémarrage de l'appliance virtuelle
- Mise à jour d'un emplacement de référentiel et mise à jour d'une appliance
- Téléchargement de lot de dépannage
- Configuration des serveurs NTP

Redémarrage de l'appliance virtuelle

Pour redémarrer l'appliance virtuelle :

REMARQUE : Le redémarrage de l'appliance virtuelle vous déconnecte de l'Administration Console, et le OpenManage Integration for VMware vCenter est indisponible jusqu'à ce que l'appliance virtuelle et ses services soient actifs.

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>
2. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
3. Pour redémarrer le OpenManage Integration for VMware vCenter, cliquez sur **Redémarrer l'appliance virtuelle**.
4. Dans la boîte de dialogue **Redémarrer l'appliance virtuelle**, pour redémarrer l'appliance virtuelle, cliquez sur **Appliquer** ou cliquez sur **Annuler** pour annuler.

Mise à jour d'un emplacement d'espace de stockage et d'une appliance virtuelle

Effectuez une sauvegarde avant la mise à jour de l'appliance virtuelle pour vous assurer que toutes les données sont protégées.

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
3. En regard de Mise à jour de l'appliance, cliquez sur **Modifier**.
4. Dans la fenêtre **Mise à jour de l'appliance**, saisissez l'**URL de l'emplacement de l'espace de stockage** et cliquez sur **Appliquer**.

   REMARQUE : Si l'emplacement de mise à jour est situé sur un réseau externe, comme le site FTP de Dell, un proxy doit être entré ci-dessous dans la zone Proxy HTTP.

Mise à jour de la version du logiciel de l'appliance virtuelle

Pour éviter toute perte de données, effectuez une sauvegarde de l'appliance avant de commencer la mise à jour du logiciel.

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **MAINTENANCE DE L'APPLIANCE**.
3. Pour mettre à jour l'appliance virtuelle à la version du logiciel affichée sous **Mise à jour de l'appliance**, cliquez sur **Mettre à jour l'appliance virtuelle**.
4. Les versions actuelles et disponibles sont affichées dans la boîte de dialogue **Mettre à jour l'appliance**. Pour lancer la mise à jour, cliquez sur **Mettre à jour**.
5. Le système est verrouillé et mis en mode de maintenance. Lorsque la mise à jour est terminée, la page Appliance affiche la nouvelle version installée.

Téléchargement du lot de dépannage

Utilisez ces informations pour résoudre des problèmes, ou les envoyer au Support technique.

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
3. Pour afficher la boîte de dialogue de lot de dépannage, cliquez sur **Générer un lot de dépannage**.
4. Pour ouvrir ou enregistrer un fichier zip contenant les informations de journal de l'appliance virtuelle, cliquez sur le lien **Télécharger un lot de dépannage**.
5. Pour quitter, cliquez sur **Fermer**.

Configuration du proxy HTTP

Vous pouvez configurer le proxy HTTP avec la Console Administration ou Dell Management Console.

1. Dans l'OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
4. Sur la page **Gestion de l'appliance** , effectuez un défilement vers le bas jusqu'à **HTTP Proxy Settings (Paramètres du proxy HTTP)** et cliquez sur **Modifier**.
5. Sur la page **Modifier**, procédez ainsi :

a. Pour activer l'utilisation des paramètres du proxy HTTP, à côté de **Utiliser les paramètres du proxy HTTP**, sélectionnez **Activer**.
b. Dans la zone de texte **Adresse du serveur proxy**, entrez l'adresse du serveur proxy.
c. Dans la zone de texte **Port du serveur proxy**, entrez le port du serveur proxy.
d. Pour utiliser les références du proxy, en regard de **Utiliser les références du proxy**, sélectionnez **Oui**.
e. Si vous utilisez les références, dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
f. Dans la zone de texte **Mot de passe**, entrez le mot de passe.

6. Cliquez sur **Appliquer**.

Configuration des serveurs NTP

Le protocole Network Time Protocol (NTP) peut être utilisé pour synchroniser les horloges de l'appliance virtuelle avec celle d'un serveur NTP.

1. Dans le OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
4. Cliquez sur **Modifier pour NTP**
5. Sélectionnez la case **Activé**. Entrez le **nom d'hôte** ou l'**adresse IP** d'un serveur NTP **Privilégié** et **Secondaire**, puis cliquez sur **Appliquer**.
6. Pour quitter, cliquez sur **Annuler**.

Génération d'une requête de signature de certificat

REMARQUE : Vous devez charger le certificat avant d'enregistrer l'OpenManage Integration for VMware vCenter auprès du vCenter.

La génération d'une requête de signature de certificat empêche le chargement sur l'appliance des certificats créés avec la CSR générée antérieurement.

1. Dans l'OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
4. Cliquez sur **Générer une requête de signature de certificat pour les certificats HTTPS**. Un message s'affiche indiquant que si une nouvelle requête est générée, les certificats créés à l'aide de la CSR précédente ne peuvent plus être chargés sur l'appliance. Pour poursuivre la requête, cliquez sur **Continuer**, pour annuler, cliquez sur **Annuler**.
5. Entrez le **Nom commun**, le (**Nom organisationnel**), l' **Unité organisationnelle**, la **Localité**), le **Nom de l'État**), le **Pays**) et l'**E-mail** de la requête. Cliquez sur **Continuer**.
6. Cliquez sur **Télécharger**, puis enregistrez le certificat HTTPS résultant à un emplacement accessible.

Chargement d'un certificat HTTPS

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

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

1. Dans l'OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
4. Cliquez sur **Charger un certificat pour les certificats HTTPS**.
5. Dans la boîte de dialogue **Charger des certificats**, cliquez sur **OK**.
6. Pour sélectionner le certificat à charger, cliquez sur **Parcourir**, puis sur **Charger**.
7. Si vous voulez abandonner le chargement, cliquez sur **Annuler**.

REMARQUE : Le certificat doit être au format PEM.

Restauration du certificat HTTPS par défaut

1. Dans le OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utlisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DE L'APPLIANCE**.
4. Cliquez sur **Restaurer le certificat par défaut pour les certificats HTTPS**.
5. Dans la boîte de dialogue de restauration du certificat par défaut, cliquez sur **Appliquer**.

Configuration des alertes globales

La gestion des alertes permet à un administrateur d'entrer les paramètres globaux de stockage des alertes de toutes les instances vCenter.

1. Dans le OpenManage Integration for VMware vCenter, sur l'onglet Résumé, utilisez le lien pour ouvrir l'Administration Console.
2. Dans la boîte de dialogue Connexion, entrez votre mot de passe.
3. Dans le volet gauche, cliquez sur **GESTION DES ALERTES**. Pour entrer de nouveaux paramètres d'alertes vCenter, cliquez sur **Modifier**.
4. Entrez les valeurs numériques des éléments suivants :
   - Nombre maximum d'alertes
   - Nombre de jours de conservation des alertes
   - Délai d'expiration des alertes en double (en secondes)
5. Pour enregistrer les paramètres, cliquez sur **Appliquer** ou cliquez sur **Annuler** pour annuler.

Gestion des sauvegardes et restaurations

La gestion des sauvegardes et restaurations s'effectue depuis l'Administration Console. Les tâches de cette page comprennent :

- Configuration des sauvegardes et restaurations
- Planification des sauvegardes automatiques
- Exécution d'une sauvegarde immédiate
- Restauration de la base de données à partir de la sauvegarde

Configuration des sauvegardes et restaurations

La fonction de sauvegarde et restauration sauvegarde la base de données d'OpenManage Integration for VMware vCenter à un emplacement distant à partir duquel elle peut être restaurée à une date ultérieure. Les profils, modèles et informations sur l'hôte sont inclus dans la sauvegarde. Il est recommandé de planifier des sauvegardes automatiques pour éviter toute perte de données. Après cette procédure, vous devez configurer une planification de sauvegarde.

Pour configurer des sauvegardes et restaurations :

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **SAUVEGARDE ET RESTAURATION**.
3. Pour modifier la sauvegarde actuelle et restaurer les paramètres, cliquez sur **Modifier**.
4. Sur la page **Paramètres et détails**, procédez ainsi :
   a. Dans la zone de texte **Emplacement de sauvegarde**, entrez le chemin des fichiers de sauvegarde.
   b. Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur.
   c. Dans la zone de texte **Mot de passe**, entrez le mot de passe.
   d. Sous **Entrer le mot de passe utilisé pour crypter les sauvegardes**, entrez le mot de passe crypté dans la zone de texte.

      Le mot de passe de cryptage peut contenir des caractères alphanumériques et les caractères spéciaux suivants : !@#$%*. Il n'y a aucune limite quant à la longueur du mot de passe.
   e. Dans la zone de texte **Vérifier le mot de passe**, entrez à nouveau le mot de passe crypté.
5. Pour enregistrer ces paramètres, cliquez sur **Appliquer**.
6. Configurez la planification des sauvegardes. Pour plus d'informations, voir Planification des sauvegardes automatiques.

Planification des sauvegardes automatiques

Il s'agit de la deuxième partie de la configuration des sauvegardes et restaurations. Pour des informations détaillées sur la configuration des références et de l'emplacement de sauvegarde, voir Configuration des sauvegardes et restaurations.

Pour planifier une sauvegarde automatique :

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **SAUVEGARDE ET RESTAURATION**.
3. Pour modifier les paramètres de sauvegarde et restauration, cliquez sur **Modifier Sauvegardes automatiques planifiées** (cela active les champs).
4. Pour activer les sauvegardes, cliquez sur **Activé**.
5. Cochez les cases correspondant aux jours de la semaine où vous voulez exécuter la sauvegarde.
6. Dans la zone de texte **Heure de sauvegarde (Format horaire sur 24 heures, HH:mm)**, entrez l'heure au format HH:mm.

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

Exécution d'une sauvegarde immédiate

Pour exécuter une sauvegarde immédiate :

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **SAUVEGARDE ET RESTAURATION**.
3. Cliquez sur **Sauvegarder maintenant**.

4. 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 correspondante.
5. Entrez un **Emplacement de sauvegarde**, **Nom d'utilisateur**, **Mot de passe** et **Mot de passe de cryptage**.

   Le mot de passe de cryptage peut contenir des caractères alphanumériques et les caractères spéciaux suivants : ! @#$%*. Il n'y a aucune limite quant à la longueur du mot de passe.
6. Cliquez sur **Sauvegarder**.

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

REMARQUE : L'opération de restauration entraîne le redémarrage de l'appliance virtuelle après qu'elle a terminé.

Pour restaurer la base de données à partir d'une sauvegarde :

1. Lancez un navigateur Web puis entrez https://<ApplianceIPAddress>.
2. Dans le volet gauche, cliquez sur **SAUVEGARDE ET RESTAURATION** et les paramètres actuels de sauvegarde et restauration s'affichent.
3. Cliquez sur **Restaurer maintenant**.
4. Dans la boîte de dialogue Restaurer, entrez un **Emplacement du fichier** au format CIFS/NFS.
5. Entrez un **Nom d'utilisateur**, **Mot de passe** et **Mot de passe de cryptage** pour le fichier de sauvegarde.

   Le mot de passe de cryptage peut contenir des caractères alphanumériques et les caractères spéciaux suivants : ! @#$%*. Il n'y a aucune limite quant à la longueur du mot de passe.
6. Pour enregistrer les modifications, cliquez sur **Appliquer**

   L'appliance redémarre lorsque vous cliquez sur Appliquer.

Comprendre la vSphere Web Client Console

La **console** se trouve dans le client vSphere de la machine virtuelle. La **console** fonctionne de pair avec l'Administration Console. La console permet de :

- Configurer les paramètres réseau
- Changer le mot de passe de l'appliance virtuelle
- Configurer le fuseau horaire local
- Redémarrer l'appliance virtuelle
- Réinitialiser l'appliance virtuelle aux paramètres d'usine
- Actualiser la console
- Option de déconnexion

Utilisez les touches fléchées pour naviguer vers le haut et le bas. Une fois que vous avez sélectionné l'option désirée, appuyez sur **<ENTRÉE>**. Après que vous accédez à l'écran **Console**, le VMware vSphere Client prend le contrôle de votre curseur. Pour échapper à ce contrôle, appuyez sur **<CTRL> + <ALT>**.

Configuration des paramètres réseau

Les modifications des paramètres réseau s'effectuent dans l'onglet **Console** de vSphere Client.

Pour configurer les paramètres réseau :

1. Dans le **vSphere Client**, sélectionnez l'OpenManage Integration for VMware vCenter, puis cliquez sur l'onglet **Console**.
2. Dans la fenêtre **Console**, sélectionnez **Configurer le réseau**, puis appuyez sur **<ENTRÉE>**.
3. Entrez les paramètres réseau souhaités sous **Modifier des périphériques** ou **Modifier DNS**, puis cliquez sur **Enregistrer et quitter**. Pour abandonner les modifications, cliquez sur **Quitter**.

Changement du mot de passe de l'appliance virtuelle

Le mot de passe de l'appliance virtuelle se change dans le vSphere Client à partir de l'onglet **Console**.
Pour changer le mot de passe de l'appliance virtuelle :

1. Dans le vSphere Web Client, sélectionnez la machine virtuelle OpenManage Integration for VMware vCenter, puis cliquez sur l'onglet **Console**.
2. Sur l'onglet **Console**, servez-vous des flèches pour sélectionner **Changer le mot de passe Admin** et appuyez sur **<ENTRÉE>**.
3. Entrez le **mot de passe Admin actuel** et appuyez sur **<ENTRÉE>**.

   Les mots de passe Admin comportent un caractère spécial, un chiffre, une lettre majuscule, une lettre minuscule, et au moins 8 lettres.
4. Entrez un nouveau mot de passe à l'affichage de **Entrer le nouveau mot de passe Admin** et appuyez sur **<ENTRÉE>**.
5. Entrez le nouveau mot de passe à nouveau dans la zone de texte **Veuillez confirmer le mot de passe Admin**, puis appuyez sur **<ENTRÉE>**. Le mot de passe d'administration est changé.

Configuration du fuseau horaire local

Pour configurer le fuseau horaire local :

REMARQUE : Vous pouvez modifier uniquement le fuseau horaire et non l'heure et la date actuelles.

1. Dans **vSphere Client**, sélectionnez laOpenManage Integration for VMware vCenter machine virtuelle, puis cliquez sur l'onglet **Console**.
2. Sélectionnez **Configurer le fuseau horaire local** et appuyez sur **<ENTRÉE>**.
3. Dans la fenêtre **Sélection du fuseau horaire**, sélectionnez le fuseau horaire souhaité et cliquez sur **OK**. Pour annuler les modifications, cliquez sur **Annuler**. Le fuseau est mis à jour.

Redémarrage de l'appliance virtuelle

Pour redémarrer l'appliance virtuelle :

1. Dans **vSphere Client**, sélectionnez laOpenManage Integration for VMware vCenter machine virtuelle, puis cliquez sur l'onglet **Console**.
2. Sélectionnez **Redémarrer cette appliance virtuelle** et appuyez sur **<ENTRÉE>**.
3. Le message suivant s'affiche :

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
4. Entrez **o** pour redémarrer ou **n** pour annuler. L'appliance est redémarrée.

Réinitialisation de l'appliance virtuelle aux paramètres d'usine

Pour réinitialiser l'appliance virtuelle aux paramètres d'usine :

1. Dans le **vSphere Client**, sélectionnez la machine virtuelle OpenManage Integration for VMware vCenter, puis cliquez sur l'onglet **Console**.
2. Sélectionnez **Réinitialiser l'appliance virtuelle sur les paramètres d'usine** et appuyez sur **<ENTRÉE>**.
3. Le message suivant s'affiche :

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```
4. Entrez **o** pour réinitialiser ou **n** pour annuler.

   L'appliance est réinitialisée aux paramètres d'usine d'origine et tous les paramètres et toutes les autres données enregistrées sont perdues.

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

Actualisation de l'affichage de la Console

Pour actualiser l'affichage de la Console, sélectionnez **Rafraîchir** et appuyez sur **<ENTRÉE>**.

Rôle utilisateur en lecture seule

Il existe un rôle utilisateur non privilégié appelé lecture seule avec accès au shell à des fins de diagnostic. L'utilisateur en lecture seule a des privilèges limités pour exécuter le montage. Le mot de passe de l'utilisateur en lecture seule est le même que celui de l'administrateur.

Chemin de migration permettant d'effectuer une migration de 1.6/1.7 à 2.3

La mise à jour du RPM vers cette version à partir de la version 1.7 ou de versions antérieures n'est pas prise en charge. Vous pouvez effectuer une migration d'une version antérieure (1.6 ou 1.7) à la version 2.3 à l'aide du chemin d'accès de sauvegarde et de restauration. En outre, le chemin de migration n'est pris en charge que depuis les versions 1.6 et 1.7. Si vous travaillez à partir d'une version antérieure à 1.6, vous devrez mettre à niveau votre appliance vers la version prise en charge avant de procéder à la migration vers OpenManage Integration for VMware vCenter version 2.3.

Suivez les étapes suivantes pour effectuer une migration de la version antérieure à la version 2.3 d'OpenManage Integration for VMware vCenter :

1. Choisissez une sauvegarde de la base de données pour la version plus ancienne. Pour plus d'informations, voir la section **Managing Backup and Restore** dans ce guide.
2. Mettez l'ancienne appliance hors tension depuis le vCenter.

   REMARQUE : Ne désenregistrez pas le Plug-in du vCenter, car cela supprimerait toutes les alarmes enregistrées sur le vCenter par le plug-in et supprimerait toutes les personnalisations effectuées sur les alarmes telles que les actions, etc. sur le vCenter. Pour en savoir plus, consultez la section **Comment effectuer une restauration si j'ai déjà désenregistré l'ancien plugin suite à la sauvegarde** de ce guide si vous avez déjà désenregistré les Plug-ins suite à la sauvegarde.
3. Déployez le nouvel OVF de la version 2.3 d'OpenManage Integration. Pour en savoir plus, consultez la section **Déploiement de l'OVF d'OpenManage Integration for VMware vCenter à l'aide du client vSphere** de ce guide pour déployer l'OVF.

4. Mettez l'appliance OpenManage Integration version 2.3 sous tension.
5. Configurez le réseau, fuseau horaire, etc. de l'appliance. Il est recommandé de s'assurer que l'adresse IP de la nouvelle appliance OpenManage Integration version 2.3 est identique à celle de l'ancienne appliance. Pour configurer les détails du réseau, consultez la section **Enregistrement d'OpenManage Integration for VMware vCenter et importation du fichier de licence** de ce guide.
6. Restaurez la base de données sur la nouvelle appliance. Pour plus d'informations, reportez-vous à la section **Restauration de la base de données à partir d'une sauvegarde** de ce guide.
7. Chargez le nouveau fichier de licence. Pour plus d'informations, voir la section **Enregistrement d'OpenManage Integration for VMware vCenter et importation du fichier de licence** dans le **OpenManage Integration Version 2.3 Quick Install Guide**.
8. Vérifiez l'appliance. Pour en savoir plus, consultez la section **Vérification de l'installation** de ce guide pour assurer la réussite de la migration de la base de données.
9. Exécutez l'inventaire sur tous les vCenter enregistrés.

REMARQUE :

Il vous est recommandé d'exécuter l'inventaire sur tous les hôtes gérés par le plug-in suite à la mise à niveau. Pour en savoir plus, consultez la section **Exécution des tâches d'inventaire** pour savoir comment exécuter l'inventaire sur demande.

Si l'adresse IP de la nouvelle appliance OpenManage Integration version 2.3 est différente de celle de l'ancienne appliance, la destination d'interruption des interruptions SNMP doit être configurée de sorte à pointer vers la nouvelle appliance. Pour les serveurs de 12e génération et de générations ultérieures, ceci se fait en exécutant l'inventaire sur ces hôtes. Pour tous les hôtes de 11e génération ou de générations antérieures, antérieurement conformes, ce changement d'adresse IP s'affiche comme étant non conforme et exige une configuration d'OMSA. Pour en savoir plus, consultez la section **Exécution de l'Assistant Correction des hôtes VSphere non conformes** de ce guide pour corriger la conformité des hôtes.

7

Dépannage

Utilisez cette section pour trouver les réponses à des questions de dépannage. Cette section comprend :

- Questions fréquemment posées (FAQ)
- Problèmes de déploiement de serveurs métal nu
- Contacter Dell
- Informations sur les produits connexes

Questions fréquemment posées (FAQ)

Cette section contient des questions courantes et leurs solutions.

L'utilisation de OpenManage Integration for VMware vCenter pour mettre à jour une carte réseau avec la version 13.5.2 du micrologiciel n'est pas prise en charge.

Il existe un problème connu avec les serveurs Dell PowerEdge de 12e génération et certaines cartes réseau Intel dotées de la version micrologicielle 13.5.2. La mise à jour de certains modèles de cartes réseau Intel à cette version du micrologiciel échoue lorsque la mise à jour du micrologiciel est effectuée à l'aide de Lifecycle Controller. Les clients possédant cette version du micrologiciel doivent mettre à jour le logiciel du pilote réseau à l'aide d'un système d'exploitation. Si la carte réseau Intel possède une version de micrologiciel autre que la version 13.5.2, vous pouvez effectuer la mise à jour à l'aide de OpenManage Integration for VMware vCenter. 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 : Remarque : lorsque vous utilisez la mise à jour de micrologiciel un à plusieurs, évitez de sélectionner des cartes réseau Intel de version 13.5.2, car la mise à jour échouera et empêchera la tâche de mise à jour du reste des serveurs.

Lors d'une tentative de mise à jour du micrologiciel avec un progiciel DUP non valide, l'état de la tâche de mise à jour matérielle sur la console vCenter ne présente ni un échec ni un temps d'attente pendant des heures, même si l'état de la tâche dans LC est « ÉCHEC ». Pourquoi ?

Lorsque le progiciel DUP non valide est collecté pour la mise à jour du micrologiciel, l'état de la tâche dans la fenêtre de la console vCenter reste 'En cours', mais le message est modifié pour motif de panne. Il s'agit d'un bogue de VMWare connu qui sera corrigé dans les futures versions de VMware vCenter.

Résolution : la tâche doit être annulée manuellement.

Versions concernées : Toutes

Le portail d'administration affiche encore toujours l'emplacement de l'espace de stockage de mise à jour inaccessible.

Si l'utilisateur a fourni un chemin inaccessible de mise à jour de l'espace de stockage , 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, mais le chemin de mise à jour de l'espace de stockage n'est pas effacé à la valeur précédant 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 les paramètres de configuration de DNS sont-ils restaurés à leurs valeurs d'origine après le redémarrage du serveur si DHCP est utilisé pour l'adresse IP de l'appliance et les paramètres DNS écrasés

Il existe un bogue connu qui fait que les paramètres DNS attribués de façon statique, sont remplacés par des valeurs de DHCP. Cela peut se produire lorsque le DHCP est utilisé pour obtenir les valeurs des paramètres IP et les valeurs DNS sont attribuées de manière statique. Lorsque le bail DHCP est renouvelé ou que l'appliance est redémarrée, les paramètres de DNS attribués de façon statique sont supprimés. Résolution : attribuez de façon statique des paramètres IP lorsque paramètres du serveur DNS diffèrent de ceux de DHCP.

Versions concernées : Toutes

Pourquoi mon système n'est pas passé en mode Maintenance lorsque j'ai effectué la mise à jour du micrologiciel 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.

Pourquoi la mise à jour du micrologiciel du système 11G montre-t-elle que je n'ai aucun des ensembles conçus pour une telle mise à jour, même si mon espace de stockage contient les bons ensembles ?

Quand j'ai ajouté un hôte au profil de connexion en mode de verrouillage, l'inventaire a démarré, mais a échoué en indiquant qu'« aucun contrôleur d'accès à distance n'a été trouvé ou que l'inventaire n'est pas pris en charge sur cet hôte ». L'inventaire est bien censé marcher pour un hôte en mode de verrouillage ?

Si vous aviez mis l'hôte en mode de verrouillage ou retiré un hôte depuis le mode verrouillage, vous devez attendre 30 minutes avant d'effectuer la prochaine opération de sélection d'un hôte 11G pour la mise à jour du micrologiciel. L'Assistant de mise à jour du micrologiciel n'affiche aucun ensemble même si l'espace de stockage fourni contient des ensembles conçus pour ce système. Ceci se produit parce que l'hôte 11G peut ne pas être configuré pour qu'OMSA envoie des interruptions à OpenManage Integration.

Solution : assurez-vous que l'hôte est conforme à l'aide de l'écran Conformité de l'hôte du client OpenManage Integration desktop. S'il n'est pas conforme, utilisez le correctif de conformité de l'hôte afin de rendre celui-ci conforme.

Versions concernées : 2.2 et 2.3

Pourquoi le déploiement de mon ESX / ESXi échoue-t-il sur les serveurs dotés d'un contrôleur d'amorçage PERC S300 ?

Les déploiements de OpenManage Integration for VMware vCenter à l'aide de différentes versions d'ESX/ESXi sur les serveurs Dell PowerEdge dotés du contrôleur d'amorçage PERC S300 ont échoué. Les systèmes d'exploitation ESX/ESXi personnalisés de Dell ne sont pas dotés du pilote pour le contrôleur d'amorçage PERC S300 ; ce qui empêche la

reconnaissance du contrôleur d'amorçage/HDD pendant l'installation du système d'opération. Les serveurs dotés de contrôleurs d'amorçage PERC S300 ne sont pas pris en charge par les déploiements de OpenManage Integration for VMware vCenter.

Pourquoi un message d'erreur s'affiche-t-il lorsque je clique sur le lien du micrologiciel ?

Si votre réseau est lent (9600BPS), un message d'erreur de communication peut s'afficher. Ce message d'erreur peut s'afficher lorsque vous cliquez sur le lien du micrologiciel dans le client vSphere de l'OpenManage Integration for VMware vCenter. Cela se produit lorsque la connexion s'interrompt lors de la tentative d'obtention de la liste d'inventaire du logiciel. Ce délai d'attente est lancé par Microsoft Internet Explorer. Pour les versions 9/10 de Microsoft Internet Explorer, la valeur du « Délai d'attente de réception » est définie sur 10 secondes. Corrigez ce problème à l'aide des étapes suivantes :

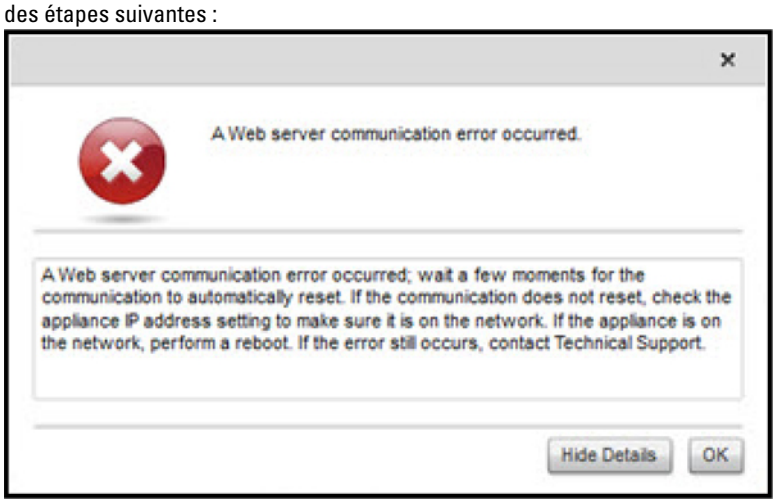

Figure 5. Erreur de communication du lien du micrologiciel

1. Ouvrez Microsoft Registry Editor (Regedit - Éditeur du Registre Microsoft).
2. Naviguez jusqu'à l'emplacement suivant :
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Ajoutez une valeur DWORD pour le délai d'attente de réception.
4. Définissez la valeur sur 30 secondes (30000) [Une valeur plus élevée peut s'avérer nécessaire dans votre environnement].
5. Quittez Regedit.
6. Redémarrez Internet Explorer.

REMARQUE : Le simple fait d'ouvrir la fenêtre Internet Explorer ne suffit pas. Redémarrez le navigateur d'Internet Explorer.

Quelle génération de serveurs Dell l'OpenManage Integration for VMware vCenter configure-t-il et prend-il en charge pour les interruptions SNMP ?

OpenManage Integration for VMware vCenter prend en charge les interruptions SNMP OMSA sur les serveurs de générations antérieures à la 12e et les interruptions iDRAC sur les serveurs de 12e génération.

Comment OpenManage Integration for VMware vCenter prend-il en charge plus de trois vCenters en Mode Lié ?

Chaque appliance virtuelle prend en charge un maximum de trois vCenters en mode Lié. Si vous disposez de plus de trois vCenter, vous aurez besoin d'une nouvelle instance de l'appliance pour chaque lot de dix vCenters, ainsi que des droits de licence correspondants.

OpenManage Integration for VMware vCenter prend-il en charge vCenter en mode lié ?

Oui, OpenManage Integration for VMware vCenter prend en charge jusqu'à dix vCenters en mode lié. Pour plus d'informations sur la façon dont OpenManage Integration for VMware vCenter fonctionne en mode lié, consultez le livre blanc, *Dell Management Plug-in for VMware vCenter : Travailler en mode lié* sur le site www.Dell.com.

Quels sont les ports requis pour le OpenManage Integration for VMware vCenter ?

REMARQUE : Llors du déploiement de l'agent OMSA à l'aide du lien *Résoudre les hôtes vSphere non conformes* disponible dans la fenêtre de Conformité dans le Dell Management Center, le OpenManage Integration for VMware vCenter démarre le service httpClient, active le port 8080 sur les versions ESXi 5.0 et ultérieures pour le téléchargement et l'installation d'OMSA VIB. Une fois l'installation d'OMSA terminée, le service s'arrête automatiquement et le port se ferme.

Utilisez ces paramètres de port pour le OpenManage Integration for VMware vCenter.

Tableau 3. Ports d'appliance virtuelle

Numéro de port	Protocoles	Type de port	Niveau de cryptage max.	Direction	Utilisation	Configurable
21	FTP	TCP	Aucun	Sortant	Client de commande FTP	Non
53	DNS	TCP	Aucun	Sortant	Client DNS	Non
80	HTTP	TCP	Aucun	Sortant	Accès aux données en ligne Dell	Non
80	HTTP	TCP	Aucun	Entrant	Administration Console	Non
162	Agent SNMP	UDP	Aucun	Entrant	Agent SNMP (serveur)	Non
11620	Agent SNMP	UDP	Aucun	Entrant	Agent SNMP (serveur)	Non
443	HTTPS	TCP	128 bits	Entrant	Serveur HTTPS	Non
443	WSMAN	TCP	128 bits	Entrée/Sortie	Communication iDRAC/OMSA	Non
4433	HTTPS	TCP	128 bits	Entrant	Découverte automatique	Non
2049	NFS	UDP	Aucun	Tous	Partage public	Non
4001–4004	NFS	UDP	Aucun	Tous	Partage public	Non

Numéro de port	Protocoles	Type de port	Niveau de cryptage max.	Direction	Utilisation	Configurable
11620	Agent SNMP	UDP	Aucun	Om	Agent SNMP (serveur)	Non

Tableau 4. Nœuds gérés

Numéro de port	Protocoles	Type de port	Niveau de cryptage max.	Direction	Utilisation	Configurable
162, 11620	SNMP	UDP	Aucun	Sortant	Événements matériels	Non
443	WSMAN	TCP	128 bits	Entrant	Communicatio n iDRAC/OMSA	Non
4433	HTTPS	TCP	128 bits	Sortant	Découverte automatique	Non
2049	NFS	UDP	Aucun	Tous	Partage public	Non
4001–4004	NFS	UDP	Aucun	Tous	Partage public	Non
443	HTTPS	TCP	128 bits	Entrant	Serveur HTTPS	Non
8080	HTTP	TCP		Entrant	Serveur HTTP ; télécharge le VIB OMSA et répare les hôtes vSphere non conformes	Non
50	RMCP	UDP/TCP	128 bits	Sortant	Protocole de vérification de courrier à distance	Non
51	IMP	UDP/TCP	S/O	S/O	Maintenance d'adresse logique IMP	Non
5353	mDNS	UDP/TCP		Tous	DNS Multicast	Non
631	IPP	UDP/TCP	Aucun	Sortant	Internet Printing Protocol (IPP)	Non
69	TFTP	UDP	128 bits	Tous	Protocole simplifié de transfert de fichiers	Non
111	NFS	UDP/TCP	128 bits	Entrant	SUN Remote Procedure Call (Portmap)	Non
68	BOOTP	UDP	Aucun	Sortant	Client de protocole Boostrap	Non

Quelles sont les normes minimales qui s'appliquent pour réussir l'installation et la mise en marche de l'appliance virtuelle ?

Les paramètres suivants décrivent les normes minimales qui s'appliquent à l'appliance :

- RAM physique : 3 Go.
- Mémoire réservée : 1 Go

  REMARQUE : Dell recommande 3 Go pour optimiser les performances.
- Disque : 32.5 Go.
- UC : 2 UC virtuelles.

Pourquoi le mot de passe utilisé pour la découverte sans système d'exploitation ne change-t-il pas pour l'utilisateur après l'application réussie du profil matériel comportant le même utilisateur doté de nouvelles références modifiées dans la liste d'utilisateurs d'iDRAC ?

Le mot de passe utilisateur utilisé dans la découverte ne change pas pour refléter les références si le modèle de profil matériel est sélectionné pour le déploiement. Cela est intentionnel pour que le plug-in puisse communiquer avec le contrôleur iDRAC en vue d'une utilisation ultérieure pour des besoins liés au déploiement.

Pourquoi la version du processeur s'affiche-t-elle comme « Non applicable » dans la vue du processeur dans la page de présentation du système ?

Dans le cas des serveurs Dell PowerEdge de 12e génération et de générations ultérieures, la version du processeur se trouve dans la colonne Brand (Marque). Dans le cas d'une génération antérieure, la version de processeur est indiquée dans la colonne Version.

Pourquoi les paramètres de configuration de DNS sont-ils restaurés à leurs valeurs d'origine après le redémarrage du serveur si DHCP est utilisé pour l'adresse IP de l'appliance et les paramètres DNS écrasés

Il existe un bogue connu qui fait que les paramètres DNS attribués de façon statique, sont remplacés par des valeurs de DHCP. Cela peut se produire lorsque le DHCP est utilisé pour obtenir les valeurs des paramètres IP et les valeurs DNS sont attribuées de manière statique. Lorsque le bail DHCP est renouvelé ou que l'appliance est redémarrée, les paramètres de DNS attribués de façon statique sont supprimés. Résolution : attribuez de façon statique des paramètres IP lorsque paramètres du serveur DNS diffèrent de ceux de DHCP.

Versions concernées : Toutes

Pourquoi est-ce que les détails de ma nouvelle version iDRAC n'apparaissent pas sur la page des Clusters & Hôtes vCenter ?

Après avoir mis à jour le micrologiciel dans le volet de tâches récentes du client Web vSphere, actualisez la page de Mise à jour du micrologiciel et vérifiez les versions de ce dernier. Si d'anciennes versions apparaissent sur la page, allez à la page traitant de la Conformité de l'hôte dans l'OpenManage Integration pour VMware vCenter et vérifiez l'état CISOR de cet hôte. Si CISOR n'est pas activé, activez-le et redémarrez l'hôte. Si CISOR était déjà activé, connectez-vous à la console iDRAC, réinitialisez l'iDRAC, attendez quelques minutes, puis actualisez la page de Mise à jour du micrologiciel dans le client bureau vSphere.

Comment puis-je tester les paramètres d'événements en utilisant OMSA pour simuler un défaut matériel de température ?

Pour s'assurer que les événements fonctionnent correctement :

1. Dans l'interface utilisateur de l'OMSA, naviguez vers **Gestion des alertes** → **Événements de plateforme**.
2. Cochez la case **Enable Platform Event Filter Alerts (Activer les alertes du filtre d'événements de la plate-forme)**.
3. Faites défiler vers le bas, puis cliquez sur **Apply Changes (Appliquer les modifications)**.
4. Pour vous assurer qu'un événement spécifique est activé, par exemple l'alerte d'avertissement de température, à partir de l'arborescence à gauche, sélectionnez **Châssis principal du système**.
5. Sous **Châssis principal du système**, sélectionnez **Températures**.
6. Sélectionnez l'onglet **Alert Management (Gestion des alertes)**, et sélectionnez **Temperature Probe Warning (Avertissement de capteur de température)**.
7. Sélectionnez la case **Broadcast a Message (Diffuser un message)** et sélectionnez **Apply Changes (Appliquer les modifications)**.
8. Pour provoquer l'événement d'avertissement de la température, à partir de l'arborescence à gauche, sélectionnez **Châssis principal du système**.
9. Sélectionnez **Temperatures (Températures)** sous **Main System Chassis (Châssis principal du système)**.
10. Sélectionnez le lien **System Board Ambient Temp (Température ambiante de la carte système)**, et sélectionnez l'option **Set to Values (Définir les valeurs)**.
11. Configurez **Maximum Warning Threshold (Seuil maximal d'avertissement)** au-dessous de la valeur de lecture actuelle affichée ; par exemple, si la valeur de lecture actuelle est égale à 27, configurez le seuil sur **25**.
12. Sélectionnez **Apply Changes (Appliquer les modifications)**, et l'événement d'avertissement de température est généré. Pour provoquer un autre événement, restaurez les paramètres initiaux en utilisant la même option **Set to Values (Définir les valeurs)**. Les événements sont générés comme des avertissements, puis reviennent à un état normal. Si tout fonctionne correctement, accédez à la vue **vCenter Tasks & Events (Tâches et événements vCenter)**, un événement d'avertissement de capteur de température devrait être affiché.

   REMARQUE : Il existe un filtre pour les événements en double ; si vous essayez de déclencher le même événement trop de fois consécutivement, vous ne recevrez qu'un seul événement. Attendez au moins 30 secondes entre les événements pour voir tous les événements.

Alors que l'agent OMSA est installé sur un système hôte Dell, je reçois un message d'erreur disant que OMSA n'est pas intallé. Que dois-je faire ?

Pour résoudre ce problème sur un serveur de 11e génération :

1. Installez **OMSA** avec le composant **Remote Enablement (Activation à distance)** sur le système hôte.
2. Si vous utilisez la ligne de commande pour installer OMSA, assurez-vous de spécifier l'**option -c**. Si OMSA est déjà installé, réinstallez-le avec l'option -c et redémarrez le service :

   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

   Pour un hôte ESXi, vous devez installer **OMSA VIB** à l'aide de l'outil **VMware Remote CLI**, et redémarrer le système.

Le mode Verrouillage avec Support ESX/ESXI OpenManage Integration for VMware vCenter peut-il être activé ?

Oui. Le mode de verrouillage est pris en charge dans la présente version sur les hôtes ESXi version 4.1 et ultérieure.

L'inventaire échoue sur les hôtes ESXi 4.0 Update 2 et ESXi Update 3 en mode de verrouillage après un redémarrage.

Le mode de verrouillage nécessite ESXi version 4.1 ou ultérieure. Si vous utilisez une version ESXi antérieure, lorsqu'un hôte est redémarré pour une raison quelconque en mode de verrouillage, l'inventaire continue d'échouer, sauf si vous effectuez les étapes suivantes sur l'hôte après un redémarrage.

Les étapes de la solution de contournement pour ESXi 4.0 Update 2 et Update 3 sont les suivantes :

1. Dans **vSphere Client**, sélectionnez **Hosts and Clusters (Hôtes et Clusters)**, puis dans le volet gauche, sélectionnez l'**hôte** et puis cliquez sur l'onglet **Configuration**.
2. Dans le volet gauche, sous **Software (Logiciel)**, cliquez sur **Security Profile (Profil de sécurité)**.
3. Faites défiler vers le bas jusqu'à **Lockdown Mode (Mode de verrouillage)**, puis cliquez sur **Edit (Modifier)**.
4. Dans la boîte de dialogue **Lockdown Mode (Mode de verrouillage)**, pour désactiver le mode de verrouillage, désélectionnez la case **Enable (Activer)**, puis cliquez sur **OK**.
5. Connectez-vous à la console de l'hôte et sélectionnez **Restart Management Agents (Redémarrer les agents de gestion)**, appuyez sur **<ENTRÉE>** et, pour confirmer, appuyez sur **<F11>**.
6. Pour activer le mode de verrouillage, répétez les étapes 1 à 4, en sélectionnant cette fois la case **Enable (Activer)**, puis cliquez sur **OK**.

Quand j'ai essayé d'utiliser le mode de verrouillage, celui-ci a échoué.

Quand j'ai ajouté un hôte au profil de connexion en mode de verrouillage, l'inventaire a démarré, mais a échoué en indiquant qu'« aucun contrôleur d'accès à distance n'a été trouvé ou que l'inventaire n'est pas pris en charge sur cet hôte ». L'inventaire est bien censé marcher pour un hôte en mode de verrouillage ?

Si vous aviez mis l'hôte en mode de verrouillage ou retiré un hôte du mode verrouillage, vous devez attendre 30 minutes avant d'effectuer la prochaine opération sur la OpenManage Integration for VMware vCenter.

Lors d'une tentative de mise à jour du micrologiciel avec un progiciel DUP non valide, l'état de la tâche de mise à jour matérielle sur la console vCenter ne présente ni un échec ni un temps d'attente pendant des heures, même si l'état de la tâche dans LC est « ÉCHEC ». Pourquoi ?

Lorsque le progiciel DUP non valide est collecté pour la mise à jour du micrologiciel, l'état de la tâche dans la fenêtre de la console vCenter reste 'En cours', mais le message est modifié pour motif de panne. Il s'agit d'un bogue de VMWare connu qui sera corrigé dans les futures versions de VMware vCenter.

Résolution : la tâche doit être annulée manuellement.

Versions concernées : Toutes

Comment dois-je configurer UserVars.CIMoeMProviderEnable avec ESXi 4.1 U1 ?

Configurez **UserVars.CIMoemProviderEnabled** sur 1.

J'utilise un serveur de référence pour créer un profil matériel, mais il a échoué. Que dois-je faire ?

Assurez-vous que les versions minimales recommandées du micrologiciel iDRAC, du micrologiciel Lifecycle Controller et du BIOS sont installées.

Pour vous assurer que les données récupérées à partir du serveur de référence sont à jour, activez **Collect System Inventory On Restart (CSIOR) (Collecter l'inventaire du système au redémarrage)** et redémarrez le serveur de référence avant l'extraction des données. Voir Configuration de CSIOR sur un serveur de référence.

J'essaie de déployer ESX / ESXi sur un serveur lame, mais cela a échoué. Que dois-je faire ?

Pour résoudre ce problème, procédez comme suit :

1. Assurez-vous que l'**emplacement ISO (chemin NFS)** et les **chemins de dossiers** de préparation sont exacts.
2. Assurez-vous que la **carte réseau** sélectionnée lors de l'attribution de l'identité du serveur est sur le même réseau que l'appliance virtuelle.
3. Si vous utilisez une **adresse IP statique**, assurez-vous que les informations réseau fournies (y compris le masque de sous réseau et la passerelle par défaut) sont exactes. En outre, assurez-vous que l'adresse IP n'est pas déjà attribuée sur le réseau.
4. Assurez-vous qu'au moins un **disque virtuel** est détecté par le système. ESXi s'installe également à partir d'une carte SD RIPS interne.

Pourquoi mes déploiements d'hyperviseur échouent-ils sur les machines R210 II ?

Un problème d'expiration de délai sur les systèmes R210 II produit une erreur d'échec de déploiement d'hyperviseur en raison de l'échec du démarrage du BIOS depuis un ISO relié. Pour résoudre ce problème, installez manuellement l'hyperviseur sur la machine.

Pourquoi vois-je des systèmes détectés automatiquement sans information de modèle dans l'Assistant Déploiement ?

Cela indique généralement que la version du micrologiciel installé sur le système ne répond pas aux exigences minimales recommandées. Dans certains cas, une mise à jour du micrologiciel n'a pas été enregistrée sur le système. Un démarrage à froid du système ou la réinstallation de la lame permet de résoudre ce problème. Le compte nouvellement activé sur l'iDRAC doit être désactivé et la détection automatique relancée pour fournir les informations de modèle et de carte réseau au OpenManage Integration for VMware vCenter.

Le partage NFS est configuré avec l'ISO ESX / ESXi, mais le déploiement échoue avec des erreurs de montage de l'emplacement du partage.

Pour trouver la solution :

1. Assurez-vous que l'iDRAC est en mesure d'envoyer un ping à l'appliance.
2. Assurez-vous que votre réseau n'est pas trop lent.

Comment puis-je forcer la suppression de l'appliance virtuelle ?

1. Allez à **https://<AdresseIP_serveur_vcenter>/mob**
2. Entrez les informations d'identification de l'administrateur vCenter VMware.
3. Cliquez sur **Content (Contenu)** .
4. Cliquez sur **ExtensionManager (Gestionnaire d'extension)**.
5. Cliquez sur **UnregisterExtension (Désenregistrer l'extension)**.
6. Entrez la clé d'extension `com.dell.plugin.openManage_integration_for_VMware_vCenter`, puis cliquez sur **Appeler une méthode**.

7. Mettez hors tension l'appliance virtuelle OpenManage Integration for VMware vCenter et supprimez-le.

La saisie d'un mot de passe sur l'écran Backup Now (Sauvegarder maintenant) produit un message d'erreur

Si vous utilisez le moniteur en basse résolution, le champ Encryption Password (Mot de passe de cryptage) ne sera pas visible sur la fenêtre BACKUP NOW (Sauvegarder maintenant). Vous devez faire défiler la page vers le bas pour entrer le mot de passe de cryptage.

Ma mise à jour du micrologiciel a échoué. Que dois-je faire ?

Vérifiez les journaux de l'appliance virtuelle pour voir si les tâches ont expiré. Si c'est le cas, iDRAC doit être réinitialisé en effectuant un redémarrage à froid. Une fois que le système est en marche, vérifiez si la mise à jour a réussi en exécutant un inventaire ou en utilisant l'onglet Firmware (Micrologiciel).

Ma mise à jour vCenter a échoué. Que puis-je faire ?

L'enregistrement vCenter peut échouer en raison de problèmes de communication, donc si vous rencontrez ce type de problème, une solution consiste à utiliser une adresse IP statique. Pour utiliser une adresse IP statique, dans l'onglet Console de l'OpenManage Integration for VMware vCenter, sélectionnez **Configurer le réseau → Modifier les périphériques** et entrez la **passerelle** et le **FQDN** (nom de domaine complet) corrects. Entrez le nom du serveur DNS sous Modifier la configuartion DNS.

REMARQUE : Assurez-vous que l'appliance virtuelle peut trouver le serveur DNS que vous avez entré.

Les performances au cours de la lecture des informations d'identification du test de profil de connexion sont extrêmement lentes ou il n'y a pas de réponse

L'iDRAC sur un serveur n'a qu'un seul utilisateur (par exemple, l'utilisateur *root*) et l'utilisateur est dans un état désactivé, ou tous les utilisateurs sont dans un état désactivé. La communication avec un serveur se trouvant dans un état désactivé est ralentie. Pour résoudre ce problème, vous pouvez soit corriger l'état désactivé du serveur, ou réinitialiser iDRAC sur le serveur pour réactiver l'utilisateur root à la valeur par défaut.

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 **Launch iDRAC GUI (Lancer l'interface utilisateur iDRAC)**.
3. Accédez à la liste des utilisateurs dans la console iDRAC, et choisissez l'une des options suivantes :
   - iDRAC 6 : sélectionnez**iDRAC settings (Paramètres iDRAC) , onglet → Network/Security (Réseau / Sécurité) → onglet Users (Utilisateurs)**.
   - iDRAC 7 : sélectionnez **iDRAC settings (Paramètres iDRAC), → onglet Utilisateurs**.
   - iDRAC 7 : sélectionnez **iDRAC settings (Paramètres iDRAC), → onglet Utilisateurs**.
4. Pour modifier les paramètres, dans la colonne User ID (ID d'utilisateur), cliquez sur le lien correspondant à l'utilisateur admin (root).
5. Cliquez sur **Configure User (Configurer l'utilisateur)**, puis cliquez sur **Next (Suivant)**.
6. Sur la page User Configuration (Configuration de l'utilisateur) de l'utilisateur sélectionné, sélectionnez la case à côté de Enable user (Activer l'utilisateur), puis cliquez sur **Apply (Appliquer)**.

Est-ce que OpenManage Integration for VMware vCenter prend en charge l'appliance VMware vCenter Server ?

Oui, OpenManage Integration for VMware vCenter prend en charge l'appliance VMware vCenter Server.

Le OpenManage Integration for VMware vCenter prend-il en charge le client Web vSphere ?

Oui, le OpenManage Integration for VMware vCenter prend en charge le client Web vSphere VMware.

Dans l'Administration Console, pourquoi le chemin d'accès vers l'Espace de stockage des mises à jour n'est-il pas défini sur la valeur par défaut après que j'effectue une réinitialisation aux paramètres d'usine ?

Après la réinitialisation de l'appliance, accédez à l'Administration Console, puis cliquez sur **GESTION DE L'APPLIANCE** dans le volet gauche. Dans la page **Paramètres de l'appliance** , le **Chemin d'accès de l'espace de stockage des mises à jour** n'est pas changé en chemin d'accès par défaut.

Solution : dans l'Administration Console, copiez manuellement le chemin d'accès dans le champ **Espace de stockage de mise à jour par défaut** pour **Mettre à jour le chemin d'espace de stockage** .

Pourquoi les paramètres d'alarme ne sont-ils pas restaurés après la sauvegarde et la restauration d'OpenManage Integration for VMware vCenter ?

La restauration de la sauvegarde de l'appliance OpenManage Integration for VMware vCenter ne restaure pas les paramètres d'alarme. Cependant, dans l'interface utilisateur graphique d'OpenManage Integration for VMware, le champ **Alarmes et événements** affiche les paramètres restaurés.

Solution : dans l'interface utilisateur graphique d'OpenManage Integration for VMware, dans l'onglet **Gérer** → **Paramètres** , modifiez manuellement les paramètres d'**Événements et alarmes** .

Problèmes de déploiement de serveurs métal nu

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 micrologiciel iDRAC et Lifecycle Controller et du BIOS répondent aux recommandations minimales.
- La tâche CSIOR doit avoir été exécutée au moins une fois sur le système ou iDRAC.

Problème de configuration matérielle

- Avant de lancer une tâche de déploiement, assurez-vous que le système a terminé la tâche CSIOR et n'est pas en cours de redémarrage.
- Il est fortement recommandé d'exécuter 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 venant d'être acheté

La fonction de détection 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 détection automatique est demandée au moment de l'achat, DHCP est activé sur

l'iDRAC et les comptes admin 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 faire usage de la fonction de détection automatique, un serveur DHCP ou un serveur DNS (ou les deux) doit être configuré pour prendre en charge le processus de détection. La tâche CSIOR a déjà été exécutée par un processus d'usine. Pour plus d'informations sur la façon de configurer un réseau pour prendre en charge la détection automatique, consultez la Spécification de configuration de réseau de détection automatique Dell sur **http://attachments.wetpaintserv.us/xBUlrs4t%2B2TzbrwqYkblvQ%3D%3D262254**.

Si la détection automatique n'a pas été demandée au moment de l'achat, elle peut être activée comme suit :

1. Lors du processus d'amorçage, appuyez sur **<Ctrl-E>.**
2. Dans la fenêtre de configuration iDRAC, activez la carte réseau (serveurs lames uniquement).
3. Activez Auto-Discovery (Détection automatique).
4. Activez DHCP.
5. Désactivez les comptes admin.
6. Activez **Get DNS server address from DHCP (Obtention de l'adresse du serveur DNS via DHCP)**.
7. Activez **Get DNS domain name from DHCP (Obtention du nom de domaine DNS via DHCP)**.
8. Dans le champs **Provisioning Server (Serveur de provisionnement)**, entrez :
   `<OpenManage Integration virtual appliance IPaddress>:4433`

Contacter Dell

REMARQUE : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le borderau de colisage, la facture le catalogue des produits Dell.

Dell propose diverses options d'assistance et de maintenance en ligne et téléphonique. Ces options varient en fonction du pays et du produit et certains services peuvent ne pas être disponibles dans votre région Pour contacter le service commercial, technique ou client de Dell :

1. Consultez le site **dell.com/support**.
2. Sélectionnez la catégorie d'assistance.
3. Sélectionnez l'option appropriée dans le menu déroulant Country/Region (Pays/Région) situé en haut de la page.
4. Sélectionnez le lien de service ou d'assistance approprié.

OpenManage Integration for VMware vCenter Informations connexes

- Affichez ou téléchargez la documentation de serveur Dell pour les serveurs PowerEdge™ à l'adresse : http://www.dell.com/poweredgemanuals
- Documents Dell OpenManage System Administrator
  http:// www.delltechcenter.com/omsa
- Documentation Dell Lifecycle Controller
  http://www.dell.com/enterprisemanagement

8

Événements relatifs à la virtualisation des serveurs Dell PowerEdge

Le tableau suivant répertorie les seuils critiques et d'avertissement relatifs à la virtualisation, y compris le nom de l'événement, sa description et son niveau de gravité pour les 11e, 12e, et 13e générations de serveurs PowerEdge.

Tableau 5. Les événements relatifs à la virtualisation des 11e, et 12e et 13e générations de serveurs PowerEdge

Nom d'événement	Description	Gravité	Action recommandée
Dell-Current sensor detected a warning value	Un capteur de courant présent dans le système spécifié a dépassé son seuil d'avertissement.	Avertissement	Pas d'action
Dell-Current sensor detected a failure value	Un capteur de courant présent dans le système spécifié a dépassé son seuil de défaillance.	Erreur	Mettez le système en mode de maintenance
Dell-Current sensor detected a non-recoverable value	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-Redundancy regained	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell-Redundancy degraded	Un capteur de redondance 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 - Redundancy lost	Un capteur de redondance dans le système spécifié a détecté que l'un des composants de l'unité redondante a été déconnecté, est en panne, ou n'est pas présent.	Erreur	Mettez le système en mode de maintenance
Dell - Power supply returned to normal	Le capteur est revenu à une valeur normale	Informatif	Pas d'action

Dell - Power supply detected a warning	La lecture d'un capteur de bloc d'alimentation dans le système spécifié a dépassé un seuil d'avertissement configurable par l'utilisateur.	Avertissement	Pas d'action
Dell - Power supply detected a failure	Un bloc d'alimentation a été déconnecté ou a échoué.	Erreur	Mettez le système en mode de maintenance
Dell - Power supply sensor detected a non-recoverable value	Un capteur de bloc d'alimentation dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer.	Erreur	Pas d'action
Dell - Memory Device Status warning	Le taux de correction d'un périphérique de mémoire a dépassé une valeur acceptable.	Avertissement	Pas d'action
Dell - Memory Device error	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 - Fan enclosure inserted into system	Le capteur est revenu à une valeur normale.	Informatif	Pas d'action
Dell - Fan enclosure removed from system	Un boîtier de ventilateur a été retiré du système spécifié.	Avertissement	Pas d'action
Dell - Fan enclosure removed from system for an extended amount of time	Un boîtier de ventilateur a été retiré du système spécifié pendant une période configurable par l'utilisateur.	Erreur	Pas d'action
Dell - Fan enclosure sensor detected a non-recoverable value	Un capteur de boîtier de ventilateur dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer.	Erreur	Pas d'action
Dell - AC power has been restored	Le capteur est revenu à une valeur normale.	Informatif	Pas d'action
Dell - AC power has been lost warning	Un cordon d'alimentation secteur a perdu son alimentation, mais une	Avertissement	Pas d'action

	redondance suffisante existe pour classer cela comme un avertissement.		
Dell - An AC power cord has lost its power	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 - Processor sensor returned to a normal value	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Processor sensor detected a warning value	Un capteur de processeur dans le système spécifié est dans un état ralenti.	Avertissement	Pas d'action
Dell - Processor sensor detected a failure value	Un capteur de processeur dans le système spécifié est désactivé, présente une erreur de configuration, ou enregistre un déclenchement thermique.	Erreur	Pas d'action
Dell - Processor sensor detected a non-recoverable value	Un capteur de processeur dans le système spécifié a échoué.	Erreur	Pas d'action
Dell - Device configuration error	Une erreur de configuration a été détectée pour un dispositif enfichable dans le système spécifié.	Erreur	Pas d'action
Dell - Battery sensor returned to a normal value	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Battery sensor detected a warning value	Un capteur de batterie dans le système spécifié a détecté qu'une batterie se trouve dans un état de défaillance prédictive.	Avertissement	Pas d'action
Dell - Battery sensor detected a failure value	Un capteur de batterie dans le système spécifié a détecté que la batterie est défaillante.	Erreur	Pas d'action
Dell - Battery sensor detected a nonrecoverable value	Un capteur de batterie dans le système spécifié a détecté que la batterie est défaillante.	Erreur	Aucune action

Dell - Thermal shutdown protection has been initiated	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 - Temperature sensor returned to a normal value	Le capteur est revenu à une valeur normale.	Informatif	Pas d'action
Dell - Temperature sensor detected a warning value	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 - Temperature sensor detected a failure value	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 - Temperature sensor detected a non-recoverable value	Un capteur de température présent sur la carte de fond de panier, la carte système ou le logement du lecteur au sein du système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer.	Erreur	Pas d'action
Dell - Fan sensor returned to a normal value	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Fan sensor detected a warning value	La lecture d'un capteur de ventilateur dans l'hôte <x> a	Avertissement	Aucune action

	dépassé une valeur de seuil d'avertissement.		
Dell - Fan sensor detected a failure value	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 - Fan sensor detected a nonrecoverable value	Un capteur de ventilateur a détecté une erreur à partir de laquelle il ne peut pas récupérer.	Erreur	Pas d'action
Dell - Voltage sensor returned to a normal value	Le capteur est revenu à une valeur normale	Informatif	Pas d'action
Dell - Voltage sensor detected a warning value	Un capteur de tension présent dans le système spécifié a dépassé son seuil d'avertissement.	Avertissement	Pas d'action
Dell - Voltage sensor detected a failure value	Un capteur de tension présent dans le système spécifié a dépassé son seuil de défaillance.	Erreur	Mettez le système en mode de maintenance
Dell - Voltage sensor detected a nonrecoverable value	Un capteur de tension dans le système spécifié a détecté une erreur à partir de laquelle il ne peut pas récupérer.	Erreur	Pas d'action
Dell - Current sensor returned to a normal value	Le capteur est revenu à une valeur normale.	Informatif	Pas d'action
Dell - Storage: storage management error	La gestion du stockage a détecté un état d'erreur indépendant du périphérique.	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Controller warning	Avertissement du contrôleur. Reportez-vous à l'onglet Tâches et Événements du client vSphere pour plus d'informations.	Avertissement	Pas d'action
Dell - Storage: Controller failure	Échec du contrôleur. Reportez-vous à l'onglet Tâches et Événements du client vSphere pour plus d'informations.	Erreur	Mettez le système en mode de maintenance

Dell - Storage: Channel Failure	Défaillance de canal.	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Enclosure hardware information	Informations du matériel de l'enceinte	Informatif	Pas d'action
Dell - Storage: Enclosure hardware warning	Avertissement du matériel de l'enceinte.	Avertissement	Pas d'action
Dell - Storage: Enclosure hardware failure	Erreur du matériel de l'enceinte.	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Array disk failure	Défaillance d'un disque de matrice	Erreur	Mettez le système en mode de maintenance
Dell - Storage: EMM failure	Défaillance d'EMM	Erreur	Mettez le système en mode de maintenance
Dell - Storage: power supply failure	Défaillance de bloc d'alimentation	Erreur	Mettez le système en mode de maintenance
Dell - Storage: temperature probe warning	Avertissement de capteur de température de disque physique (trop froid ou trop chaud).	Avertissement	Pas d'action
Dell - Storage: temperature probe failure	Erreur de capteur de température de disque physique (trop froid ou trop chaud).	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Fan failure	Défaillance du ventilateur.	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Battery warning	Avertissement de la batterie.	Avertissement	Pas d'action
Dell - Storage: Virtual disk degraded warning	Avertissement de disque virtuel dégradé.	Avertissement	Pas d'action
Dell - Storage: Virtual disk degraded failure	Défaillance de disque virtuel dégradé	Erreur	Mettez le système en mode de maintenance
Dell - Storage: Temperature probe information	Informations de capteur de température	Informatif	Pas d'action
Dell - Storage: Array disk warning	Avertissement d'un disque de matrice.	Avertissement	Pas d'action
Dell - Storage: Array disk information	Informations d'un disque de matrice.	Informatif	Pas d'action
Dell - Storage: Power supply warning	Avertissement de bloc d'alimentation.	Avertissement	Pas d'action
Dell - Chassis Intrusion - Physical Security Violation	Intrusion dans le châssis - Violation de la sécurité physique	Erreur	Aucune action

Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	Événement relatif à l'intrusion dans le châssis (Violation de la sécurité physique) supprimé	INFOS	Aucune action
Dell - CPU Presence (Processor Presence detected)	Présence de l'UC (Présence du processeur détecté)	INFOS	Aucune action
Dell - System Event Log (SEL) Full (Logging Disabled)	Journal des événements système (SEL) plein (Connexion désactivée)	Erreur	Aucune action
Dell - System Event Log (SEL) Cleared	Journal des événements système (SEL) effacé	INFOS	Aucune action
Dell - SD Card redundancy Has Returned to Normal	La redondance de la carte SD est revenue à l'état normal	INFOS	Aucune action
Dell - SD Card Redundancy has been Lost	La redondance de la carte SD est perdue	Erreur	Aucune action
Dell - SD Card Redundancy Degraded	Redondance de la carte SD dégradée	Avertissement	Aucune action
Dell - Module SD Card Present (SD Card Presence Detected)	Carte SD du module présente (Présence de la carte SD détectée)	INFOS	Aucune action
Dell - Module SD Card Failed (Error)	Échec de la carte SD du module (Erreur)	Erreur	Aucune action
Dell - Module SD Card Write Protect(Warning)	Carte SD du module protégée contre l'écriture (Avertissement)	Avertissement	Aucune action
Dell - Module SD Card not Present	Carte SD du module absente	INFOS	Aucune action
Dell - Watchdog Timer Expired	Horloge de la surveillance expirée	Erreur	Aucune action
Dell - Watchdog Reset	Surveillance réinitialisée	Erreur	Aucune action
Dell - Watchdog Power Down	Surveillance hors tension	Erreur	Aucune action
Dell - Watchdog Power cycle	Cycle d'alimentation de la surveillance	Erreur	Aucune action
Dell - System Power Exceeds PSU Wattage	La puissance système excède le voltage du PSU	Erreur	Aucune action
Dell - System Power Exceeds Error Cleared	La puissance système excède l'erreur effacée	INFOS	Aucune action

Dell - Power Supply Inserted	Bloc d'alimentation inséré	INFOS	Aucune action
Dell - Internal Dual SD Module is present	Le double module SD interne est présent	INFOS	Aucune action
Dell - Internal Dual SD Module is online	Le double module SD interne est en ligne	INFOS	Aucune action
Dell - Internal Dual SD Module is operating normally	Le double module SD interne fonctionne normalement	INFOS	Aucune action
Dell - Internal Dual SD Module is write protected	Le double module SD interne est protégé contre l'écriture	Avertissement	Aucune action
Dell - Internal Dual SD Module is writable	Le double module SD interne est inscriptible	INFOS	Aucune action
Dell - Integrated Dual SD Module is absent	Le double module SD intégré est absent	Erreur	Aucune action
Dell - Integrated Dual SD Module redundancy is lost	Perte de la redondance du double module SD interne	Erreur	Aucune action
Dell - Internal Dual SD Module is redundant	Le double module SD interne est redondant	INFOS	Aucune action
Dell - Internal Dual SD Module is not redundant	Le double module SD interne n'est pas redondant	INFOS	Aucune action
Dell - Integrated Dual SD Module failure	Échec du double module SD intégré	Erreur	Aucune action
Dell - Internal Dual SD Module is offline	Échec du double module SD interne est hors ligne	Avertissement	Aucune action
Dell - Integrated Dual SD Module redundancy is degraded	Dégradation de la redondance du double module SD intégré	Avertissement	Aucune action
Dell - SD card device has detected a warning	Le périphérique de la carte SD a détecté un avertissement	Avertissement	Aucune action
Dell - SD card device has detected a failure	Le périphérique de la carte SD a détecté un échec	Erreur	Aucune action
Dell - Integrated Dual SD Module warning	Avertissement du double module SD intégré	Avertissement	Aucune action
Dell - Integrated Dual SD Module information	Informations relatives à l'avertissement du double module SD intégré	INFOS	Aucune action

Dell - Integrated Dual SD Module redundancy information	Informations relatives à la redondance du double module SD intégré	INFOS	Aucune action
Dell - Network failure or critical event	Défaillance réseau ou événement critique	Erreur	Aucune action
Dell - Network warning	Avertissement du réseau	Avertissement	Aucune action
Dell - Network information	Informations concernant le réseau	INFOS	Aucune action
Dell - Physical disk failure	Panne de disque physique	Erreur	Aucune action
Dell - Physical disk warning	Avertissement du disque physique	Avertissement	Aucune action
Dell - Physical disk information	Informations sur les disques physiques	INFOS	Aucune action
Dell - An error was detected for a PCI device	Une erreur a été détectée sur un périphérique PCI	Erreur	Aucune action
Dell - A warning event was detected for a PCI device	Un événement d'alerte a été détecté sur un périphérique PCI	Avertissement	Aucune action
Dell - An informational event was detected for a PCI device	Un événement informatif a été détecté sur un périphérique PCI	INFOS	Aucune action

A

Comprendre la détection automatique

La Détection automatique est un processus qui consiste à ajouter un serveur sans système d'exploitation Dell PowerEdge de 11e, 12e ou 13e génération à un pool de serveurs disponibles pour utilisation par l'OpenManage Integration for VMware vCenter. Une fois le serveur détecté, utilisez-le en vue du déploiement d'hyperviseur ou de matériel. Cette annexe fournit les informations nécessaires sur la détection automatique afin de vous aider à configurer le système. La Détection automatique est une fonctionnalité du Lifecycle Controller permettant de configurer un nouveau serveur et de l'enregistrer à l'aide de la console. Les avantages de l'utilisation de cette fonctionnalité comprennent notamment l'élimination du processus lourd de la configuration locale manuelle d'un nouveau serveur et la possibilité pour une console de détecter automatiquement un nouveau serveur qui a été connecté au réseau et mis sous tension.

La fonction Détection automatique est parfois appelée *Détection et protocole de transfert* en rapport avec le processus qu'elle effectue. Une fois qu'un nouveau serveur doté d'une fonction de détection automatique active est raccordé au secteur et connecté au réseau, le Lifecycle Controller du serveur Dell tente de *détecter* une console de déploiement intégrée au serveur de provisionnement Dell. La fonction Détection automatique lance alors un *protocole de transfert* entre le serveur de provisionnement et le Lifecycle Controller.

OpenManage Integration for VMware vCenter est une console de déploiement dotée d'un serveur de provisionnement intégré. L'emplacement du serveur de provisionnement est fourni à l'iDRAC à l'aide de diverses méthodes. L'adresse IP ou le nom d'hôte de l'emplacement du serveur de provisionnement sont définis sur l'adresse IP ou le nom d'hôte de la machine virtuelle de l'appliance OpenManage Integration for VMware vCenter.

REMARQUE : Un nouveau serveur configuré pour la Détection automatique tente de trouver l'emplacement du serveur de provisionnement toutes les 90 secondes sur une période de 24 heures. Ensuite, vous pourrez relancer manuellement la Détection automatique.

Lorsque l'OpenManage Integration for VMware vCenter reçoit la requête de détection automatique pour VMware vCenter, il valide le certificat SSL, puis lance toutes les procédures de sécurité configurées en option, notamment les certificats de sécurité et la validation de liste des expéditeurs certifiés côté client. Une deuxième demande de validation issue du nouveau serveur renvoie des références nom d'utilisateur/mot de passe temporaire devant être configurées sur l'iDRAC. Des appels ultérieurs sont lancés par l'OpenManage Integration for VMware vCenter pour VMware vCenter, qui recueille des informations sur le serveur, supprime les références temporaires et configure des références personnalisées permanentes pour l'accès administratif

En cas de réussite de la détection automatique, les références de déploiement fournies à la page **Paramètres** → **Déploiement** au moment de la détection sont créées sur l'iDRAC cible. Ensuite, la fonction Détection automatique est désactivée. Le serveur apparaît alors dans le pool de serveurs sans système d'exploitation disponibles sous l'option Déploiement dans l'OpenManage Integration for VMware vCenter.

La détection automatique peut actuellement être effectuée via le client vSphere Desktop.

Configuration requise pour la détection automatique

Avant toute tentative de détection de serveurs Dell PowerEdge sans système d'exploitation de 11e ou 12e génération ou de générations ultérieures, installez l'OpenManage Integration for VMware vCenter. Seuls les serveurs Dell PowerEdge de 11e génération ou de générations ultérieures dotés d'un iDRAC Express ou iDRAC Enterprise peuvent être détectés dans le pool de serveurs sans système d'exploitation OpenManage Integration for VMware vCenter. La connectivité

réseau à partir de l'iDRAC de serveur Dell sans système d'exploitation vers la machine virtuelle OpenManage Integration for VMware vCenter est requise.

REMARQUE : Les hôtes dotés d'hyperviseurs existants ne doivent pas être détectés dans le OpenManage Integration for VMware vCenter, à la place, ajoutez l'hyperviseur au profil de connexion, puis réconciliez-le avec le OpenManage Integration for VMware vCenter à l'aide de l'Assistant Conformité d'hôte.

Pour que la détection automatique se produise, les conditions suivantes doivent être réunies :

- **Alimentation :** connectez le serveur à la prise secteur. Il n'est pas nécessaire de mettre le serveur sous tension.
- **Connectivité réseau :** l'iDRAC du serveur doit disposer d'une connectivité réseau et doit communiquer avec le serveur de provisionnement sur le port 4433. Vous pouvez obtenir l'adresse IP à l'aide du serveur DHCP ou la spécifier manuellement dans l'utilitaire de configuration de l'iDRAC.
- **Paramètres réseau supplémentaires :** si vous utilisez DHCP, activez le paramètre *Obtenir l'adresse serveur DNS depuis DHCP* afin de permettre la survenance de la résolution de noms DNS.
- **Emplacement du service de provisionnement :** l'iDRAC doit connaître l'adresse IP ou le nom d'hôte du serveur du service.
- **Accès au compte désactivé :** activez l'accès du compte administratif pour l'iDRAC. S'il existe des comptes iDRAC possédant des droits d'administrateur, désactivez-les d'abord dans la console Web de l'iDRAC. Une fois la détection automatique terminée, le compte administrateur de l'iDRAC sera réactivé.
- **Détection automatique activée :** la détection automatique doit être activée sur l'iDRAC du serveur pour que le processus de détection automatique puisse commencer.

Activer et désactiver des comptes administratifs sur les serveurs iDRAC

Avant de configurer une détection automatique, désactivez tous les comptes d'administrateur autres que le compte racine. Le compte racine est désactivé pendant le processus de détection automatique. Une fois la détection automatique configurée, revenez à l'interface GUI de l'iDRAC6 et réactivez les comptes qui avaient été désactivés. Ce processus concerne les serveurs Dell PowerEdge de 11e, 12e et 13e générations.

REMARQUE : Pour éviter un échec de la détection automatique, activez un compte non admin sur l'iDRAC. Ceci permet un accès à distance en cas d'échec de la détection automatique.

1. Dans un navigateur, entrez l'**adresse IP d' iDRAC**.
2. Connectez-vous à l'**interface GUI d'iDRAC**.
3. Effectuez l'une des opérations suivantes :
   - Pour iDRAC6 : dans le volet gauche, sélectionnez l'onglet **Paramètres d'iDRAC** → **Réseau/Sécurité** → **Utilisateurs**.
   - Pour iDRAC7 : dans le volet gauche, sélectionnez l'onglet **Paramètres d'iDRAC** → **Authentification de l'utilisateur** → **Utilisateurs**.
4. Sous l'onglet Utilisateurs, localisez 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. À la page Configuration de l'utilisateur, sous Généralités, décochez la case **Activer l'utilisateur**.
8. Cliquez sur **Appliquer**.
9. Une fois la détection automatique configurée, répétez les étapes 1 à 8 pour réactiver chaque compte; cependant, cette fois-ci, cochez la case **Activer l'utilisateur**, puis cliquez sur **Appliquer**.

Configuration manuelle d'un serveur pour la détection automatique (11e génération de serveurs PowerEdge)

Vous devez disposer des adresses IP de l'iDRAC et de l'hôte.
Si vous n'avez pas commandé votre appliance sans système d'exploitation permettant d'utiliser la détection automatique auprès du fabricant, vous pouvez la configurer manuellement. L'iDRAC possède deux interfaces utilisateurs, tous deux accessibles à l'aide de l'adresse IP de l'iDRAC que vous souhaitez configurer.

En cas de réussite de détection automatique de serveurs sans système d'exploitation, le nouveau compte d'administrateur est créé ou un compte existant est activé avec les informations d'identification que le service de protocole de transfert a retournées. Tous les autres comptes administratifs qui n'avaient pas été désactivés avant la détection automatique ne sont pas activés. Vous devez réactiver ces comptes d'administrateur une fois que la détection automatique a réussi. Voir Activer ou désactiver des comptes d'administrateur sur iDRAC.

REMARQUE : Si, pour quelque raison, la détection automatique a échoué, vous ne pourrez pas vous connecter à distance à l'iDRAC. Pour que la connexion à distance réussisse, il vous faudra activer un compte non admin sur l'iDRAC. S'il n'existe pas de compte activé sur l'iDRAC, la seule façon d'accéder à l'iDRAC consiste à vous connecter localement à la boîte et d'activer le compte sur l'iDRAC.

1. Entrez l'**adresse IP de l'iDRAC** dans le navigateur.
2. Connectez-vous à l'**interface GUI d'iDRAC Enterprise**.
3. Sous l'onglet **Integrated Dell Remote Access Controller 6 — Enterprise** → **Résumé**, dans l'aperçu de la console virtuelle, cliquez sur **Lancer**.
4. Dans la boîte de dialogue Avertissement — Sécurité, cliquez sur **Oui**.
5. Dans la console de utilitaire d'iDRAC Utility, appuyez sur la touche **F12** une ou deux fois pour faire apparaître la boîte de dialogue Authentification requise.
6. Dans la boîte de dialogue Authentification requise, le nom s'affiche. Appuyez sur **Entrée**.
7. Entrez votre **mot de passe**.
8. Appuyez sur **Entrée**.
9. Lorsque la boîte de dialogue Arrêter/Redémarrer s'affiche, appuyez sur la touche **F11**.
10. L'hôte redémarre et l'écran affiche des informations relatives au chargement de la mémoire et du RAID. Ensuite, lorsqu'il affiche l'iDRAC et vous invite à appuyer sur les touches CTRL + E. Maintenant, appuyez immédiatement sur les touches **CTRL + E**.

    Si la boîte de dialogue s'affiche, cela signifie que votre action a fonctionné. Sinon, allez au menu Alimentation, puis mettez le système hors tension puis de nouveau sous tension avant de recommencer cette étape.

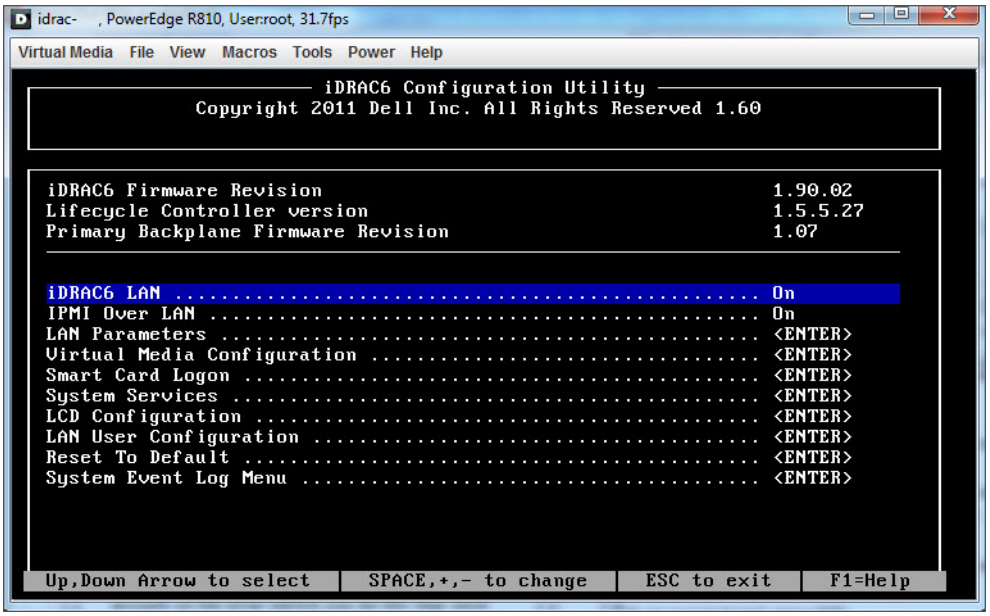

Figure 6. Appuyez sur les touches CTRL + E pour activer cet écran.

11. Dans l'utilitaire Configuration d'iDRAC6, utilisez les touches fléchées pour sélectionner l'option **Paramètres du LAN**.
12. Appuyez sur **Entrée**.
13. Si cet hôte est une lame, vous devez, pour configurer le NIC, utiliser la barre d'espacement afin de basculer les options sur **Activer**.
14. Si vous utilisez DHCP, utilisez les touches fléchées pour sélectionner l'option **Nom de domaine via DHCP**.
15. Utilisez la barre d'espacement pour basculer l'option sur **Activer**.
16. Si vous utilisez DHCP, utilisez les touches fléchées pour naviguer vers les paramètres IPv4, puis sélectionnez l'option **Serveurs DNS via DHCP**.
17. Utilisez la barre d'espacement pour basculer l'option sur **Activer**.
18. Pour quitter, appuyer sur la touche **Échap** de votre clavier.
19. Utilisez les touches fléchées pour sélectionner l'option **Configuration de l'utilisateur LAN** .
20. Utilisez les touches fléchées pour sélectionner l'option **Serveur de provisionnement**.
21. Appuyez sur **Entrée**.
22. Entrez l'adresse IP de l'hôte.
23. Appuyez sur la touche **Échap**.
24. Utilisez les touches fléchées pour sélectionner l'option **Accéder au compte**.
25. Utilisez la barre d'espacement pour basculer l'option sur **Désactiver**.
26. Utilisez les touches fléchées pour sélectionner l'option **Détection automatique**.
27. Utilisez la barre d'espacement pour basculer l'option sur **Activé**.
28. Appuyez sur la touche **Échap** de votre clavier.
29. Appuyez de nouveau sur **Échap**.

Configuration manuelle d'un serveur pour la détection automatique (12e génération de serveurs PowerEdge)

Vous devez disposer des adresses IP de l'iDRAC et de l'hôte.

Si vous n'avez pas commandé votre appliance sans système d'exploitation permettant d'utiliser la détection automatique auprès du fabricant, vous pouvez la configurer manuellement. L'iDRAC possède deux interfaces utilisateurs, tous deux accessibles à l'aide de l'adresse IP de l'iDRAC que vous souhaitez configurer.

En cas de réussite de détection automatique de serveurs sans système d'exploitation, le nouveau compte d'administrateur est créé ou un compte existant est activé avec les informations d'identification que le service de protocole de transfert a retournées. Tous les autres comptes administratifs qui n'avaient pas été désactivés avant la détection automatique ne sont pas activés. Réactivez ces comptes d'administrateur une fois que la détection automatique a réussi. Voir Activer ou désactiver des comptes d'administrateur sur iDRAC.

REMARQUE : Si, pour quelque raison, la détection automatique a échoué, vous ne pourrez pas vous connecter à distance à l'iDRAC. Pour que la connexion à distance réussisse, il vous faudra activer un compte non admin sur l'iDRAC. Si aucun compte n'est activé sur l'iDRAC, la seule façon d'accéder à l'iDRAC consiste à vous connecter localement à la boîte et d'activer le compte sur l'iDRAC.

1. Entrez l'**adresse IP de l'iDRAC** dans le navigateur.
2. Connectez-vous à l'**interface GUI d'iDRAC Enterprise**.
3. Sous l'onglet **Integrated Dell Remote Access Controller 7 — Enterprise** → **Résumé**, dans l'aperçu de la console virtuelle, cliquez sur **Lancer**.
4. Dans la boîte de dialogue Avertissement — Sécurité, cliquez sur **Oui**.
5. Dans la console de utilitaire d'iDRAC Utility, appuyez sur la touche **F12** une ou deux fois pour faire apparaître la boîte de dialogue Authentification requise.
6. Dans la boîte de dialogue Authentification requise, le nom s'affiche. Appuyez sur **Entrée**.
7. Entrez votre **mot de passe**.
8. Appuyez sur **Entrée**.
9. Lorsque la boîte de dialogue Arrêter/Redémarrer s'affiche, appuyez sur la touche **F11**.
10. L'hôte redémarre et l'écran affiche des informations relatives au chargement de mémoire et du RAID. Ensuite, lorsqu'il affiche un écran Dell vous invitant à appuyer sur la touche F2, appuyez immédiatement sur la touche **F2**.

    Patientez jusqu'à ce que l'écran Configuration du système Dell s'affiche. La configuration du système Dell prend quelques minutes avant de s'afficher.
11. Sur l'écran Configuration du système Dell, utilisez les touches fléchées pour sélectionner l'option **Paramètres d'iDRAC**.
12. Utilisez les touches fléchées pour sélectionner l'option **Activation à distance**.
13. Pour activer la détection automatique, cliquez sur **Activer**.
14. Appuyez sur la touche **Échap**.
15. Appuyez sur la touche **Échap**.
16. Sur l'écran Avertissement, cliquez sur **Oui** pour quitter.