Guide de l’utilisateur de Dell EMC OpenManage Enterprise version 3.7

Juillet 2021
Rév. A00

Remarques, précautions et avertissements

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

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

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

Table des matières

Tableaux

1

À propos de Dell EMC OpenManage Enterprise

OpenManage Enterprise est une application Web de gestion et de surveillance des systèmes fournie sous la forme d'une appliance virtuelle. Elle offre une vue complète des serveurs, châssis, périphériques de stockage et commutateurs réseau Dell EMC présents sur le réseau d'entreprise. Avec OpenManage Enterprise, une application Web de gestion de systèmes un-à-plusieurs, les utilisateurs peuvent :

- Détecter les périphériques présents dans un environnement de datacenter.
- Afficher l'inventaire matériel et surveiller l'intégrité des périphériques.
- Afficher et gérer les alertes reçues par l'appliance et configurer les stratégies d'alerte.
- Surveiller les versions des firmwares/pilotes et gérer les mises à jour des firmwares/pilotes sur les périphériques dotés de lignes de base de firmware.
- Gérer les tâches à distance (par exemple, le contrôle de l'alimentation) sur les périphériques.
- Gérer les paramètres de configuration sur les périphériques à l'aide des modèles de déploiement.
- Gérer les paramètres d'identité virtuelle sur les périphériques à l'aide des pools d'identités intelligents.
- Détecter et corriger les écarts de configuration sur les périphériques à l'aide des lignes de base de configuration.
- Récupérer et surveiller les informations sur la garantie des périphériques.
- Regrouper les périphériques dans des groupes statiques ou dynamiques.
- Créer et gérer les utilisateurs OpenManage Enterprise.

REMARQUE :

- Les fonctionnalités de surveillance et de gestion des systèmes d'OpenManage Enterprise conviennent particulièrement aux LAN d'entreprise et ne sont pas recommandées dans le cadre d'une utilisation sur des WAN.
- pour plus d'informations sur les navigateurs pris en charge, voir la *Matrice de support d'OpenManage Enterprise* disponible sur le site de support.

Ci-après certaines des fonctionnalités de sécurité d'OpenManage Enterprise :

- Accès basé sur des rôles limitant l'accès aux paramètres de la console et aux actions de périphérique.
- Le contrôle d'accès basé sur le périmètre permet aux administrateurs de limiter les groupes de périphériques auxquels les gestionnaires de périphériques peuvent accéder et qu'ils peuvent gérer.
- Appliance renforcée avec SELinux (Security-Enhanced Linux) et un pare-feu interne.
- Chiffrement des données sensibles dans une base de données interne.
- Utilisation de la communication chiffrée hors de l'appliance (HTTPs).
- Création et application des stratégies en rapport avec les configurations et les firmwares.
- Provisionnement pour la configuration et la mise à jour des serveurs sans système d'exploitation.

OpenManage Enterprise est doté d'une GUI basée sur le domaine et les tâches, dans laquelle la navigation est conçue en tenant compte de la séquence de tâches utilisée le plus souvent par un administrateur et par le gestionnaire de périphériques. Lorsque vous ajoutez un périphérique dans un environnement, OpenManage Enterprise détecte automatiquement ses propriétés, le place dans le groupe de périphériques approprié, et vous permet de le gérer. Séquence typique de tâches réalisées par les utilisateurs OpenManage Enterprise :

- Installation d'OpenManage Enterprise , page 20
- Configuration d'OpenManage Enterprise en utilisant l'interface texte utilisateur , page 27
- Détection de périphériques pour la surveillance ou la gestion , page 41
- Gestion des périphériques et des groupes de périphériques , page 55
- Surveillance des appareils à l'aide du tableau de bord OpenManage Enterprise , page 38
- Organisation des périphériques dans des groupes , page 55
- Gestion des firmwares et des pilotes de périphérique , page 77
- Affichage et configuration des périphériques individuels , page 68
- Surveillance et gestion des alertes d'appareil , page 118
- Affichage et renouvellement de la garantie des appareils , page 138
- Gérer des modèles de déploiement d'appareil , page 86
- Gestion de la conformité de la configuration du périphérique , page 110
- Gérer les modèles de conformité , page 111
- Surveillance des journaux d'audit , page 127
- Gestion des paramètres de l'appliance OpenManage Enterprise , page 147

- Exécution immédiate d'une tâche d'inventaire , page 75
- Gestion de la garantie des périphériques , page 137
- Rapports , page 139
- Gestion des fichiers MIB , page 144
- Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Intégration de services d'annuaire dans OpenManage Enterprise , page 156

Sujets :

Nouveautés de cette version

- Prise en charge du plug-in CloudIQ : un ou plusieurs groupes de périphériques peuvent être sélectionnés pour envoyer des données à CloudIQ à des fins de surveillance.

Améliorations

- Possibilité d'afficher les périphériques qui ont été déconnectés en cas d'échec d'authentification à partir de la page Tous les périphériques.
- Fonctionnalités d'interface texte utilisateur (TUI) pour activer ou désactiver l'enregistrement de débogage pour les services d'appliance et de plug-in.

Autres informations utiles

En plus de ce guide, vous pouvez accéder aux documents suivants, qui fournissent plus d'informations sur OpenManage Enterprise et d'autres produits connexes.

Tableau 1. Autres informations utiles

Document	Description	Disponibilité
Matrice de support de Dell EMC OpenManage Enterprise	Répertorie les périphériques pris en charge par OpenManage Enterprise.	1. Rendez-vous sur Dell.com/OpenManageManuals. 2. Cliquez sur **Dell OpenManage Enterprise** et sélectionnez la version requise d'OpenManage Enterprise. 3. Cliquez sur **Documentation** pour accéder à ces documents.
Notes de mise à jour Dell EMC OpenManage Enterprise	Fournit des informations sur les problèmes connus d'OpenManage Enterprise et les solutions à ces problèmes.	
Guide de l'utilisateur de Dell EMC OpenManage Mobile	Fournit des informations sur l'installation et l'utilisation de l'application OpenManage Mobile.	
Guide de l'utilisateur Dell EMC Repository Manager	Fournit des informations sur l'utilisation de Gestionnaire des espaces de stockage pour gérer les mises à jour du système.	
Guide API RESTful de Dell EMC OpenManage Enterprise et OpenManage Enterprise – Modular Edition	Fournit des informations sur l'intégration d'OpenManage Enterprise en utilisant les API REST (Representational State Transfer) et comprend également des exemples d'utilisation des API REST pour effectuer des tâches courantes.	
Guide de l'utilisateur de Dell EMC OpenManage Enterprise Services (anciennement SupportAssist Enterprise)	Fournit des informations sur l'installation, la configuration, l'utilisation et le dépannage d'OpenManage Enterprise.	Dell.com/ServiceabilityTools

Tableau 1. Autres informations utiles (suite)

Document	Description	Disponibilité
Dell EMC OpenManage Enterprise Power Manager	Fournit des informations sur l'installation, la configuration, l'utilisation et le dépannage d'OpenManage Enterprise Power Manager.	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_power_manager
Dell EMC OpenManage Enterprise Update Manager	Fournit des informations sur l'installation, la configuration, l'utilisation et le dépannage d'OpenManage Enterprise Update Manager.	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_openmanage_enterprise_update_manager
Dell EMC CloudIQ	Fournit des informations sur l'installation, la configuration, l'utilisation et le dépannage de CloudIQ.	

Contacter Dell EMC

REMARQUE : Si vous ne disposez pas d'une connexion Internet active, vous trouverez les coordonnées sur votre facture d'achat, bordereau d'expédition, facture ou catalogue de produits Dell EMC.

Dell EMC propose plusieurs options de services et support en ligne et par téléphone. La disponibilité des services varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre zone géographique. Pour toute question commerciale, de support technique ou de service à la clientèle, n'hésitez pas à contacter Dell EMC :

1. Rendez-vous sur Dell.com/support.
2. Sélectionnez la catégorie de support.
3. Rechercher votre pays ou région dans le menu déroulant **Choisissez un pays ou une région** situé au bas de la page.
4. Sélectionnez le lien correspondant au service ou au support technique requis.

Licence OpenManage Enterprise Advanced

REMARQUE : La licence *OpenManage Enterprise Advanced* n'est pas obligatoire pour l'installation et l'utilisation d'OpenManage Enterprise. Seule la fonctionnalité de gestion de la configuration de serveur (déploiement des configurations d'appareil et vérification de la conformité de la configuration sur les serveurs) exige que la licence *OpenManage Enterprise Advanced* soit installée sur les serveurs cibles. Cette licence n'est pas obligatoire pour la création de modèles de déploiement à partir d'un serveur.

La licence *OpenManage Enterprise Advanced* est une licence perpétuelle, valide pendant toute la durée de vie du serveur. Vous pouvez la lier au numéro de série, pour un seul serveur à la fois. OpenManage Enterprise fournit un rapport intégré qui présente la liste des périphériques et leurs licences. Sélectionnez **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport de licence**, puis cliquez sur **Exécuter**. Voir la section Exécution des rapports , page 140.

REMARQUE : L'activation de la fonctionnalité de gestion de la configuration de serveur d'OpenManage Enterprise ne nécessite aucune licence distincte. Si la licence *OpenManage Enterprise Advanced* est installée sur un serveur cible, vous pouvez utiliser la fonctionnalité de gestion de la configuration sur ce serveur.

Licence OpenManage Enterprise Advanced : les serveurs pris en charge

Vous pouvez déployer la licence *OpenManage Enterprise Advanced* sur les serveurs PowerEdge suivants :

- Serveurs YX3X disposant de la version 2.50.50.50 ou ultérieure du firmware iDRAC8. Les versions du firmware YX3X sont rétro-compatibles et peuvent être installées sur du matériel YX2X. Voir Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.
- Serveurs YX4X disposant de la version 3.10.10.10 ou ultérieure du firmware iDRAC9. Voir Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185

Achat de la licence OpenManage Enterprise Advanced

Vous pouvez acheter la licence *OpenManage Enterprise Advanced* lors de l'achat d'un serveur ou en contactant votre agent commercial. Vous pouvez télécharger les licences acquises depuis le portail de gestion de licences logicielles à l'adresse Dell.com/support/retail/lkm.

Vérification des informations de licence

L'application OpenManage Enterprise fournit un rapport intégré qui affiche la liste des périphériques qu'elle surveille ainsi que leurs licences. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport de licence**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

Vous pouvez vérifier si la licence *OpenManage Enterprise Advanced* est installée sur un serveur en procédant comme suit :

- Sur toutes les pages d'OpenManage Enterprise, cliquez sur le symbole **i**, puis cliquez sur **Licences** dans le coin supérieur droit.
- Dans la boîte de dialogue **Licences**, lisez le message et cliquez sur les liens appropriés pour afficher et télécharger les fichiers open source liés à OpenManage Enterprise ou d'autres licences open source.

Fonctions basées sur les licences dans OpenManage Enterprise

La licence *OpenManage Enterprise Advanced* est obligatoire pour utiliser les fonctionnalités suivantes d'OpenManage Enterprise :

- Déploiement de la configuration de serveurs.
- Création et correction de la ligne de base de conformité de configuration de serveurs.
- Amorçage à partir de l'image ISO.
- Activation des plug-ins disponibles (par exemple, Power Manager) pour étendre la capacité de l'appliance.

REMARQUE : Pour accéder aux fonctionnalités d'OpenManage Enterprise, telles que la fonction de support de la Console virtuelle, qui dépend d'iDRAC, vous avez besoin de la licence iDRAC Enterprise. Pour plus d'informations, consultez la *documentation d'iDRAC* disponible sur le site de support.

2

Fonctionnalités de sécurité d'OpenManage Enterprise

Ci-après certaines des fonctionnalités de sécurité d'OpenManage Enterprise :

- Le contrôle d'accès basé sur les rôles permet de gérer différentes fonctionnalités de gestion des périphériques pour différents rôles d'utilisateur (Administrateur, Gestionnaire de périphériques, Observateur).
- Le contrôle d'accès basé sur le périmètre permet à un administrateur de déterminer les groupes de périphériques que les gestionnaires de périphériques sont censés gérer.
- Appliance renforcée avec SELinux (Security-Enhanced Linux) et un pare-feu interne.
- Chiffrement des données sensibles dans une base de données interne.
- Utilisation de la communication chiffrée hors de l'appliance (HTTPS).
- Seuls les navigateurs dotés du chiffrement 256 bits sont pris en charge. Pour en savoir plus, reportez-vous à la section Configuration matérielle minimale requise pour le déploiement d'OpenManage Enterprise , page 21

AVERTISSEMENT : Les utilisateurs non autorisés peuvent obtenir l'accès au niveau du système d'exploitation à l'appliance OpenManage Enterprise en contournant les restrictions de sécurité de Dell EMC. L'une des possibilités consiste à mettre le disque de la machine virtuelle (VMDK) dans une autre machine virtuelle Linux comme disque secondaire afin d'obtenir l'accès à la partition du système d'exploitation sur laquelle les informations d'identification de connexion au niveau du système d'exploitation peuvent éventuellement être modifiées. Dell EMC recommande à ses clients de crypter le disque (fichier image) pour rendre plus difficile l'accès non autorisé. Les clients doivent également veiller à ce que les mécanismes de chiffrement utilisés leur permettent de déchiffrer les fichiers ultérieurement, sous peine de ne plus pouvoir amorcer le périphérique.

REMARQUE :

- Toute modification apportée au rôle d'utilisateur prendra effet immédiatement et les utilisateurs concernés seront déconnectés de leur session active.
- les utilisateurs des répertoires AD et LDAP peuvent être importés et attribués à l'un des rôles d'OpenManage Enterprise (Admin, Gestionnaire de périphériques ou Observateur).
- L'exécution d'actions de gestion des périphériques nécessite un compte avec les privilèges appropriés sur l'appareil donné.

Sujets :

Types de rôles d'utilisateur OpenManage Enterprise

REMARQUE :

- les utilisateurs des répertoires AD et LDAP peuvent être importés et attribués à l'un des rôles d'OpenManage Enterprise (Admin, Gestionnaire de périphériques ou Observateur).
- Les actions exécutées sur les périphériques nécessitent un compte doté de privilèges sur le périphérique.

Tableau 2. Types de rôles d'utilisateur OpenManage Enterprise

Un utilisateur doté de ce rôle ...	Dispose des privilèges utilisateur suivants
Administrateur	Un administrateur dispose d'un accès complet à toutes les tâches qui peuvent être réalisées sur la console. • Il bénéficie d'un accès complet (à l'aide de l'interface GUI et REST) pour lire, afficher, créer, modifier, supprimer, exporter

Tableau 2. Types de rôles d'utilisateur OpenManage Enterprise (suite)

Un utilisateur doté de ce rôle ...	Dispose des privilèges utilisateur suivants
	et supprimer des informations relatives aux périphériques et groupes surveillés par OpenManage Enterprise. ● Il peut créer un Microsoft Active Directory (AD) local et des utilisateurs LDAP, et leurs attribuer des rôles appropriés ● Activer et désactiver des utilisateurs ● Modifier les rôles d'utilisateurs existants ● Supprimer les utilisateurs ● Modifier le mot de passe de l'utilisateur
Gestionnaire de périphériques	● Exécuter des tâches, des politiques et d'autres actions sur les appareils (du champ d'application) affectés par l'administrateur.
Observateur	● Un observateur peut uniquement consulter les informations affichées sur OpenManage Enterprise et exécuter des rapports. ● Par défaut, il dispose d'un accès en lecture seule à la console et à tous les groupes. ● Ne peut pas exécuter de tâches ou créer et gérer des stratégies.

REMARQUE :

- Si un Observateur ou un Gestionnaire de périphériques devient un Administrateur, il obtient l'ensemble des privilèges Administrateur. Si un Observateur devient Gestionnaire de périphériques, l'Observateur dispose des mêmes privilèges qu'un Gestionnaire de périphériques.
- Toute modification apportée au rôle d'utilisateur prendra effet immédiatement et les utilisateurs concernés seront déconnectés de leur session active.
- Un journal d'audit est enregistré lorsque :
  - Un groupe est attribué ou une autorisation d'accès est modifiée.
  - Le rôle d'utilisateur est modifié.

Information associée

Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise

OpenManage Enterprise possède un contrôle d'accès basé sur les rôles (RBAC) qui définit clairement les privilèges utilisateur pour les trois rôles intégrés : Administrateur, Gestionnaire de périphériques et Observateur. En outre, l'utilisation du contrôle d'accès basé sur le périmètre (SBAC) permet à un administrateur de limiter les groupes de périphériques auxquels un gestionnaire de périphériques a accès. Les rubriques suivantes décrivent en détail les fonctions RBAC et SBAC.

Privilèges du contrôle d'accès basé sur les rôles (RBAC) dans OpenManage Enterprise

Les utilisateurs se voient attribuer des rôles qui déterminent leur niveau d'accès aux paramètres de l'appliance et aux fonctionnalités de gestion des périphériques. Cette fonctionnalité est intitulée Contrôle d'accès basé sur les rôles. La console applique le privilège demandé pour une action spécifique avant d'autoriser cette action. Pour plus d'informations sur la gestion des utilisateurs sur OpenManage Enterprise, voir Gestion des utilisateurs OpenManage Enterprise , page 148.

Ce tableau répertorie les divers privilèges qui sont activés pour chaque rôle.

Tableau 3. Privilèges d'utilisateur basés sur des rôles dans OpenManage Enterprise

Fonctionnalités d'OpenManage Enterprise	Description des privilèges	Niveaux d'utilisateur pour l'accès à OpenManage Enterprise		
		Admin	Gestionnaire de périphériques	Observateur
configuration d'appliance	Paramètres de l'appliance globale impliquant la configuration de l'appliance.	O	N	N
Configuration de la sécurité	Paramètres de sécurité de l'appliance	O	N	N
Gestion des alertes	Actions/gestion des alertes	O	N	N
Gestion de la structure	Actions/gestion de la structure	O	N	N
Gestion du réseau	Actions/gestion du réseau	O	N	N
Gestion des groupes	Créer, lire, mettre à jour et supprimer (CRUD = Create, Read, Update, Delete) pour les groupes statiques et dynamiques	O	N	N
Gestion de la détection	Opérations CRUD sur les tâches de détection, exécution de tâches de détection	O	N	N
Gestion d'inventaire	Opérations CRUD sur les tâches d'inventaire, exécution de tâches d'inventaire	O	N	N
Gestion des interruptions	Importation de MIB, modification d'interruption	O	N	N
Gestion des déploiements automatiques	Gestion des opérations de configuration de déploiement automatique	O	N	N
Configuration de la surveillance	Politiques d'alerte, transfert, SupportAssist, etc.	O	O	N
Bouton d'alimentation	Redémarrage/cycle d'alimentation de l'appareil	O	O	N
Configuration de périphérique	Configuration de l'appareil, application de modèles, gestion/migration de l'identité d'E/S, adressage du stockage (pour les appareils de stockage), etc.	O	O	N
Déploiement des systèmes d'exploitation	Déploiement du système d'exploitation, adressage de LUN, etc.	O	O	N
Mise à jour de l'appareil	Mise à jour de firmware de l'appareil, application des lignes de base mises à jour, etc.	O	O	N
Gestion des modèles	Création/gestion de modèles	O	O	N
Gestion des lignes de base	Création/gestion de politiques de ligne de base de firmware/configuration	O	O	N
Gestion de l'alimentation	Définition de budgets d'alimentation	O	O	N
Gestion des tâches	Exécution/gestion de tâches	O	O	N
Gestion des rapports	Opérations CRUD sur les rapports	O	O	N

Tableau 3. Privilèges d'utilisateur basés sur des rôles dans OpenManage Enterprise (suite)

Fonctionnalités d'OpenManage Enterprise	Description des privilèges	Niveaux d'utilisateur pour l'accès à OpenManage Enterprise		
		Admin	Gestionnaire de périphériques	Observateur
Exécution des rapports	Exécution des rapports	O	O	O
Afficher	Affichage de toutes les données, exécution/gestion des rapports, etc.	O	O	O

Contrôle d'accès basé sur le périmètre (SBAC) dans OpenManage Enterprise

En utilisant la fonction de contrôle d'accès basé sur les rôles (RBAC), les administrateurs peuvent attribuer des rôles lors de la création d'utilisateurs. Les rôles déterminent leur niveau d'accès aux paramètres de l'appliance et aux fonctionnalités de gestion des périphériques. Le contrôle d'accès basé sur le périmètre (SBAC) est une extension de la fonction RBAC qui permet à un administrateur de restreindre un rôle de gestionnaire de périphériques à un sous-ensemble de groupes de périphériques appelé périmètre.

Lors de la création ou de la mise à jour d'un utilisateur gestionnaire de périphériques, les administrateurs peuvent attribuer le périmètre afin de limiter l'accès opérationnel du gestionnaire de périphériques à un ou plusieurs groupes de systèmes, groupes personnalisés et/ou groupes de plug-ins.

Les rôles Administrateur et Observateur possèdent un périmètre illimité. Cela signifie qu'ils disposent d'un accès opérationnel tel que spécifié par les privilèges de RBAC à toutes les entités de périphériques et de groupes.

Le périmètre peut être mis en œuvre comme suit :

1. Créer ou modifier un utilisateur
2. Attribuer un rôle Gestionnaire de périphériques
3. Attribuer le périmètre afin de limiter l'accès opérationnel

Pour plus d'informations sur la gestion des utilisateurs, voir Gestion des utilisateurs OpenManage Enterprise , page 148.

Lorsqu'un utilisateur gestionnaire de périphériques avec un périmètre attribué se connecte, le gestionnaire de périphériques peut uniquement voir et gérer les périphériques définis. En outre, le gestionnaire de périphériques peut voir et gérer des entités telles que les tâches, les modèles de firmware ou de configuration et les lignes de base, les stratégies d'alerte, les profils, etc. associés aux périphériques définis, uniquement si le gestionnaire de périphériques possède l'entité (il l'a créée ou la détient). Pour plus d'informations sur les entités qu'un gestionnaire de périphériques peut créer, reportez-vous à la section *Privilèges du contrôle d'accès basé sur les rôles dans OpenManage Enterprise*.

Par exemple, en cliquant sur **Configuration** > **Modèles**, un utilisateur gestionnaire de périphériques peut afficher les modèles par défaut et personnalisés appartenant à l'utilisateur gestionnaire de périphériques. En outre, l'utilisateur gestionnaire de périphériques peut effectuer d'autres tâches, comme RBAC le privilégie, sur les modèles qu'il possède.

En cliquant sur **Configuration** > **Pools d'identités**, un utilisateur gestionnaire de périphériques peut voir toutes les identités créées par un administrateur ou l'utilisateur gestionnaire de périphériques. Le gestionnaire de périphériques peut également effectuer des actions sur les identités spécifiées par le privilège RBAC. Toutefois, le gestionnaire de périphériques peut uniquement consulter l'utilisation de ces identités qui sont associées aux périphériques dans le périmètre du gestionnaire de périphériques.

De même, en cliquant sur **Configuration** > **Pools VLAN**, le gestionnaire de périphériques peut voir tous les VLAN créés par l'administrateur et les exporter. Le gestionnaire de périphériques ne peut pas effectuer d'autres opérations. Si le gestionnaire de périphériques possède un modèle, il peut le modifier pour utiliser les réseaux VLAN, mais il ne peut pas modifier le réseau VLAN.

Dans OpenManage Enterprise, le périmètre peut être attribué lors de la création d'un utilisateur local ou de l'importation d'un utilisateur AD/LDAP. L'attribution du périmètre aux utilisateurs OIDC peut être effectuée uniquement sur les fournisseurs Open ID Connect (OIDC).

SBAC pour les utilisateurs locaux :

Lors de la création ou de la modification d'un utilisateur local doté du rôle Gestionnaire de périphériques, l'administrateur peut sélectionner un ou plusieurs groupes de périphériques qui définissent le périmètre du gestionnaire de périphériques.

Par exemple, vous (en tant qu'administrateur) créez un utilisateur Gestionnaire de périphériques nommé dm1 et attribuez le groupe *g1* présent sous des groupes personnalisés. Ensuite, dm1 aura un accès opérationnel à tous les périphériques dans *g1* uniquement. L'utilisateur dm1 ne pourra pas accéder à d'autres groupes ou entités lié(e)s à d'autres périphériques.

En outre, avec SBAC, dm1 ne pourra pas non plus voir les entités créées par d'autres gestionnaires de périphériques (disons dm2) sur le même groupe *g1*. Cela signifie que l'utilisateur Gestionnaire de périphériques ne pourra voir que les entités appartenant à l'utilisateur.

Par exemple, vous (en tant qu'administrateur) créez un autre utilisateur gestionnaire de périphériques nommé dm2 et attribuez le même groupe *g1* présent sous des groupes personnalisés. Si dm2 crée un modèle de configuration, des lignes de base de configuration ou des profils pour les périphériques dans *g1*, dm1 n'aura pas accès à ces entités et vice versa.

Un gestionnaire de périphériques avec le périmètre défini sur Tous les périphériques a un accès opérationnel, tel que spécifié par les privilèges de RBAC, à tous les périphériques et toutes les entités de groupe appartenant au gestionnaire de périphériques.

SBAC pour les utilisateurs d'AD/LDAP :

Lors de l'importation ou de la modification des groupes AD/LDAP, les administrateurs peuvent attribuer des périmètres à des groupes d'utilisateurs dotés du rôle Gestionnaire de périphériques. Si un utilisateur est membre de plusieurs groupes AD, chacun doté d'un rôle Gestionnaire de périphériques, et que chaque groupe AD a des attributions de périmètre distinctes, le périmètre de l'utilisateur correspond à l'union des périmètres de ces groupes AD.

Par exemple :

- L'utilisateur dm1 est membre de deux groupes AD (*RR5-Floor1-LabAdmins* et *RR5-Floor3-LabAdmins*). Les deux groupes AD ont reçu le rôle Gestionnaire de périphériques. Les attributions de périmètre pour les groupes AD sont les suivantes : *RR5-Floor1-LabAdmins* obtient *ptlab-servers* et *RR5-Floor3-LabAdmins* obtient *smdlab-servers*. Désormais, le périmètre du gestionnaire de périphériques dm1 est l'union de *ptlab-servers* et de *smdlab-servers*.
- L'utilisateur dm1 est membre de deux groupes AD (*adg1* et *adg2*). Les deux groupes AD ont reçu le rôle gestionnaire de périphériques, avec des attributions de périmètre pour les groupes AD, comme suit : *adg1* a accès à *g1* et *adg2* a accès à *g2*. Si *g1* est le super-ensemble de *g2*, le périmètre de dm1 correspond au périmètre plus étendu (*g1*, à tous ses groupes enfants et tous les périphériques de noeud feuille).

Lorsqu'un utilisateur est membre de plusieurs groupes AD ayant des rôles différents, le rôle de fonctionnalité supérieure est prioritaire (dans l'ordre Administrateur, Gestionnaire de périphériques, Observateur).

Un gestionnaire de périphériques avec périmètre illimité dispose d'un accès opérationnel tel que spécifié par les privilèges de RBAC à toutes les entités de périphériques et de groupes.

REMARQUE : Après la mise à niveau d'OpenManage Enterprise depuis la version 3.5 ou une version antérieure, les gestionnaires de périphériques AD/LDAP et OIDC (PingFederate ou KeyCloak) doivent recréer toutes les entités de la version précédente, puisque ces entités ne sont disponibles que pour les administrateurs après la mise à niveau. Pour en savoir plus, consultez les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC pour les utilisateurs d'OIDC :

L'attribution du périmètre aux utilisateurs d'OIDC n'a pas lieu dans la console OME. Vous pouvez attribuer des périmètres aux utilisateurs d'OIDC au niveau d'un fournisseur OIDC lors de la configuration de l'utilisateur. Lorsque l'utilisateur se connecte avec les informations d'identification du fournisseur OIDC, le rôle et l'attribution du périmètre seront disponibles pour OME. Pour en savoir plus sur la configuration des périmètres et rôles utilisateur, voir Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161.

REMARQUE : Si PingFederate est utilisé en tant que fournisseur OIDC, seuls les rôles d'administrateur peuvent être utilisés. Pour en savoir plus, consultez la section Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161 et les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfert de propriété : l'administrateur peut transférer les ressources dont il est propriétaire d'un gestionnaire de périphériques (source) vers un autre gestionnaire de périphériques. Par exemple, un administrateur peut transférer toutes les ressources attribuées à partir d'un dm1 source vers dm2. Un gestionnaire de périphériques avec des entités détenues, telles que les lignes de base du firmware et/ou de configuration, les modèles de configuration, les stratégies d'alerte et les profils est considéré comme un utilisateur source éligible. Le transfert de propriété transfère uniquement les entités et non les groupes de périphériques (périmètre) appartenant à un gestionnaire de périphériques vers un autre. Pour plus d'informations, voir Transfert de propriété des entités du gestionnaire de périphériques , page 155.

Références connexes

Types de rôles d'utilisateur OpenManage Enterprise , page 15

3

Installation d'OpenManage Enterprise

Dell EMC OpenManage Enterprise est fourni en tant qu'appliance que vous pouvez installer sur un hyperviseur. Il vous permet de gérer les ressources pour minimiser l'interruption de service. L'appliance virtuelle est configurable à partir de la console Web de l'application après le provisionnement réseau initial dans l'interface utilisateur texte (TUI). Pour connaître les étapes d'affichage et de mise à jour de la version de la console, voir Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168. Ce chapitre décrit les conditions préalables et la configuration minimales requises pour l'installation.

REMARQUE : Pour plus d'informations sur les navigateurs pris en charge, voir la *Matrice de support d'OpenManage Enterprise* disponible sur le site de support.

Sujets :

Prérequis pour l'installation et configuration minimale requise

Pour une liste des plateformes, systèmes d'exploitation et navigateurs pris en charge, voir la *matrice de prise en charge Dell EMC OpenManage Enterprise* sur le site de support et le Dell TechCenter.

Pour installer OpenManage Enterprise, vous devez avoir des privilèges administrateur local et le système que vous utilisez doit respecter les critères indiqués dans la Configuration matérielle minimale recommandée et la Configuration minimale requise pour l'installation d'OpenManage Enterprise.

Matériel minimal recommandé

Ce tableau décrit les configurations matérielles minimales recommandées pour OpenManage Enterprise.

Tableau 4. Matériel minimal recommandé

Matériel minimal recommandé	Déploiements de grande taille	Déploiements de petite taille
Nombre de périphériques qui peuvent être gérés par l'appliance	Jusqu'à 8 000	1 000
RAM	32 Go	16 Go
Processeurs	8 noyaux au total	4 noyaux au total
Disque dur	400 Go	400 Go

Configuration matérielle minimale requise pour le déploiement d'OpenManage Enterprise

Tableau 5. Configuration minimale requise

Détails	Configuration minimale requise

Hyperviseurs pris en charge	• Version VMware vSphere :
	  ○ vSphere ESXi 5.5 et versions ultérieures
	• Microsoft Hyper-V pris en charge sur :
	  ○ Windows Server 2012 R2 et versions ultérieures
	• KVM pris en charge sur :
	  ○ Red Hat Enterprise Linux 6.5 et versions ultérieures

Réseau	Carte réseau virtuelle NIC disponible avec accès aux réseaux de gestion de tous les périphériques qui est gérée à partir d'OpenManage Enterprise.
Navigateurs pris en charge	• Internet Explorer (64 bits) 11 et supérieur • Mozilla Firefox 52 et versions ultérieures • Google Chrome 58 et supérieur • Microsoft Edge version 41.16299 et ultérieures
Interface utilisateur	HTML 5, basé sur JS

REMARQUE : Pour obtenir la dernière mise à jour concernant la configuration minimale requise pour OpenManage Enterprise, voir *Matrice de prise en charge de Dell EMC OpenManage Enterprise* sur le site de support.

Déploiement d'OpenManage Enterprise sur VMware vSphere

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.

1. Téléchargez le fichier `openmanage_enterprise_ovf_format.zip` à partir du site de support et extrayez le fichier à un emplacement accessible par le client VMware vSphere. Il est recommandé d'utiliser un lecteur local ou un CD/DVD, car l'installation à partir d'un emplacement réseau peut prendre jusqu'à 30 minutes.
2. Dans vSphere Client, sélectionnez **Fichier** > **Déployer le modèle OVF**.
   L'Assistant **Déploiement du modèle OVF** s'affiche.
3. Sur la page **Source**, cliquez sur **Parcourir**, puis sélectionnez le package OVF. Cliquez sur **Suivant**.
4. Dans la page **Détails du modèle OVF**, passez en revue les informations affichées. Cliquez sur **Suivant**.
5. Sur la page **Contrat de licence utilisateur final**, lisez le contrat de licence et cliquez sur **Accepter**. Pour continuer, cliquez sur **Suivant**.
6. Sur la page **Nom et emplacement**, saisissez un nom composé de 80 caractères au maximum, puis sélectionnez un emplacement d'inventaire où le modèle sera stocké. Cliquez sur **Suivant**.
7. Selon la configuration vCenter, l'une des options suivantes s'affiche :
   - **Si des pools de ressources sont configurés** : dans la page **Pool de ressources**, sélectionnez le pool de serveurs virtuels sur lequel vous souhaitez déployer la machine virtuelle de l'appliance.
   - **Si des pools de ressources ne sont PAS configurés** : dans la page **Hôtes/Clusters**, sélectionnez l'hôte ou le cluster sur lequel vous souhaitez déployer la machine virtuelle de l'appliance.
8. Si plusieurs banques de données sont disponibles sur l'hôte, la page **Banque de données** les affiche toutes. Sélectionnez l'emplacement où vous souhaitez stocker les fichiers de machine virtuelle, puis cliquez sur **Suivant**.

9. Sur la page **Format de disque**, cliquez sur **Allocation statique** pour allouer au préalable un espace de stockage physique aux machines virtuelles lors de la création d'un disque.
10. Sur la page **Prêt à terminer**, passez en revue les options que vous avez sélectionnées sur les pages précédentes et cliquez sur **Terminer** pour exécuter la tâche de déploiement.
    Une fenêtre sur l'état d'achèvement vous permettant de suivre la progression de la tâche s'affiche.

Déploiement d'OpenManage Enterprise sur l'hôte Hyper-V 2012 R2 et les versions antérieures

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.
- Après avoir installé ou mis à niveau l'appliance sur Hyper-V, mettez-la hors tension, retirez l'adaptateur réseau standard et ajoutez un adaptateur réseau hérité, puis mettez l'appliance sous tension.

1. Téléchargez le fichier **`openmanage_enterprise_vhd_format.zip`** à partir du site de support. Extrayez le fichier, puis déplacez ou copiez le fichier VHD joint sur le système, à l'emplacement où vous souhaitez stocker l'unité virtuelle OpenManage Enterprise.
2. Démarrez le gestionnaire **Hyper-V** dans Windows Server 2012 R2 ou versions antérieures. Windows Hyper-V devrait s'afficher dans le Gestionnaire Hyper-V. Dans le cas contraire, cliquez avec le bouton droit de la souris sur **Gestionnaire Hyper-V** et sélectionnez **Connexion au serveur**.
3. Cliquez sur **Actions** > **Nouveau** > **Machine virtuelle** pour démarrer l'**Assistant Nouvelle machine virtuelle**.
4. Cliquez sur **Suivant** sur la première page **Avant de commencer**.
5. Sur la **page Spécifier un nom et un emplacement**,
   - renseignez le **nom de la machine virtuelle.**
   - (Facultatif) Cochez la case **Stocker la machine virtuelle à un autre emplacement** pour activer le champ **Emplacement**, puis cliquez sur Parcourir et naviguez pour sélectionner un emplacement de dossier sur lequel stocker la VM.

   REMARQUE : Si la case n'est pas cochée, la machine virtuelle est stockée dans le dossier par défaut.
6. Cliquez sur **Suivant**.
7. Sur la page **Spécifier une génération**, sélectionnez **Génération 1** et cliquez sur **Suivant**.

   REMARQUE : OpenManage Enterprise ne prend pas en charge la génération 2.
8. Sur la page **Affecter la mémoire**, saisissez la mémoire de démarrage dans le champ **Mémoire de démarrage**, puis cliquez sur **Suivant**.

   REMARQUE : Assurez-vous qu'au minimum de 16 000 Mo (16 Go) soient affectés.
9. Sur la page **Configurer la mise en réseau**, sélectionnez l'adaptateur réseau dans la liste déroulante **Connexion**. Vérifiez que le **commutateur virtuel** est connecté au réseau. Cliquez sur **Suivant**.

   REMARQUE : S'il est défini sur « **Non connecté** », OME ne fonctionnera pas correctement lors du premier redémarrage, et exige un redéploiement si cette situation se reproduit.
10. Sur la page **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque virtuel existant**, puis naviguez vers l'emplacement sur lequel le fichier VHD est copié, comme mentionné à l'**étape 1**. Cliquez sur **Suivant**.
11. Suivez les instructions qui s'affichent.

    REMARQUE : Assurez-vous de disposer d'un espace de stockage minimal de 20 Go
12. Ouvrez les **Paramètres** de la nouvelle VM et mettez la machine virtuelle sous tension.
13. Sur l'écran Interface TUI, acceptez le CLUF et lorsque vous y êtes invité, modifiez le mot de passe de l'appliance et définissez les paramètres réseau sur l'IP de l'appliance.

Déploiement d'OpenManage Enterprise sur un hôte Hyper-V 2016

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.
- Après avoir installé ou mis à niveau l'appliance sur Hyper-V, mettez-la hors tension, retirez l'adaptateur réseau standard et ajoutez un adaptateur réseau hérité, puis mettez l'appliance sous tension.

1. Téléchargez le fichier **openmanage_enterprise_vhd_format.zip** à partir du site de support. Extrayez le fichier, puis déplacez ou copiez le fichier VHD joint sur le système, à l'emplacement où vous souhaitez stocker l'unité virtuelle OpenManage Enterprise.
2. Démarrez le **Gestionnaire Hyper-V** dans Windows Server 2016. Windows Hyper-V devrait s'afficher dans le Gestionnaire Hyper-V. Dans le cas contraire, cliquez avec le bouton droit de la souris sur **Gestionnaire Hyper-V** et sélectionnez **Connexion au serveur**.
3. Cliquez sur **Actions** > **Nouveau** > **Machine virtuelle** pour démarrer l'**Assistant Nouvelle machine virtuelle**.
4. Cliquez sur **Suivant** sur la première page **Avant de commencer**.
5. Sur la **page Spécifier un nom et un emplacement**,
   - renseignez le **nom de la machine virtuelle.**
   - (Facultatif) Cochez la case **Stocker la machine virtuelle à un autre emplacement** pour activer le champ **Emplacement**, puis cliquez sur Parcourir et naviguez pour sélectionner un emplacement de dossier sur lequel stocker la VM.

   REMARQUE : Si la case n'est pas cochée, la machine virtuelle est stockée dans le dossier par défaut.
6. Cliquez sur **Suivant**.
7. Sur la page **Spécifier une génération**, sélectionnez **Génération 1** et cliquez sur **Suivant**.

   REMARQUE : OpenManage Enterprise ne prend pas en charge la génération 2.
8. Sur la page **Affecter la mémoire**, saisissez la mémoire de démarrage dans le champ **Mémoire de démarrage**, puis cliquez sur **Suivant**.

   REMARQUE : Assurez-vous qu'au minimum de 16 000 Mo (16 Go) soient affectés.
9. Sur la page **Configurer la mise en réseau**, sélectionnez l'adaptateur réseau dans la liste déroulante **Connexion**. Vérifiez que le **commutateur virtuel** est connecté au réseau. Cliquez sur **Suivant**.

   REMARQUE : S'il est défini sur « **Non connecté** », OME ne fonctionnera pas correctement lors du premier redémarrage, et exige un redéploiement si cette situation se reproduit.
10. Sur la page **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque virtuel existant**, puis naviguez vers l'emplacement sur lequel le fichier VHD est copié, comme mentionné à l'**étape 1**. Cliquez sur **Suivant**.
11. Suivez les instructions qui s'affichent.

    REMARQUE : Assurez-vous de disposer d'un espace de stockage minimal de 20 Go
12. Ouvrez les **Paramètres** de la nouvelle VM et mettez la machine virtuelle sous tension.
13. Sur l'écran Interface TUI, acceptez le CLUF et lorsque vous y êtes invité, modifiez le mot de passe de l'appliance et définissez les paramètres réseau sur l'IP de l'appliance.

Déploiement d'OpenManage Enterprise sur un hôte Hyper-V 2019

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

- Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.
- Après avoir installé ou mis à niveau l'appliance sur Hyper-V, mettez-la hors tension, retirez l'adaptateur réseau standard et ajoutez un adaptateur réseau hérité, puis mettez l'appliance sous tension.

1. Téléchargez le fichier **openmanage_enterprise_vhd_format.zip** à partir du site de support. Extrayez le fichier, puis déplacez ou copiez le fichier VHD joint sur le système, à l'emplacement où vous souhaitez stocker l'unité virtuelle OpenManage Enterprise.
2. Démarrez le **Gestionnaire Hyper-V** dans Windows Server 2019. Windows Hyper-V devrait s'afficher dans le Gestionnaire Hyper-V. Dans le cas contraire, cliquez avec le bouton droit de la souris sur **Gestionnaire Hyper-V** et sélectionnez **Connexion au serveur**.
3. Cliquez sur **Actions** > **Nouveau** > **Machine virtuelle** pour démarrer l'**Assistant Nouvelle machine virtuelle**.
4. Cliquez sur **Suivant** sur la première page **Avant de commencer**.
5. Sur la **page Spécifier un nom et un emplacement**,
   - renseignez le **nom de la machine virtuelle.**
   - (Facultatif) Cochez la case **Stocker la machine virtuelle à un autre emplacement** pour activer le champ **Emplacement**, puis cliquez sur Parcourir et naviguez pour sélectionner un emplacement de dossier sur lequel stocker la VM.

   REMARQUE : Si la case n'est pas cochée, la machine virtuelle est stockée dans le dossier par défaut.
6. Cliquez sur **Suivant**.
7. Sur la page **Spécifier une génération**, sélectionnez **Génération 1** et cliquez sur **Suivant**.

   REMARQUE : OpenManage Enterprise ne prend pas en charge la génération 2.
8. Sur la page **Affecter la mémoire**, saisissez la mémoire de démarrage dans le champ **Mémoire de démarrage**, puis cliquez sur **Suivant**.

   REMARQUE : Assurez-vous qu'au minimum de 16 000 Mo (16 Go) soient affectés.
9. Sur la page **Configurer la mise en réseau**, sélectionnez l'adaptateur réseau dans la liste déroulante **Connexion**. Vérifiez que le **commutateur virtuel** est connecté au réseau. Cliquez sur **Suivant**.

   REMARQUE : S'il est défini sur « **Non connecté** », OME ne fonctionnera pas correctement lors du premier redémarrage, et exige un redéploiement si cette situation se reproduit.
10. Sur la page **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque virtuel existant**, puis naviguez vers l'emplacement sur lequel le fichier VHD est copié, comme mentionné à l'**étape 1**. Cliquez sur **Suivant**.
11. Suivez les instructions qui s'affichent.

    REMARQUE : Assurez-vous de disposer d'un espace de stockage minimal de 20 Go
12. Ouvrez les **Paramètres** de la nouvelle VM et mettez la machine virtuelle sous tension.
13. Sur l'écran Interface TUI, acceptez le CLUF et lorsque vous y êtes invité, modifiez le mot de passe de l'appliance et définissez les paramètres réseau sur l'IP de l'appliance.

Déploiement d'OpenManage Enterprise en utilisant une machine virtuelle basée sur le noyau

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.

1. Installez les packages de virtualisation requis lors de l'installation du système d'exploitation.
2. Téléchargez le fichier `openmanage_enterprise_kvm_format.zip` sur le site de support. Extrayez le fichier sur votre système, à l'emplacement où vous voulez stocker l'unité virtuelle OpenManage Enterprise.
3. Démarrez le gestionnaire virtuel, puis sélectionnez **Fichier** > **Propriétés**.
4. Sur la page **Interfaces réseau**, cliquez sur **Ajouter**.
5. Sélectionnez le type d'interface **Pont**, puis cliquez sur **Suivant**.

6. Définissez le mode de démarrage sur **onboot** et cochez la case **Activer maintenant**.
7. Sélectionnez l'interface sur laquelle établir un pont dans la liste et vérifiez que les propriétés correspondent à celles du périphérique hôte, puis cliquez sur **Terminer**.
   Une interface virtuelle est maintenant créée et vous pouvez configurer les paramètres du pare-feu à l'aide du terminal.
8. Dans le Virtual Machine Manager, cliquez sur **Fichier** > **Nouveau**.
9. Entrez un nom pour la VM et sélectionnez l'option **Importer l'image disque existante**, puis cliquez sur **Suivant**.
10. Naviguez dans le système de fichiers et sélectionnez le fichier QCOW2 téléchargé à l'étape 1, puis cliquez sur **Suivant**.
11. Affectez 16 Go à la mémoire et sélectionnez deux cœurs de processeur, puis cliquez sur **Suivant**.
12. Attribuez l'espace disque requis pour la VM et cliquez sur **Suivant**.
13. Sous **Options avancées**, assurez-vous que le réseau de périphériques hôtes ponté est sélectionné et que KVM est bien le Type de machine virtuelle sélectionné.
14. Cliquez sur **Terminer**.
    L'appliance OpenManage Enterprise est maintenant déployée en utilisant le KVM. Pour commencer à utiliser OpenManage Enterprise, reportez-vous à Connexion à OpenManage Enterprise , page 27.

Déploiement d'OpenManage Enterprise par programmation

OpenManage Enterprise peut être déployé par programmation (à l'aide d'un script) sur VMware ESXi version 6.5 ou version ultérieure.

REMARQUE : Le déploiement par programmation/script n'est pris en charge qu'à l'aide de l'interface principale.

REMARQUE : Si vous avez ajouté un adaptateur secondaire avant de mettre l'appliance sous tension pour la première fois, l'adaptateur est configuré avec IPv4 et IPv6 désactivés. Lors de la connexion à l'interface TUI, et après avoir accepté le CLUF et modifié le mot de passe admin, l'adaptateur s'affiche comme étant **DÉSACTIVÉ** et doit être configuré par l'utilisateur.

REMARQUE : Vous devez utiliser les dernières versions d'OVF Tool et Python 3.0 ou ultérieures pour pouvoir programmer le déploiement.

Pour déployer OpenManage Enterprise par programmation, procédez comme suit :

1. Téléchargez et extrayez le fichier `openmanage_enterprise_ovf_format.zip` ou téléchargez individuellement les fichiers OVF suivants à partir du site de support :
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`
   - `openmanage_enterprise.x86_64-0.0.1.ovf`
   - `openmanage_enterprise.x86_64-0.0.1.vmx`
   - `ovf_properties.config`
   - `update_ovf_property.py`
2. Ouvrez le fichier `ovf_properties.config` et définissez les paramètres suivants :

Tableau 6. Paramètres utilisés dans `ovf_properties.config`

Paramètre	Valeurs acceptées	Description
bEULATxt	true ou false	En définissant la valeur de ce paramètre sur Vrai, vous indiquez accepter les conditions générales du Contrat de licence utilisateur final (CLUF). Le CLUF se trouve au bas du fichier ovf_properties.config.
adminPassword	Ce mot de passe doit contenir au moins un caractère pour chacune des catégories suivantes : majuscule, minuscule, chiffre et caractère spécial. Par exemple, Dell123$	Saisissez un nouveau mot de passe d'administrateur pour OpenManage Enterprise.
bEnableDHCP	true ou false	Définissez la valeur de ce paramètre sur Vrai si vous souhaitez que l'appliance active

Tableau 6. Paramètres utilisés dans `ovf_properties.config` (suite)

Paramètre	Valeurs acceptées	Description
		le protocole DHCP IPv4 et ignore les adresses IPv4 statiques.
bEnableIpv6AutoConfig	true ou false	Définissez la valeur de ce paramètre sur Vrai si vous voulez que l'appliance active la configuration IPv6 automatique et ignore les adresses IPv6 statiques.
staticIP	adresse IP statique au format CIDR	Il peut s'agir d'une adresse IPv4 ou IPv6. (Vous ne pouvez pas définir les types IPv4 et IPv6 simultanément.)
gateway	IPv4 ou IPv6	Vous ne pouvez pas définir la passerelle statique simultanément sur les types IPv4 et IPv6.

3. Exécutez le script `update_ovf_property.py`.

   Ce script modifie le fichier `openmanage_enterprise.x86_64-0.0.1.ovf` pour le déploiement conformément aux valeurs définies dans fichier ovf_properties.config. Lorsque le script termine l'exécution, un échantillon de commande ovftool s'affiche. Elle contient des variables, telles que `<DATASTORE>, <user>, <password>, <IP address>`, ainsi de suite, que vous devez remplacer, en fonction de votre environnement de déploiement. Ces paramètres définissent les ressources utilisées sur le système ESXi cible, ainsi que les informations d'identification et l'adresse IP du système cible.

   REMARQUE : N'oubliez pas de remplacer l'intégralité, notamment les symboles < et >.

4. Exécutez la commande ovftool modifiée à l'étape précédente.

   REMARQUE : La commande ovftool doit s'exécuter avec les balises --X:injectOvfEnv et --powerOn, car celles-ci sont requises pour programmer le déploiement.

   Une fois la commande ovftool est exécutée, le manifeste valide et le déploiement débute.

4

Prise en main d'OpenManage Enterprise

Sujets :

Connexion à OpenManage Enterprise

Lorsque vous démarrez le système pour la première fois depuis l'interface texte utilisateur, vous êtes invité à accepter le contrat EULA, puis à modifier le mot de passe d'administrateur. Si vous vous connectez à OpenManage Enterprise pour la première fois, vous devez définir les informations d'identification d'utilisateur via l'interface texte utilisateur. Voir Configuration d'OpenManage Enterprise en utilisant l'interface texte utilisateur , page 27.

PRÉCAUTION : Si vous oubliez le mot de passe administrateur, il ne peut pas être récupéré à partir de l'appliance OpenManage Enterprise.

1. Démarrez le navigateur pris en charge.
2. Dans le champ **Adresse**, saisissez l'adresse IP de l'appliance OpenManage Enterprise.

   Sur la page de connexion, le logo OpenManage Enterprise et un avis de sécurité indiquant « En accédant à l'ordinateur, vous confirmez que cet accès est conforme à la politique de sécurité de votre organisation » s'affichent. L'avis de sécurité peut être personnalisé par les administrateurs à l'aide de l'API. Pour plus d'informations, voir le guide de l'API OpenManage Enterprise.
3. Saisissez les informations d'identification de l'utilisateur, puis cliquez sur **Connexion**.

   REMARQUE : Le nom d'utilisateur par défaut est `admin`.

Si vous vous connectez pour la première fois à OpenManage Enterprise, la page **Bienvenue dans OpenManage Enterprise** s'affiche. Cliquez sur **Paramètres initiaux** et effectuez la configuration de base. Voir la section Configuration d'OpenManage Enterprise , page 31. Pour détecter les périphériques, cliquez sur **Détecter des périphériques**.

REMARQUE : Par défaut, après trois échecs de tentatives de connexion, votre compte OpenManage Enterprise est verrouillé et vous ne pouvez pas vous connecter avant la fin de la durée de verrouillage du compte. La durée de verrouillage du compte est de 900 secondes par défaut. Pour modifier cette durée, reportez-vous à Définition des propriétés de sécurité de connexion , page 165.

Configuration d'OpenManage Enterprise en utilisant l'interface texte utilisateur

L'outil Interface texte utilisateur (TUI) permet de modifier le mot de passe administrateur, d'afficher l'état de l'appliance et la configuration du réseau, de configurer les paramètres de gestion de réseau, d'activer une demande de débogage sur le terrain, de sélectionner le réseau principal et de configurer l'appliance pour la détection automatique des serveurs de votre réseau.

Lorsque vous amorcez le système pour la première fois à partir de l'interface TUI, vous êtes invité à accepter le contrat de licence utilisateur final (CLUF). Ensuite, modifiez le mot de passe d'administrateur, configurez les paramètres de réseau de l'appliance et chargez la console Web dans un navigateur pris en charge pour la mise en route. Seuls les utilisateurs disposant des privilèges d'administrateur d'OpenManage peuvent configurer OpenManage Enterprise.

Sur l'interface TUI, utilisez les flèches ou appuyez sur la touche **Tab** pour passer à l'option suivante dans l'interface TUI ou sur les touches **Maj + Tab** pour revenir aux options précédentes. Appuyez sur **Entrée** pour sélectionner une option. La barre **Espace** coche ou décoche une case.

REMARQUE :

- Pour configurer IPv6, assurez-vous que celui-ci est déjà configuré par un serveur vCenter.
- Par défaut, la dernière adresse IP découverte d'un périphérique est utilisée par OpenManage Enterprise pour effectuer toutes les opérations. Pour que tout changement d'adresse IP soit effectif, vous devez redécouvrir le périphérique.

Vous pouvez configurer OpenManage Enterprise via l'interface TUI. L'écran de l'interface TUI propose les options suivantes :

Tableau 7. Options de l'Interface texte utilisateur

Options	Descriptions
Modifier le mot de passe admin	Sélectionnez l'écran **Modifier le mot de passe administrateur** pour saisir un nouveau mot de passe, puis confirmez-le. Vous devez modifier le mot de passe dans l'interface TUI lors de votre première connexion.
Afficher l'état actuel de l'appliance	Sélectionnez **Afficher l'état actuel de l'appliance** pour afficher l'URL et l'état de l'appliance. Vous pouvez également afficher l'état des services Exécution des tâches, Traitement des événements, Tomcat, Base de données et Surveillance.
Afficher la configuration réseau actuelle	Sélectionnez **Afficher la configuration réseau actuelle** pour afficher les détails de la configuration IP. Le menu **Choisir un adaptateur réseau** répertorie tous les adaptateurs réseau disponibles. Cliquez sur un adaptateur réseau pour afficher les paramètres actifs de cette dernière.
Définir le nom d'hôte de l'appliance	Sélectionnez **Définir le nom d'hôte de l'appliance** pour configurer le nom d'hôte de l'appliance sur le DNS. Ce champ accepte les caractères suivants pour les noms d'hôte : caractères alphanumériques (a-z, A-Z, 0-9), points (.) et tirets (-). **REMARQUE :** L'utilisation de points désigne les informations relatives au nom de domaine. Si les informations DNS de l'appliance sont configurées de manière statique plutôt que d'obtenir les détails du domaine par DHCP, vous devez configurer le nom d'hôte en utilisant le nom de domaine complet (FQDN) afin que les informations de recherche de domaine puissent être renseignées.
Définir les paramètres de mise en réseau	Sélectionnez **Définir les paramètres de mise en réseau** pour reconfigurer les adaptateurs réseau. Le menu **Choisir un adaptateur réseau** répertorie tous les adaptateurs réseau disponibles. Sélectionnez un adaptateur réseau, reconfigurez ses paramètres réseau, puis sélectionnez **Appliquer** pour enregistrer les modifications apportées à l'interface appropriée. Par défaut, seul IPv4 est activé sur l'interface réseau principale avec une adresse IP statique factice dans l'appliance. Toutefois, si une nouvelle interface réseau est ajoutée, IPv4 et IPv6 sont activés pour la multiconnexion. Si l'appliance OpenManage Enterprise ne parvient pas à acquérir une adresse IPv6, vérifiez que l'environnement est configuré de telle sorte que le bit géré (M) soit activé pour les annonces de routeur. Le gestionnaire de réseau des distributions Linux actuelles entraîne une perte de liaison lorsque ce bit est activé, mais que DHCPv6 n'est pas disponible. Assurez-vous que DHCPv6 est activé sur le réseau ou désactivez la balise de gestion pour les annonces de routeur. **REMARQUE :** • La configuration de DNS n'est disponible que sur l'interface réseau principale. Si vous souhaitez que la résolution DNS

Tableau 7. Options de l'Interface texte utilisateur (suite)

Options	Descriptions
	soit configurée pour cette interface, tous les noms de l'hôte doivent être résolus par le serveur DNS configuré sur l'interface principale.
Sélectionner l'interface réseau principale	L'option **Sélectionner l'interface réseau principale** vous permet de désigner un réseau principal. Sélectionner l'interface principale donne la priorité à l'interface sélectionnée en termes de routage et elle est utilisée comme route par défaut. Cette interface a la priorité de routage en cas d'ambiguïté. L'interface principale est également censée être l'interface « publique », qui permet la connectivité réseau/Internet de l'entreprise. Des règles de pare-feu différentes sont appliquées à l'interface principale, ce qui permet un contrôle d'accès plus strict tel que la restriction d'accès par plage d'adresses IP. **REMARQUE :** Si la multiconnexion est activée, vous pouvez accéder à l'appliance à partir de deux réseaux. Dans ce cas, l'interface principale est utilisée par l'appliance pour toutes les communications externes et lorsque les paramètres de proxy sont utilisés. Pour plus d'informations sur la multiconnexion sur OpenManage, voir le livre blanc technique *Exécution de script à distance avec Dell EMC OpenManage Enterprise* sur le site de support.
Configurer les routes statiques	Sélectionnez **Configurer les routes statiques** si les réseaux nécessitent la configuration d'une route statique pour atteindre un sous-réseau spécifique sur les réseaux IPv4 et IPv6. **REMARQUE :** Une interface peut prendre en charge jusqu'à 20 routes statiques.
Configurer la détection initiée par serveur	Sélectionnez **Configurer la détection initiée par serveur** pour permettre à l'appliance d'enregistrer automatiquement les enregistrements requis auprès du serveur DNS configuré. **REMARQUE :** • Assurez-vous que l'appliance est enregistrée auprès du DNS et qu'elle peut mettre à jour de manière dynamique les enregistrements. • Vous devez configurer les systèmes cibles pour demander les détails de l'enregistrement auprès du DNS. • Pour modifier le nom de domaine DNS, vérifiez que l'enregistrement DNS dynamique est activé sur le serveur DNS. En outre, pour que l'appliance soit enregistrée sur le serveur DNS, sélectionnez l'option **Non sécurisé et sécurisé** sous Mises à jour dynamiques.
Configurer la taille de disque de l'appliance	Sélectionnez **Configurer la taille de disque de l'appliance** pour rechercher l'espace disque disponible ou un ou plusieurs nouveaux disques, puis affectez l'espace disque supplémentaire ou le ou les nouveaux disques à l'appliance, le cas échéant. **REMARQUE :** • Il est vivement recommandé de réaliser un snapshot de la machine virtuelle de la console en tant que sauvegarde avant d'appliquer toute modification de configuration au disque. • Après l'ajout de l'espace disque, la suppression ou la réduction de l'espace disque étendu n'est pas prise en charge. Pour supprimer un disque nouvellement ajouté

Tableau 7. Options de l'Interface texte utilisateur (suite)

Options	Descriptions
	ou pour inverser l'augmentation de la taille d'un disque existant, vous devez revenir au snapshot de VM précédent. • Si la recherche initiale ne détecte aucun espace non affecté, affectez de l'espace disque supplémentaire ou des disques à la console sur votre hyperviseur et relancez la recherche. • La recherche et l'affectation d'espace disque sont limitées à quatre disques au maximum.
Activer le mode FSD (Field Service Debug, débogage sur le terrain)	Sélectionnez **Activer le mode Field Service Debug (FSD)** pour le débogage de la console. Pour plus d'informations, voir Flux de débogage sur le terrain , page 182.
Services de redémarrage	Sélectionnez **Redémarrer les services** avec les options suivantes pour redémarrer les services et la gestion de réseau : • **Redémarrer tous les services** • **Redémarrer la gestion de réseau**

Configurer l'enregistrement de débogage	Sélectionnez **Configurer l'enregistrement de débogage** à l'aide des options suivantes :
	• **Activer tous les journaux de débogage**
	  ○ Permet de collecter les journaux de débogage de toutes les tâches de surveillance des applications, des événements, de l'historique d'exécution des tâches et des plug-ins installés.
	• **Désactiver tous les journaux de débogage**
	  ○ Permet de désactiver tous les journaux de débogage.
	• **Configurer la journalisation de débogage**
	  ○ Pour activer l'enregistrement de débogage de manière sélective pour les services d'appliance et de plug-in.
	  ○ Utilisez le menu **Options** pour sélectionner tous les services, effacer toutes les sélections ou restaurer l'état avant d'apporter des modifications.
	• **Activer la conservation SCP** : pour collecter les fichiers .XML du modèle.
	• **Désactiver la conservation SCP** : pour désactiver la conservation SCP.
	Vous pouvez télécharger les journaux de débogage en cliquant sur **Surveiller** > **Journaux d'audit** > **Exporter** > **Exporter les journaux de la console** dans OpenManage Enterprise.

Modifier la disposition du clavier	Sélectionnez **Modifier la disposition du clavier** pour modifier la disposition du clavier si nécessaire.
Redémarrer l'appliance	Sélectionnez **Redémarrer l'appliance** pour redémarrer l'appliance. **REMARQUE :** Après l'exécution d'une commande de redémarrage des services, il est possible que l'interface utilisateur affiche le message suivant : `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` Ce problème de blocage se produit probablement parce que l'hyperviseur est surchargé. Dans de telles situations, il est recommandé d'avoir au moins 16 Go de RAM et un CPU de 8 000 MHz réservé à l'appliance OpenManage Enterprise. Il est également recommandé de redémarrer l'appliance OpenManage Enterprise lorsque ce message s'affiche.

Configuration d'OpenManage Enterprise

Lors de votre première connexion à OpenManage Enterprise, la page **Bienvenue sur OpenManage Enterprise** s'affiche, ce qui permet le réglage de l'heure (manuellement ou à l'aide de la synchronisation de l'heure du serveur NTP), ainsi que les configurations de proxy.

1. Pour configurer l'heure manuellement effectuer les opérations ci-dessous dans la section **Configuration de l'heure** :
   - Utilisez le menu déroulant **Fuseau horaire** pour sélectionner le fuseau horaire approprié.
   - Dans la case **Date**, saisissez ou sélectionnez une date.
   - Dans la case **Heure**, renseignez l'heure.
   - Cliquez sur **Appliquer** pour enregistrer les paramètres.
2. Si vous souhaitez utiliser le serveur NTP pour synchroniser l'heure, procédez comme suit dans la section **Configuration de l'heure** :

   REMARQUE : Lorsque les paramètres du serveur NTP sont mis à jour, les utilisateurs connectés sont automatiquement déconnectés de leurs sessions OpenManage Enterprise.

   - Cochez la case **Utiliser NTP**.
   - Saisissez l'adresse IP ou le nom d'hôte dans **Adresse du serveur NTP principal** et **Adresse du serveur NTP secondaire** (facultatif) pour synchroniser l'heure.
3. Si vous souhaitez définir le serveur proxy pour la communication externe, procédez comme suit dans la section Configuration du proxy :
   - Cochez la case **Activer les paramètres de proxy HTTP**.
   - Saisissez l'**Adresse du proxy**.
   - Saisissez le **Numéro de port** du serveur proxy.
   - Si le serveur proxy nécessite des informations d'identification pour ouvrir une session, cochez la case **Activer l'authentification du proxy**, puis saisissez le nom d'utilisateur et le mot de passe.
   - Cochez la case **Ignorer la validation de certificat** si le proxy configuré intercepte le trafic SSL et n'utilise pas de certificat tiers de confiance. Cette option permet d'ignorer les vérifications de certificat intégrées utilisées pour la garantie et la synchronisation de catalogue.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

REMARQUE : Pour plus d'informations sur les navigateurs pris en charge, voir la *Matrice de prise en charge d'OpenManage Enterprise* disponible sur le site de support.

Paramètres recommandés de performance et d'évolutivité pour une utilisation optimale d'OpenManage Enterprise

Le tableau suivant répertorie les paramètres de performance des fonctionnalités prises en charge dans OpenManage Enterprise. Afin d'assurer une performance optimale d'OpenManage Enterprise, Dell EMC vous recommande d'exécuter les tâches selon la fréquence indiquée sur le nombre maximum de périphériques qui sont recommandés par tâche.

Tableau 8. Éléments à prendre en compte en matière d'évolutivité et de performance d'OpenManage Enterprise

Tâches	Fréquence recommandée pour l'exécution des tâches	Tâches si prédéfinies ?	Nombre maximum d'appareils qui sont recommandés par tâche.
Découverte	Une fois par jour pour un environnement affecté par de fréquentes modifications réseau.	Non	10 000/tâche
Inventaire	OpenManage Enterprise fournit une tâche prédéfinie qui actualise automatiquement l'inventaire une fois par jour.	Oui Vous pouvez désactiver cette fonctionnalité.	Les périphériques qui sont surveillés par OpenManage Enterprise
La garantie	OpenManage Enterprise fournit une tâche prédéfinie qui	Oui Vous pouvez désactiver cette fonctionnalité.	Les périphériques qui sont surveillés par OpenManage Enterprise

Tableau 8. Éléments à prendre en compte en matière d'évolutivité et de performance d'OpenManage Enterprise (suite)

Tâches	Fréquence recommandée pour l'exécution des tâches	Tâches si prédéfinies ?	Nombre maximum d'appareils qui sont recommandés par tâche.
	actualise automatiquement la garantie une fois par jour.		
Interrogation de l'intégrité	Toutes les heures	Oui Vous pouvez modifier la fréquence.	Sans objet
Mise à jour du firmware/pilote	Besoin de base		150/tâche
Inventaire de la configuration	Besoin de base		1500/ligne de base

Protocoles et ports pris en charge dans OpenManage Enterprise

Protocoles et ports pris en charge sur les postes de gestion

Tableau 9. Protocoles et ports pris en charge par OpenManage Enterprise sur les postes de gestion

Numéro de port	Protocole	Type de port	Niveau de chiffrement maximum	Source	Direction	Destination	Utilisation
22	SSH	TCP	256 bits	Station de gestion	Entrant	Appliance OpenManage Enterprise	• Exigé pour les communications entrantes uniquement en cas d'utilisation de FSD. L'administrateur OpenManage Enterprise doit l'activer uniquement en cas d'interaction avec le personnel de support Dell EMC.
25	SMTP	TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Station de gestion	• Pour recevoir des alertes par e-mail provenant d'OpenManage Enterprise.
53	DNS	UDP/TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Station de gestion	• Pour les requêtes DNS.
68 / 546 (IPv6)	DHCP	UDP/TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Station de gestion	• Configuration réseau.
80*	HTTP	TCP	Aucun	Station de gestion	Entrant	Appliance OpenManage Enterprise	• Page de destination de l'interface utilisateur graphique (GUI) Web. Permet de rediriger un utilisateur vers HTTPS (port 443).

Tableau 9. Protocoles et ports pris en charge par OpenManage Enterprise sur les postes de gestion (suite)

Numéro de port	Protocole	Type de port	Niveau de chiffrement maximum	Source	Direction	Destination	Utilisation
123	NTP	TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Serveur NTP	• Synchronisation de l'heure (si l'option est activée).
137, 138, 139, 445	CIFS	UDP/TCP	Aucun	iDRAC/CMC	Entrant	Appliance OpenManage Enterprise	• Pour charger ou télécharger les modèles de déploiement. • Pour charger les logs TSR et de diagnostic. • Pour télécharger les fichiers DUP de firmware/pilote et le processus FSD. • Amorcer sur l'image ISO du réseau.
				Appliance OpenManage Enterprise	Sortant	Partage CIFS	• Pour importer les catalogues de firmwares/pilotes depuis le partage CIFS.
111, 2049 (par défaut)	NFS	UDP/TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Partage NFS externe	• Pour télécharger le catalogue et les DUP à partir du partage NFS pour les mises à jour du firmware. • Pour une mise à niveau manuelle de la console à partir d'un partage réseau.
162*	SNMP	UDP	Aucun	Station de gestion	Entrée/Sortie	Appliance OpenManage Enterprise	• Réception des événements au moyen du protocole SNMP. Le sens est « sortant » uniquement en cas d'utilisation de la stratégie de transfert d'interruption.
443 (valeur par défaut)	HTTPS	TCP	SSL 128 bits	Station de gestion	Entrée/Sortie	Appliance OpenManage Enterprise	• GUI Web. • Pour télécharger les mises à jour et les informations de garantie sur Dell.com. Le chiffrement 256 bits est autorisé lors de la communication avec OpenManage Enterprise via le protocole HTTPS

Tableau 9. Protocoles et ports pris en charge par OpenManage Enterprise sur les postes de gestion (suite)

Numéro de port	Protocole	Type de port	Niveau de chiffrement maximum	Source	Direction	Destination	Utilisation
							pour l'interface utilisateur graphique (GUI) Web. • Détection initiée par serveur.
514	Syslog	TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Serveur Syslog	• Pour envoyer une alerte et des informations sur le journal d'audit au serveur Syslog.
3 269	LDAPS	TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Station de gestion	• Connexion AD/ LDAP pour le catalogue global.
636	LDAPS	TCP	Aucun	Appliance OpenManage Enterprise	Sortant	Station de gestion	• Connexion AD/ LDAP pour le contrôleur de domaine.

*Vous pouvez configurer jusqu'à 499 ports à l'exclusion des numéros de port qui sont déjà alloués.

Protocoles et ports pris en charge sur les nœuds gérés

Tableau 10. Protocoles et ports pris en charge par OpenManage Enterprise sur les nœuds gérés

Numéro de port	Protocole	Type de port	Niveau de chiffrement maximum	Source	Direction	Destination	Utilisation
22	SSH	TCP	256 bits	Appliance OpenManage Enterprise	Sortant	Nœud géré	• Pour la détection effectuée à l'aide d'un système d'exploitation Linux, Windows et Hyper-V.
161	SNMP	UDP	Aucun	Appliance OpenManage Enterprise	Sortant	Nœud géré	• Pour les requêtes SNMP.
162*	SNMP	UDP	Aucun	Appliance OpenManage Enterprise	Entrée/ Sortie	Nœud géré	• Envoi et réception d'interruptions SNMP.
443	Propriétaire/ WS-Man/ Redfish	TCP	256 bits	Appliance OpenManage Enterprise	Sortant	Nœud géré	• Découverte et inventaire d'iDRAC7 et versions supérieures. • Pour la gestion du CMC.
623	IPMI/ RMCP	UDP	Aucun	Appliance OpenManage Enterprise	Sortant	Nœud géré	• Accès IPMI au moyen du réseau local
69	TFTP	UDP	Aucun	CMC	Entrant	Station de gestion	• Pour la mise à jour du firmware CMC.

* Vous pouvez configurer jusqu'à 499 ports à l'exclusion des numéros de port qui sont déjà alloués.

REMARQUE : Dans un environnement IPv6, vous devez activer IPv6 et désactiver IPv4 dans l'appliance OpenManage Enterprise pour vous assurer que toutes les fonctionnalités fonctionnent comme prévu.

Liens vers des cas d'utilisation pour les protocoles et ports pris en charge dans OpenManage Enterprise

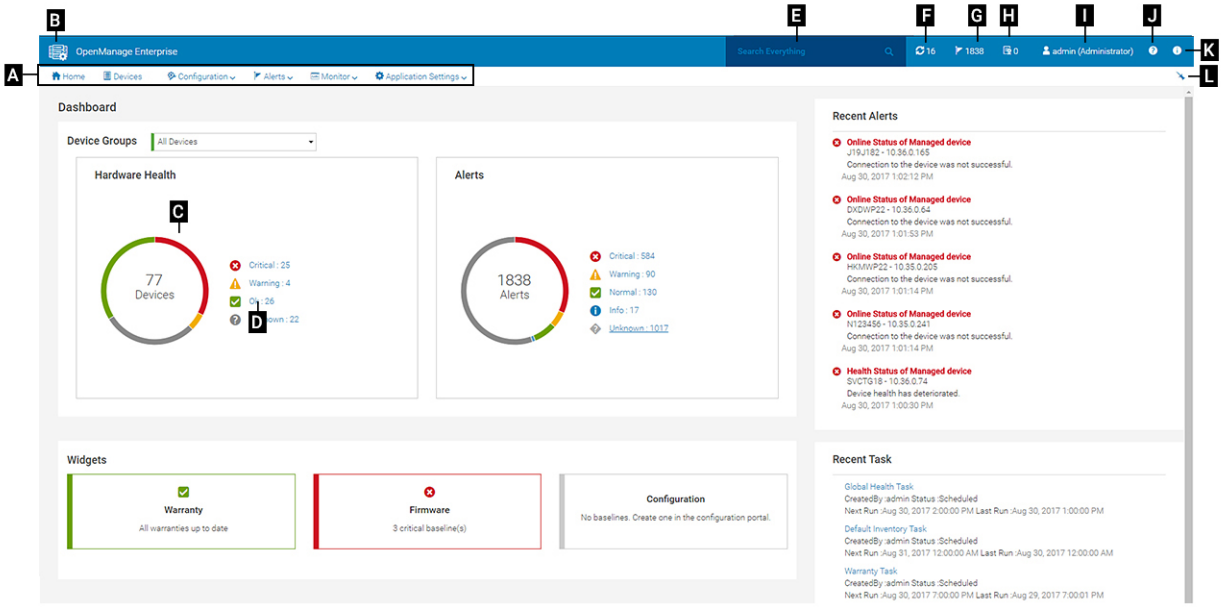
Tableau 11. Liens vers des cas d'utilisation pour les protocoles et ports pris en charge dans OpenManage Enterprise

Cas d'utilisation	URL
Mise à niveau de l'appliance OpenManage Enterprise	https://downloads.dell.com/openmanage_enterprise/
Accès à la garantie des appareils	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements
Mise à jour des catalogues	https://downloads.dell.com/catalog/
Envoi de notifications de nouvelle alerte à l'aide de l'application OpenManage Mobile	https://openmanagecloud.dell.com

5

Présentation de l'interface graphique d'OpenManage Enterprise–Tech Release

Dans l'interface graphique d'OpenManage Enterprise, vous pouvez utiliser des éléments de menu, des liens, des boutons, des volets, des boîtes de dialogue, des listes, des onglets, des cases de filtres et des pages pour naviguer entre des pages et effectuer des tâches de gestion des périphériques. Les fonctionnalités telles que la liste des périphériques, les graphiques circulaires, les journaux d'audit, les paramètres OpenManage Enterprise, les alertes système, ainsi que la mise à jour du firmware/pilote s'affichent à plusieurs endroits. Il est recommandé de vous familiariser avec les éléments de l'interface graphique utilisateur pour utiliser facilement et efficacement OpenManage Enterprise pour la gestion de vos périphériques de datacenter.



- A— Le menu **OpenManage Enterprise** sur toutes les pages d'OpenManage Enterprise fournit des liens vers des fonctionnalités qui permettent aux administrateurs d'afficher le tableau de bord (**Accueil**), de gérer des périphériques (**Périphériques**), de gérer les lignes de base, les modèles et les lignes de base de conformité de configuration du firmware/pilote (**Configuration**), de créer et de stocker des alertes (**Alertes**), puis d'exécuter des tâches, de détecter et collecter des données d'inventaire et de générer des rapports (**Surveiller**). Vous pouvez également personnaliser diverses propriétés de votre application OpenManage Enterprise (**Paramètres d'application**). Cliquez sur le symbole en forme d'épingle dans le coin supérieur droit pour épingler les éléments du menu afin qu'ils s'affichent sur toutes les pages OpenManage Enterprise. Pour supprimer le marquage, cliquez à nouveau sur le symbole en forme d'épingle.
- B—Le symbole du tableau de bord. Cliquez pour ouvrir la page du tableau de bord à partir de n'importe quelle page d'OpenManage Enterprise. Sinon, cliquez sur **Accueil**. Voir le Tableau de bord.
- C—Le graphique circulaire fournit un snapshot de l'état d'intégrité de tous les périphériques surveillés par OpenManage Enterprise. Vous permet d'agir rapidement sur les périphériques qui sont dans un état critique. Chaque couleur du graphique représente un groupe de périphériques ayant un état d'intégrité particulier. Cliquez sur les bandes de couleur pour afficher les périphériques respectifs dans la liste des périphériques. Cliquez sur le nom ou l'adresse IP du périphérique pour afficher la page de propriétés de périphérique. Voir la section Affichage et configuration des périphériques individuels , page 68.
- D—Symboles utilisés pour indiquer l'état d'intégrité des périphériques. Voir la section États d'intégrité du périphérique , page 40.
- E—Dans la case **Rechercher tout**, saisissez tous les éléments surveillés et affichés par OpenManage Enterprise pour consulter les résultats, comme l'adresse IP du périphérique, le nom de la tâche, le nom du groupe, la ligne de base du firmware/pilote et les données de garantie sur tous les périphériques dans votre périmètre, comme défini par le contrôle d'accès basé sur le périmètre (SBAC). Vous ne pouvez pas trier ou exporter les données récupérées à l'aide de la fonctionnalité Rechercher Tout. Sur les pages individuelles ou les boîtes de dialogue, saisissez du texte ou effectuez une sélection depuis la section **Filtres avancés** pour affiner vos résultats de recherche.

- **Les opérateurs suivants ne sont pas pris en charge : +, - et ".**

- F—Nombre de tâches OpenManage Enterprise actuellement dans la file d'attente. Tâches liées à la détection, l'inventaire, la garantie, la mise à jour du firmware et/ou pilote, etc. Cliquez pour afficher l'état des tâches qui s'exécutent sous les catégories Intégrité, Inventaire et Rapport sur la page Détails du travail. Pour afficher tous les événements, cliquez sur **Toutes les tâches**. Voir la section Utilisation des tâches pour le contrôle de périphériques , page 129. Cliquez pour rafraîchir.
- G—Nombre d'événements générés dans le journal d'alertes. En outre, en fonction de vos paramètres d'affichage ou non des alertes qui n'ont pas été acquittées, le nombre d'alertes présentes dans cette section varie. Par défaut, seules les alertes qui n'ont pas été acquittées s'affichent. Pour masquer ou afficher les alertes acquittées, consultez Personnalisation de l'affichage des alertes , page 166. Ce nombre diminue si des alertes sont supprimées. Pour en savoir plus sur les symboles utilisés pour les états de gravité, voir la section États d'intégrité du périphérique , page 40. Cliquez sur un symbole de niveau de gravité pour afficher tous les événements survenus dans cette catégorie de gravité sur la page d'alertes. Pour afficher tous les événements, cliquez sur **Tous les événements**. Voir Gestion des alertes des périphériques.
- H—Nombre total de garanties d'appareil dont l'état est Critique (expirée) et Avertissement (expirant bientôt). Voir Gestion de la garantie des périphériques.
- I—Nom d'utilisateur actuellement connecté. Positionnez le pointeur sur le nom d'utilisateur pour afficher les rôles qui lui sont attribués. Pour plus d'informations sur les utilisateurs basés sur des rôles, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16. Cliquez pour vous déconnecter, puis connectez-vous à nouveau avec un autre nom d'utilisateur.
- J—Actuellement, le fichier d'aide contextuelle s'affiche uniquement pour la page sur laquelle vous vous trouvez et pas sur les pages du portail d'accueil. Cliquez pour afficher des instructions basées sur les tâches afin d'utiliser efficacement les liens, boutons, boîtes de dialogue, assistants et pages dans OpenManage Enterprise.
- K—Cliquez sur ce lien pour afficher la version actuelle d'OpenManage Enterprise installée sur le système. Cliquez sur **Licences** pour lire le message. Cliquez sur les liens appropriés pour afficher et télécharger les fichiers open source liés à OpenManage Enterprise ou d'autres licences open source.
- L—Cliquez sur le symbole pour épingler ou détacher les éléments du menu. Lorsqu'ils sont détachés, pour épingler les éléments du menu, développez le menu **OpenManage Enterprise**, puis cliquez sur le symbole en forme d'épingle.

Les données concernant les éléments répertoriés dans un tableau peuvent être affichées dans le détail et exportées en totalité ou en fonction des éléments sélectionnés. Voir Exportation de toutes les données ou des données sélectionnées , page 68. Un texte bleu indique que des informations approfondies sur les éléments d'un tableau peuvent être affichées et mises à jour, dans la même fenêtre ou sur une page séparée. Les données tabulées peuvent être filtrées en utilisant la fonction **Filtres avancés**. Les filtres varient en fonction du contenu que vous affichez. Saisissez ou sélectionnez les données dans les champs. Les textes incomplets ou les chiffres n'affichent pas le résultat attendu. Les données correspondant aux critères du filtre s'affichent dans la liste. Pour supprimer les filtres, cliquez sur **Effacer tous les filtres**.

Pour trier les données dans un tableau, cliquez sur l'en-tête de colonne. Vous ne pouvez pas trier ou exporter les données récupérées à l'aide de la fonctionnalité Rechercher Tout.

Des symboles sont utilisés pour identifier les principaux éléments, le tableau de bord, l'état d'intégrité des périphériques, la catégorie d'alerte, l'état de conformité du firmware et du pilote, l'état de connexion, l'état d'alimentation, etc. Cliquez sur les boutons suivant et précédent du navigateur pour naviguer entre les pages d'OpenManage Enterprise. Pour plus d'informations sur les navigateurs pris en charge, voir le document *Matrice de support de Dell EMC OpenManage Enterprise* disponible sur le site de support.

Lorsque cela est pertinent, la page est divisée en volets (de gauche, actif et de droite) pour simplifier la tâche de gestion des périphériques. Au besoin, des instructions en ligne et des info-bulles s'affichent lorsque le pointeur est maintenu sur un élément de l'interface graphique utilisateur.

Des aperçus d'un périphérique, d'une tâche, d'un inventaire, d'une ligne de base du firmware/pilote, de l'application de gestion, de la console virtuelle et d'autres éléments s'affichent dans le volet de droite. Sélectionnez un élément dans le volet en cours, puis cliquez sur **Afficher les détails** dans le volet de droite pour afficher des informations approfondies sur cet élément.

Lorsque vous êtes connecté, toutes les pages sont actualisées automatiquement. Lors de la connexion suivant le déploiement de l'appliance, si une mise à jour d'OpenManage Enterprise est disponible, vous êtes invité à mettre à jour la version immédiatement en cliquant sur **Mettre à jour**. Les utilisateurs disposant de tous les privilèges OpenManage Enterprise (Administrateur, Gestionnaire de périphériques et Observateur) peuvent consulter le message, mais seul un administrateur peut mettre à jour la version. Un administrateur peut choisir de recevoir un rappel ou d'ignorer le message. Pour plus d'informations sur la mise à jour de votre version d'OpenManage Enterprise, voir Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168.

Pour toutes les actions basées sur des tâches d'OpenManage Enterprise, lorsqu'une tâche est créée ou commence à être exécutée, le coin inférieur droit affiche le message correspondant. Les détails concernant la tâche peuvent être consultés sur la page **Détails de la tâche**. Voir Afficher les listes de tâches , page 129.

6

Portail d'accueil OpenManage Enterprise

En cliquant sur **OpenManage Enterprise** > **Home**, la page d'accueil d'OpenManage Enterprise s'affiche. Sur la page d'accueil, vous pouvez :

- Afficher le tableau de bord afin d'obtenir un snapshot en temps réel des conditions d'intégrité des périphériques, puis effectuer des actions, au besoin. Voir le Tableau de bord.
- Afficher les alertes critiques et d'avertissement et les résoudre. Voir Gestion des alertes des périphériques.
- La section Widgets répertorie la garantie cumulée, la conformité du firmware/pilote et les états de conformité de la configuration de tous les périphériques. Pour plus d'informations sur les fonctionnalités sous la catégorie Widgets, voir Surveillance des appareils à l'aide du tableau de bord OpenManage Enterprise , page 38. Le volet de droite répertorie les alertes récentes et les tâches générées par OpenManage Enterprise. Pour afficher plus d'informations sur une alerte ou une tâche, cliquez sur le titre de l'alerte ou de la tâche. Voir Surveillance et gestion des alertes d'appareil , page 118 et Utilisation des tâches pour le contrôle de périphériques , page 129.
- Si une version mise à jour d'OpenManage Enterprise est disponible, vous êtes immédiatement alerté de la disponibilité d'une mise à jour. Pour mettre à jour, cliquez sur **Mettre à jour**. Pour plus d'informations sur la mise à jour de votre version d'OpenManage Enterprise, voir Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168.
- La section **Alertes récentes** répertorie les alertes les plus récentes générées par les périphériques surveillés par OpenManage Enterprise. Cliquez sur le titre d'une alerte pour afficher des informations détaillées sur celle-ci. Voir Gestion des alertes des périphériques.
- La section **Tâches récentes** répertorie les dernières tâches créées et exécutées. Cliquez sur le titre de la tâche pour afficher des informations détaillées sur celle-ci. Voir Afficher les listes de tâches , page 129.

REMARQUE : Si vous êtes connecté en tant que gestionnaire de périphériques, le portail d'accueil affiche des informations relatives au périphérique ou au groupe de périphériques détenu par le gestionnaire de périphériques. En outre, la liste déroulante Groupes de périphériques répertorie uniquement les groupes de périphériques pour lesquels le gestionnaire de périphériques a un accès opérationnel. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Sujets :

Surveillance des appareils à l'aide du tableau de bord OpenManage Enterprise

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Sauf lors de la première connexion, le tableau de bord est la première page qui s'affiche à chaque nouvelle connexion à OpenManage Enterprise.

Pour ouvrir la page Tableau de bord à partir de n'importe quelle page d'OpenManage Enterprise, cliquez sur le symbole du tableau de bord, dans le coin supérieur gauche. Sinon, cliquez sur **Accueil**.

À l'aide des données de surveillance en temps réel, le tableau de bord affiche l'intégrité du périphérique, la conformité du firmware/pilote, la garantie, les alertes, ainsi que d'autres aspects des périphériques et groupes de périphériques dans l'environnement de votre datacenter.

Toutes les mises à jour disponibles de la console s'affichent également sur le tableau de bord. Vous pouvez effectuer la mise à niveau immédiate d'OpenManage Enterprise ou définir un rappel de sorte qu'OpenManage Enterprise vous le notifie plus tard.

Lorsque vous démarrez l'application pour la première fois, la page Tableau de bord s'affiche vierge par défaut. Pour que des périphériques puissent être surveillés et affichés sur le tableau de bord, ajoutez-les à OpenManage Enterprise. Pour ajouter des périphériques, reportez-vous aux rubriques Détection de périphériques pour la surveillance ou la gestion , page 41 et Organisation des périphériques dans des groupes , page 55.

- Gestion des firmwares et des pilotes de périphérique , page 77
- Gestion des alertes de périphériques
- Détection de périphériques
- Création de rapports
- Gestion des paramètres de l'appliance OpenManage Enterprise , page 147

REMARQUE : Si vous sélectionnez un groupe de périphériques dans la liste déroulante **Groupes de périphériques**, toutes les données affichées dans le tableau de bord concerneront uniquement le groupe de périphériques sélectionné.

Par défaut, la section **Intégrité matérielle** affiche un graphique circulaire qui présente l'intégrité actuelle de tous les périphériques surveillés par OpenManage Enterprise. Cliquez sur les sections du graphique circulaire pour afficher les informations sur les périphériques avec leurs états d'intégrité respectifs.

Un graphique circulaire de la section **Alertes** répertorie les alertes reçues par les périphériques des groupes de périphériques sélectionnés. Voir Surveillance et gestion des alertes d'appareil , page 118. Le nombre total d'alertes du graphique circulaire varie en fonction de l'activation ou de la désactivation de l'affichage des alertes qui n'ont pas été acquittées. Par défaut, seules les alertes qui n'ont pas été acquittées s'affichent. Voir Personnalisation de l'affichage des alertes , page 166. Pour afficher les alertes de chaque catégorie, cliquez sur les bandes de couleur correspondantes. Dans la boîte de dialogue **Alertes**, la section Critique répertorie les alertes d'intégrité critique. Pour afficher toutes les alertes générées, cliquez sur **Toutes**. La colonne **NOM DE LA SOURCE** indique le périphérique qui a généré l'alerte. Cliquez sur ce nom pour afficher et configurer les propriétés du périphérique. Voir Affichage et configuration des périphériques individuels , page 68.

Pour plus d'informations sur le graphique circulaire, voir Graphique circulaire , page 39 et États d'intégrité du périphérique , page 40. Pour afficher le résumé des périphériques dans un autre groupe de périphériques surveillés par OpenManage Enterprise, sélectionnez-le dans le menu déroulant **Groupes de périphériques**. Pour afficher la liste des périphériques présentant un état d'intégrité particulier, vous pouvez cliquer sur la bande de couleur associée à une catégorie d'intégrité ou cliquer sur les symboles d'état d'intégrité respectifs en regard du graphique circulaire.

REMARQUE : Dans la liste des périphériques, cliquez sur le nom ou l'adresse IP du périphérique pour afficher ses données de configuration, puis sur modifier. Voir Affichage et configuration des périphériques individuels , page 68.

La section Widgets fournit un récapitulatif de certaines des fonctionnalités clés d'OpenManage Enterprise. Pour afficher le récapitulatif de chaque catégorie, cliquez sur le titre du widget.

- **Garantie** : affiche le nombre de périphériques dont la garantie arrive à expiration. Cela est basé sur les **Paramètres de garantie**. Si l'utilisateur choisit d'obtenir des notifications d'expiration de la garantie, alors le nombre d'appareils dont la garantie a expiré est indiqué. Sinon, le nombre de d'appareils pour lesquels la garantie expire bientôt ou est active est indiqué. Cliquez pour afficher plus d'informations dans la boîte de dialogue **Garantie**. Pour plus d'informations sur la gestion de la garantie du périphérique, voir la rubrique Gestion de la garantie des périphériques , page 137. Positionnez le pointeur sur la section **Garantie** pour lire les définitions des symboles utilisés dans la section.
- **Firmwares/pilotes** : affiche l'état de la conformité des firmwares/pilotes des lignes de base de périphérique créées sur OpenManage Enterprise. Si elles sont disponibles, les lignes de base du firmware/pilote Critique et Avertissement sont répertoriées dans cette section.
  - Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc technique *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération) disponible sur le Dell TechCenter.
  - Cliquez pour afficher plus d'informations sur la page **Conformité du firmware/pilote**.
  - Pour en savoir plus sur la mise à jour de firmware, la création du catalogue du firmware, la création de la ligne de base du firmware et la génération du rapport de conformité de la ligne de base, voir Gestion des firmwares et des pilotes de périphérique , page 77.
- **Configuration** : affiche l'état cumulé des lignes de base de la conformité de la configuration créées sur OpenManage Enterprise. Si elles sont disponibles, les lignes de base de la configuration Critique et Avertissement sont répertoriées. Voir Gérer les modèles de conformité , page 111.
- **Taux d'utilisation des ressources** : affiche l'utilisation du processeur et de la mémoire par l'appliance. Les vérifications par code couleur suivantes sont utilisées pour indiquer les différentes étapes de l'utilisation :
  - Vert : ressource utilisée à moins de 80 %
  - Jaune : ressource utilisée à plus de 80 % et moins de 95 %
  - Rouge : ressource utilisée à plus de 95 %

  REMARQUE : L'utilisation globale des ressources, illustrée sous la forme d'une barre verticale à code couleur sur la gauche du widget, correspond au cumul le plus défavorable de l'une des ressources.

Graphique circulaire

Vous pouvez afficher un graphique circulaire dans différentes sections de votre application OpenManage Enterprise. Les résultats affichés par le graphique circulaire dépendent des éléments que vous sélectionnez dans un tableau. Un graphique circulaire indique plusieurs états dans OpenManage Enterprise :

- État d'intégrité des périphériques : affiché sur la page Tableau de bord. Les couleurs utilisées dans le graphique circulaire divisent le cercle proportionnellement de façon à indiquer l'intégrité des périphériques surveillés par OpenManage Enterprise. Chaque état de périphérique est identifié par un symbole de couleur. Voir la section États d'intégrité du périphérique , page 40. Si le graphique circulaire indique l'état d'intégrité de 279 périphériques dans le groupe, dans lequel 131 ont un état « critique », 50 « avertissement » et 95 « OK », le cercle est composé de bandes de couleur représentant proportionnellement ces chiffres.

REMARQUE : Le graphique circulaire d'un seul périphérique consiste en un cercle épais d'une seule couleur qui indique l'état du périphérique. Par exemple, dans le cas d'un périphérique à l'état Avertissement, un cercle de couleur jaune s'affiche.

- États d'alerte des périphériques : indique le total des alertes générées pour les périphériques surveillés par OpenManage Enterprise. Voir Surveillance et gestion des alertes d'appareil , page 118.

  REMARQUE : Le nombre total d'alertes du graphique circulaire varie en fonction de l'activation ou de la désactivation de l'affichage des alertes qui n'ont pas été acquittées. Par défaut, seules les alertes qui n'ont pas été acquittées s'affichent. Voir Personnalisation de l'affichage des alertes , page 166.
- Conformité de la version du micrologiciel d'un périphérique par rapport à la version sur le catalogue : voir Gestion des firmwares et des pilotes de périphérique , page 77.
- Ligne de base de conformité de la configuration des périphériques et des groupes de périphériques : voir Gestion de la conformité de la configuration du périphérique , page 110.

REMARQUE : Le niveau de conformité du périphérique sélectionné est indiqué par un graphique circulaire. Lorsque plusieurs périphériques sont associés à une configuration de base, l'état du périphérique ayant le niveau de conformité le plus bas par rapport à la configuration de base est indiqué comme correspondant au niveau de conformité de cette configuration de base. Par exemple, si de nombreux périphériques sont associés à une ligne de base de micrologiciel et si le niveau de conformité de quelques périphériques est Sain ou Rétrograder , mais si la conformité d'un seul appareil du groupe est Mettre à niveau , le niveau de conformité de la ligne de base du firmware est Mettre à niveau. L'état cumulé équivaut à l'état du périphérique qui présente un niveau élevé de gravité. Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc technique *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération) disponible sur le Dell TechCenter.

REMARQUE : Le graphique circulaire d'un seul périphérique se compose d'un cercle épais d'une seule couleur qui indique le niveau de conformité du micrologiciel de périphérique. Par exemple, dans le cas d'un périphérique à l'état Critique, un cercle de couleur rouge s'affiche, indiquant que le micrologiciel du périphérique doit être mis à jour.

États d'intégrité du périphérique

Tableau 12. États d'intégrité du périphérique dans OpenManage Enterprise

État d'intégrité	Définition
Critique	Indique qu'une défaillance très importante du périphérique ou de l'environnement s'est produite.
Avertissement	Le périphérique est sur le point d'échouer. Indique que certains aspects du périphérique ou de l'environnement sont anormaux. Nécessite une intervention immédiate.
OK	Le périphérique est pleinement fonctionnel.
Inconnu	L'état du périphérique est inconnu.

REMARQUE : Les données affichées sur le tableau de bord dépendent des privilèges d'utilisateur dont vous disposez pour utiliser OpenManage Enterprise. Pour en savoir plus sur les utilisateurs, voir Gestion des utilisateurs.

7

Détection de périphériques pour la surveillance ou la gestion

En cliquant sur **OpenManage Enterprise** > **Contrôler** > **Détection**, vous pouvez détecter des périphériques dans l'environnement de votre datacenter pour les gérer, améliorer leur facilité d'utilisation et la disponibilité des ressources pour les opérations cruciales pour votre entreprise. La page **Détection** affiche le nombre de périphériques détectés, ainsi que les informations sur l'état de la tâche de détection pour ce périphérique. Les états de tâche possibles sont les suivants : En file d'attente, Terminé et Arrêté. Le volet de droite affiche des informations sur la tâche telles que le nombre total de périphériques possibles, les périphériques détectés par types de périphériques et leur nombre respectif, l'heure de la prochaine exécution si la tâche est planifiée, ainsi que l'heure de la dernière détection. **Afficher les détails** affiche les détails de la tâche de détection en particulier dans le volet de droite.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Afin de prendre en charge la détection avec des informations d'identification de domaine, OpenManage Enterprise 3.2 et versions supérieures utilise le protocole OpenSSH au lieu du protocole WSMAN utilisé dans les versions précédentes. Par conséquent, tous les appareils Windows et Hyper-V détectés avant la mise à jour de l'appliance doivent être supprimés et redétectés avec leurs informations d'identification OpenSSH. Reportez-vous à la documentation de Microsoft pour activer OpenSSH sur Windows et Hyper-V.
- Sur les pages **Détection et planifications d'inventaire**, l'état d'une tâche planifiée est identifié par **En file d'attente** dans la colonne **État**. Cependant, le même état est indiqué comme **Planifié** sur la page **Tâches**.
- Par défaut, la dernière adresse IP découverte d'un périphérique est utilisée par OpenManage Enterprise pour effectuer toutes les opérations. Pour que tout changement d'adresse IP soit effectif, vous devez redécouvrir le périphérique.
- Pour les appareils tiers, vous pouvez voir des entrées en double s'ils sont découverts à l'aide de plusieurs protocoles. Cette duplication peut être corrigée en supprimant les entrées et en redécouvrant le ou les appareils en utilisant uniquement le protocole IPMI.

La fonction Détection permet d'effectuer les opérations suivantes :

- Afficher, ajouter et supprimer des périphériques de la liste d'exclusion globale. Voir Exclusion globale des plages , page 49.
- Créer, exécuter, modifier, supprimer et arrêter les tâches de détection de périphériques.

Tâches associées

Suppression d'une tâche de détection de périphérique , page 54
Affichage des détails d'une tâche de détection de périphériques , page 47
Arrêt des tâches de détection de périphériques , page 48
Exécution d'une tâche de détection de périphériques , page 48
Spécification du mode détection pour créer une tâche de détection de serveur , page 50
Création de protocole de tâche de détection d'appareils personnalisé pour les serveurs : paramètres supplémentaires pour les protocoles de détection , page 50
Spécification du mode détection pour créer une tâche de détection de stockage Dell , page 52
Création de modèle de tâche personnalisée de détection de périphériques pour des périphériques SNMP , page 53
Spécification du mode de détection pour créer une tâche de détection MULTIPLE , page 54
Modification d'une tâche de détection de périphériques , page 48

Sujets :

- Affichage des détails d'une tâche de détection de périphériques
- Modification d'une tâche de détection de périphériques
- Exécution d'une tâche de détection de périphériques
- Arrêt des tâches de détection de périphériques
- Spécification de plusieurs périphériques via l'importation des données provenant du fichier .csv
- Exclusion globale des plages
- Spécification du mode détection pour créer une tâche de détection de serveur
- Création de protocole de tâche de détection d'appareils personnalisé pour les serveurs : paramètres supplémentaires pour les protocoles de détection
- Spécification du mode de détection pour créer une tâche de détection de châssis
- Création de protocoles de tâche de détection d'appareils personnalisés pour les boîtiers : paramètres supplémentaires pour les protocoles de détection
- Spécification du mode détection pour créer une tâche de détection de stockage Dell
- Spécification du mode de détection pour créer une tâche de détection de commutateur de réseau
- Création de protocole HTTPS de tâche de détection d'appareils personnalisé pour les périphériques de stockage : paramètres supplémentaires pour les protocoles de détection
- Création de modèle de tâche personnalisée de détection de périphériques pour des périphériques SNMP
- Spécification du mode de détection pour créer une tâche de détection MULTIPLE
- Suppression d'une tâche de détection de périphérique

Détection automatique des serveurs à l'aide de la fonctionnalité de détection initiée par serveur

OpenManage Enterprise permet la détection automatique des serveurs dotés du firmware iDRAC, version 4.00.00.00 ou ultérieure. L'appliance peut être configurée pour permettre à ces serveurs de localiser automatiquement la console en interrogeant le DNS et de lancer leur détection.

Pour une détection initiée par serveur, les conditions préalables suivantes doivent être remplies :

- Cette fonctionnalité s'applique uniquement aux serveurs dotés du firmware iDRAC, version 4.00.00.00 ou ultérieure.
- Les serveurs doivent figurer dans le même domaine ou sous-domaine qu'OpenManage Enterprise.
- L'application OpenManage Enterprise doit être enregistrée auprès du DNS pour y ajouter les informations de configuration à l'aide de l'interface TUI. Il est recommandé que le DNS autorise les mises à jour automatiques à partir d'OpenManage Enterprise.
- Les anciens enregistrements de la console de l'appliance sur le DNS, le cas échéant, doivent être nettoyés afin d'éviter de multiples annonces des serveurs.

REMARQUE : Le contrôle d'accès basé sur le périmètre (SBAC) n'affecte pas les listes de périphériques sur la page **Surveiller** > **Détection initiée par serveur**. Les gestionnaires de périphériques verront les périphériques au-delà de leur périmètre sur cette page.

Les étapes indiquées ci-dessous sont suivies pour une détection automatique de serveurs dans OpenManage Enterprise :

1. Ajoutez les informations de configuration d'OpenManage Enterprise auprès du DNS à l'aide de l'une des méthodes suivantes :
   - TUI : à l'aide de l'interface TUI, activez l'option **Configurer la détection initiée par serveur**. Pour plus d'informations, voir Configuration d'OpenManage Enterprise en utilisant l'interface texte utilisateur , page 27.
   - Manuellement : ajoutez à votre serveur DNS les 4 enregistrements suivants sur le réseau pour lequel l'interface est configurée sur l'appliance. Assurez-vous de remplacer toutes les instances de `<domain>` ou `<subdomain.domain>` par le domaine DNS approprié et le nom d'hôte du système.
     - `<OME hostname>.<domain> 3600 A <OME IP address>`
     - `_dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>`

     Pour créer des enregistrements avec `nsupdate` dans Linux, utilisez les commandes suivantes :
     - Pour créer un enregistrement de nom d'hôte

       ```
       >update add omehost.example.com 3600 A XX.XX.XX.XX
       ```

- Pour ajouter des enregistrements pour la détection initiée par serveur

```
>update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._
tcp.example.com.

>update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/
Actions/DiscoveryConfigService.SignalNodePresence

>update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443 omehost.example.com.
```

Pour créer des enregistrements avec `dnscmd` sur un serveur DNS Windows, utilisez les commandes suivantes :

- Pour créer un enregistrement de nom d'hôte

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- Pour ajouter des enregistrements pour la détection initiée par serveur

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR
ptr.dcimprovsrv._tcp.example.com

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp SRV 0 0 443
omehost.example.com
```

2. Par défaut, la stratégie d'approbation de détection dans l'appliance est définie sur Automatique, et les serveurs qui établissent le contact avec la console sont automatiquement détectés. Pour modifier les paramètres, reportez-vous à la section Gestion des préférences de la console , page 164.
3. Une fois que l'appliance est configurée, comme indiqué dans les étapes précédentes, les serveurs peuvent établir le contact avec OpenManage Enterprise en interrogeant le DNS. L'appliance vérifie les serveurs après s'être assuré que le certificat client des serveurs est signé par l'autorité de certification Dell.

   REMARQUE : Si des modifications ont été apportées au certificat SSL ou à l'adresse IP du serveur, le serveur relance le contact avec OpenManage Enterprise.
4. La page **Surveiller** > **Détection initiée par serveur** répertorie les serveurs qui établissent le contact avec la console. En outre, les serveurs dont les informations d'identification ont été ajoutées dans la console, mais qui doivent encore établir le contact, sont également répertoriés. Les états suivants des serveurs basés sur les conditions mentionnées précédemment sont affichés :
   - Annoncé : le serveur établit le contact avec la console, mais ses informations d'identification ne sont pas ajoutées à la console.
   - Informations d'identification ajoutées : les informations d'identification du serveur sont ajoutées à la console, mais le serveur n'établit pas de contact avec la console.
   - Prêt pour la détection : les informations d'identification du serveur sont ajoutées, et le serveur établit un contact.

     REMARQUE : L'appliance déclenche une tâche de détection toutes les 10 minutes afin de détecter tous les serveurs dont l'état est défini sur « Prêt pour la détection ». Toutefois, si la stratégie d'approbation de détection de l'appliance est définie sur « Manuel », l'utilisateur doit déclencher manuellement la tâche de détection pour chaque serveur. Pour en savoir plus, voir Gestion des préférences de la console , page 164
   - Tâche soumise pour détection : cet état indique que la tâche de détection est lancée automatiquement ou manuellement pour le serveur.
   - Détecté : le serveur est détecté et répertorié sur la page Tous les périphériques.

Les tâches suivantes peuvent être exécutées sur la page **Surveiller** > **Détection initiée par serveur** :

1. **Importer** : pour importer les informations d'identification du serveur :
   a. Cliquez sur **Importer**.
   b. Dans l'Assistant Importer à partir d'un fichier, cliquez sur **Télécharger le fichier de numéros de série** pour accéder au fichier .csv et le sélectionner.

      Pour afficher un exemple de fichier CSV des informations d'identification de serveur, cliquez sur **Télécharger un exemple de fichier CSV**.
   c. Cliquez sur **Terminer**.
2. **Détecter** : pour détecter manuellement les serveurs dont l'état est défini sur « Prêt pour la détection » :
   a. Sélectionnez les serveurs répertoriés sur la page Détection initiée par serveur qui se trouvent à l'état « Prêt pour la détection ».

b. Cliquez sur **Découvrir**.

Une tâche de détection est déclenchée pour détecter les serveurs. Après la détection, ces serveurs sont répertoriés sur la page Tous les périphériques.

3. **Supprimer** : pour supprimer les serveurs répertoriés sur la page Détection initiée par serveur :
   a. Sélectionnez les serveurs de la page Détection initiée par serveur qui sont déjà détectés et répertoriés sur la page Tous les périphériques.
   b. Cliquez sur **Supprimer**.

   Les serveurs sont supprimés de la page Détection initiée par serveur.

   REMARQUE : Les entrées correspondant aux serveurs détectés sont automatiquement purgées après 30 jours.
4. **Exporter** : pour exporter les informations d'identification du serveur au format HTML, CSV ou PDF :
   a. Sélectionnez un ou plusieurs serveurs sur la page Détection initiée par serveur.
   b. Cliquez sur **Exporter**.
   c. Dans l'Assistant Exporter tout, sélectionnez l'un des formats de fichier suivants : HTML, CSV ou PDF.
   d. Cliquez sur **Terminer**. Une tâche est créée, et les données sont exportées vers l'emplacement sélectionné.

Création d'une tâche de détection de périphérique

Les étapes suivantes expliquent comment démarrer une tâche de détection de périphériques dans OpenManage Enterprise pour détecter les périphériques dans votre datacenter à l'aide de l'Assistant de création de tâches de détection.

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Pour lancer Créer une tâche de détection, vous pouvez effectuer l'une des opérations suivantes :
   - Cliquez sur **Surveiller** > **Détection** > **Créer**.
   - Sinon, dans la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), cliquez sur le menu déroulant **Détection**, puis cliquez sur **Détecter des périphériques**.
2. Dans la boîte de dialogue **Créer une tâche de détection**, un nom de tâche par défaut est renseigné. Pour le modifier, saisissez le nom de la tâche de détection.
   Par défaut, la boîte de dialogue vous permet de définir les propriétés de périphériques similaires en une fois.
   - Pour inclure plus de périphériques ou de plages à la tâche de détection en cours, cliquez sur **Ajouter**. Un autre ensemble des champs suivants est affiché. Il vous permet de définir les propriétés du périphérique : Type, adresse IP/Nom de l'hôte/Plage et Paramètres.

     AVERTISSEMENT : Un maximum de 8 000 périphériques peut être géré par OpenManage Enterprise. Par conséquent, ne spécifiez pas de réseaux de grande taille qui contiennent plus de périphériques que le nombre maximum pris en charge par OpenManage Enterprise. Le cas échéant, le système peut soudainement cesser de répondre.

     REMARQUE : Lors de la détection d'un grand nombre de périphériques, évitez de créer plusieurs tâches de détection à l'aide d'une adresse IP individuelle et utilisez plutôt la plage d'adresses IP des périphériques.
   - Pour détecter des périphériques en important des plages provenant du fichier .csv. Voir Spécification de plusieurs périphériques via l'importation des données provenant du fichier .csv , page 48.
   - Pour exclure certains périphériques, retirez les périphériques à exclure, ou pour afficher la liste des périphériques exclus de la détection, voir Exclusion globale de périphérique(s) des résultats de détection.
3. Dans le menu déroulant **Types de périphériques**, pour détecter :
   - Un serveur, sélectionnez **SERVEUR**. Voir Spécification du mode de détection pour créer une tâche de détection de serveur.
   - Un châssis, sélectionnez **CHÂSSIS**. Voir Spécification du mode de détection pour créer une tâche de détection de châssis.
   - Un périphérique de stockage Dell EMC ou un commutateur réseau, sélectionnez **STOCKAGE DELL**, ou **COMMUTATEUR RÉSEAU**. Voir Spécification du mode de détection pour créer une tâche de détection de stockage, stockage Dell et commutateur réseau.
   - Pour détecter des périphériques à l'aide de plusieurs protocoles, sélectionnez **MULTIPLE**. Voir la section Spécification du mode de détection pour créer une tâche de détection MULTIPLE , page 54.
4. Dans la case **Adresse IP/Nom de l'hôte/Plage**, saisissez l'adresse IP, le nom de l'hôte ou la plage d'adresses IP à détecter ou inclure. Pour en savoir plus sur les données que vous pouvez saisir dans ce champ, cliquez sur le symbole **i**.

   REMARQUE :
   - La taille de la plage est limitée à 16 385 (0x4001).

- Les formats CIDR IPv6 et IPv6 sont également pris en charge.

5. Dans la section **Paramètres**, saisissez le nom d'utilisateur et le mot de passe du protocole utilisé pour la détection des plages.
6. Cliquez sur **Paramètres supplémentaires** pour sélectionner un autre protocole et changer les paramètres.
7. Dans la section **Programmer une tâche de détection**, exécutez la tâche immédiatement ou programmez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
8. Cochez la case **Activer la réception d'interruptions pour les serveurs iDRAC et les châssis MX7000 détectés** pour permettre à OpenManage Enterprise de recevoir les interruptions entrantes des serveurs et des châssis MX7000 détectés.

   REMARQUE : L'activation de ce paramètre permet d'activer les alertes sur l'iDRAC (si elles sont désactivées) et de définir une destination d'alerte pour l'adresse IP du serveur OpenManage Enterprise. Si vous devez activer des alertes spécifiques, vous devez les configurer sur l'iDRAC en activant les serveurs d'alerte et les interruptions SNMP appropriés. Pour en savoir plus, voir le Guide de l'utilisateur d'iDRAC.

9. Sélectionnez **Définir la chaîne de communauté pour la destination d'interruption à partir des paramètres d'application**. Cette option est uniquement disponible pour les boîtiers MX7000 et les serveurs iDRAC détectés.
10. Cochez la case **Envoyer par e-mail à la fin**, puis saisissez l'adresse e-mail qui doit recevoir une notification à propos de l'état de la tâche de détection. Si l'adresse e-mail n'est pas configurée, le lien **Accéder aux Paramètres SMTP** s'affiche. Cliquez sur le lien et configurez les paramètres SMTP. Voir Configuration des alertes SMTP, SNMP et Syslog , page 123. Si vous sélectionnez cette option sans configurer SMTP, le bouton **Terminer** ne s'affiche pas pour poursuivre la tâche.
11. Cliquez sur **Terminer**. Le bouton Terminer ne s'affiche que si les champs sont correctement ou complètement remplis. La tâche de détection est créée et exécutée. L'état est affiché dans la page **Détails de la tâche**.

Pendant la détection de périphériques, les privilèges disponibles qui sont activés sur un périphérique distant pour le compte d'utilisateur qui est spécifié pour la plage de détection sont vérifiés. Si l'authentification de l'utilisateur aboutit, le périphérique est automatiquement intégré ou pourra être intégré ultérieurement avec d'autres informations d'identification de l'utilisateur. Voir la section Intégration de périphériques , page 45.

REMARQUE : Pendant la détection de CMC, les serveurs, l'IOM et les modules de stockage (configurés avec une adresse IP et un SNMP sur « public » comme chaîne de communauté) résidant sur CMC sont également détectés et intégrés. Si vous activez la réception d'interruptions pendant la détection de CMC, OpenManage Enterprise, et non le châssis, est défini comme destination d'interruption sur tous les serveurs.

REMARQUE : Pendant la découverte du CMC, les modules d'agrégation d'E/S en mode MUX programmable (PMUX) ne sont pas découverts.

Intégration de périphériques

L'intégration permet de gérer, et non uniquement surveiller, les serveurs.

- Si vous indiquez les informations d'identification de niveau administrateur au cours de la détection, les serveurs sont intégrés (l'état du périphérique est « Géré » dans la vue Tous les périphériques).
- Si vous indiquez des informations d'identification de niveau inférieur au cours de la détection, les serveurs ne sont pas intégrés (l'état est « Surveillé » dans la vue Tous les périphériques).
- Si la console est également définie en tant que récepteur d'interruptions sur les serveurs, l'état d'intégration de ces serveurs est « Géré avec des alertes »).
- **Erreur** : indique un problème d'intégration du périphérique.
- **Proxy** : disponible uniquement pour le châssis MX7000. Indique que le périphérique est détecté via un châssis MX7000 et non directement.

Si vous souhaitez intégrer des périphériques avec un compte d'utilisateur autre que celui spécifié pour la détection, ou bien réessayer l'intégration suite à un échec d'intégration lors de la détection, procédez comme suit :

REMARQUE :

- Tous les périphériques qui ont été intégrés via cet assistant restent intégrés via ce compte d'utilisateur et ne seront pas substitués par le compte d'utilisateur de détection lors de futures détections de ces périphériques.
- Pour les périphériques déjà découverts, si la destination de trap SNMP est définie manuellement dans iDRAC sur OpenManage Enterprise, les alertes sont reçues et traitées par l'appliance. Toutefois, l'état géré du périphérique tel qu'il s'affiche sur la page Tous les périphériques reste identique à celui de l'état découvert initial, c'est-à-dire « Surveillé », « Géré » ou « Géré avec des alertes ».

- La page Tous les périphériques affiche l'**État géré** de tous les châssis intégrés en tant que « Géré », quelles que soient les informations d'identification de rôle utilisateur de châssis utilisées au moment de l'intégration. Si un châssis a été intégré avec les informations d'identification d'un utilisateur « en lecture seule », il se peut qu'un problème survienne lors des activités de mise à jour exécutées sur le châssis. Par conséquent, il est recommandé d'intégrer les châssis avec les informations d'identification d'un administrateur de châssis pour exécuter toutes les activités.
- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Dans le menu **OpenManage Enterprise**, sous **Périphériques**, cliquez sur **Tous les périphériques**.
   Un graphique circulaire indique l'état de tous les périphériques dans le volet en cours. Voir le Graphique circulaire. Le tableau répertorie les propriétés des périphériques sélectionnés, ainsi que leurs états d'intégration, qui sont les suivants :
   - **Erreur** : le périphérique ne peut pas être intégré. Essayez en vous connectant à l'aide des privilèges recommandés. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
   - **Géré** : le périphérique est intégré et peut être géré par la console OpenManage Enterprise.
   - **Surveillé** : le périphérique ne peut pas être géré (par exemple, découvert avec SNMP).
   - **Géré avec des alertes** : le périphérique est intégré et la console OpenManage Enterprise a correctement inscrit son adresse IP avec le périphérique en tant que destination d'interruption au cours de la découverte.
2. Dans le volet en cours, cochez la case correspondant aux périphériques, puis cliquez sur **Plus d'actions** > **Intégration**.
   Depuis la page Tous les périphériques, assurez-vous de sélectionner uniquement les types de périphérique qui sont pris en charge pour l'intégration. Pour rechercher les périphériques appropriés dans le tableau, cliquez sur **Filtres avancés**, puis sélectionnez ou saisissez les données de l'état d'intégration dans la case du filtre.
   REMARQUE : Tous les périphériques détectés ne sont pas pris en charge pour l'intégration et uniquement iDRAC et CMC sont pris en charge. Assurez-vous de sélectionner l'option d'intégration pour le type de périphérique pris en charge.
3. Dans la boîte de dialogue **Intégration**, saisissez les informations d'identification WS-Man : nom d'utilisateur et mot de passe.
4. Dans la section **Paramètres de connexion** :
   a. Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
   b. Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
      REMARQUE : Si la valeur d'expiration du délai saisie est supérieure à la durée d'expiration de la session en cours, vous êtes automatiquement déconnecté d'OpenManage Enterprise. Toutefois, si la valeur se trouve dans la fenêtre de délai d'expiration de la session en cours, la session est poursuivie et n'est pas déconnectée.
   c. Dans le champ **Port**, saisissez le numéro de port utilisé par la tâche pour exécuter la détection.
   d. Champ facultatif. Sélectionner **Activer la vérification du nom commun (CN)**.
   e. Champ facultatif. Sélectionnez **Activer la vérification d'autorité de certification (AC)**, puis accédez au fichier de certificat.
5. Cliquez sur **Terminer**.
   REMARQUE : La case **Activer la réception d'interruptions pour les serveurs détectés** n'est effective que pour les serveurs détectés à l'aide de leur interface iDRAC. La sélection n'est pas effective pour les autres serveurs, tels que ceux détectés à l'aide de la détection de système d'exploitation.

Matrice de support du protocole pour la détection de périphériques

Le tableau suivant fournit des informations sur les protocoles pris en charge pour la découverte de périphériques.

REMARQUE : La fonctionnalité de détection, de surveillance et de gestion des serveurs PowerEdge YX1X dotés d'iDRAC6 par les protocoles pris en charge est limitée. Pour en savoir plus, voir Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

Tableau 13. Matrice de support de protocoles de détection

Périphérique /Système d'exploitation	Protocoles						
	Web Services-Management (WS-MAN)	**Redfish**	**Protocole SNMP (Simple Network Management Protocol - Protocole de gestion de réseau simple)**	**Secure Shell (SSH)**	**Intelligent Platform Management Interface (Interface intelligente de gestion de plateforme) (IPMI)**	**ESXi (VMWare)**	**HTTPS**
iDRAC6 et versions ultérieures	**Pris en charge**	**Pris en charge** Uniquement pour iDRAC9 version 4.40.10 .00 et versions ultérieures **Non pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
PowerEdge C*	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Châssis PowerEdge (CMC)	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Châssis PowerEdge MX7000	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Périphériques de stockage	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Commutateurs Ethernet	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
ESXi	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge
Linux	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge
Windows	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge
Hyper-V	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge	Non pris en charge
Serveurs non Dell	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	Non pris en charge
PowerVault ME	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	**Pris en charge**	Non pris en charge	**Pris en charge**

Affichage des détails d'une tâche de détection de périphériques

1. Cliquez sur **Moniteur** > **Détection**.
2. Cochez la ligne correspondant au nom de la tâche de détection, puis cliquez sur **Afficher les détails** dans le volet de droite.

La page **Détails de la tâche** affiche les informations respectives de la tâche de détection.

3. Pour plus d'informations sur la gestion des tâches, voir Utilisation des tâches pour le contrôle de périphériques , page 129.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Modification d'une tâche de détection de périphériques

Vous pouvez modifier une seule tâche de détection de périphériques à la fois.

1. Cochez la case correspondant à la tâche de détection à modifier, puis cliquez sur **Modifier**.
2. Dans la boîte de dialogue **Créer une tâche de détection**, modifiez les propriétés.
   Pour en savoir plus sur les tâches à effectuer dans cette boîte de dialogue, voir Création d'une tâche de détection de périphérique.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Exécution d'une tâche de détection de périphériques

REMARQUE : Vous ne pouvez pas exécuter une nouvelle fois une tâche qui est déjà en cours d'exécution.

Pour exécuter une tâche de détection de périphériques :

1. Dans la liste des tâches de détection de périphériques existantes, cochez la case correspondant à la tâche que vous souhaitez exécuter maintenant.
2. Cliquez sur **Exécuter**.
   La tâche démarre immédiatement et un message s'affiche dans l'angle inférieur droit.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Arrêt des tâches de détection de périphériques

Vous pouvez arrêter la tâche uniquement si elle est en cours d'exécution. Il est impossible d'arrêter les tâches de détection qui sont terminées ou celles qui ont échoué. Pour arrêter une session :

1. Dans la liste des tâches de détection existantes, cochez la case correspondant à la tâche que vous souhaitez arrêter.

   REMARQUE : Vous ne pouvez pas arrêter plusieurs tâches à la fois.

2. Cliquez sur **Arrêter**.
   La tâche est arrêtée et un message s'affiche dans l'angle inférieur droit.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Spécification de plusieurs périphériques via l'importation des données provenant du fichier .csv

1. Dans la boîte de dialogue **Créer une tâche de détection**, une tâche de détection est renseignée par défaut dans la zone **Nom de tâche de détection**. Pour la modifier, saisissez un nom de tâche de détection.
2. Cliquez sur **Importer**.

REMARQUE : Téléchargez un échantillon du fichier .CSV, si nécessaire.

3. Dans la boîte de dialogue **Importer**, cliquez sur **Importer**, naviguez jusqu'au fichier .CSV contenant une liste de plages valides, puis cliquez sur **OK**.

   REMARQUE : Un message d'erreur s'affiche si le fichier .CSV contient des plages non valides et les plages en double sont exclues pendant l'opération d'importation.

Exclusion globale des plages

À l'aide de l'Assistant d'exclusion globale des plages, vous pouvez saisir les adresses ou la plage des périphériques à exclure des activités de surveillance et de gestion d'OpenManage Enterprise. Les étapes suivantes décrivent la façon dont vous pouvez exclure la plage de périphériques :

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Actuellement, vous ne pouvez pas exclure un périphérique en utilisant son nom d'hôte, mais seulement en utilisant son adresse IP ou son nom de domaine complet.

1. Pour activer l'Assistant d'exclusion globale des plages, vous pouvez effectuer l'une des opérations suivantes :
   - À partir de la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), menu déroulant **Détection**, cliquez sur **Modifier les plages d'exclusion**.
   - Dans la vue **Contrôler** > **Détection**, cliquez sur la **Liste d'exclusion globale** située dans le coin supérieur droit.
2. Dans la boîte de dialogue **Exclusion globale de plages** :
   a. Dans le champ **Description de la plage d'exclusion**, saisissez les informations concernant la plage exclue.
   b. Dans le champ **Saisir des plages d'exclusion**, saisissez l'adresse ou la plage des périphériques à exclure. Vous pouvez saisir dans ce champ jusqu'à 1 000 adresses à la fois, en les séparant par un saut de ligne. Ce qui implique que chaque plage d'exclusion doit être saisie dans des lignes différentes dans le champ.
   Les plages pouvant être exclues sont les mêmes que les plages prises en charge et applicables pour rechercher un périphérique. Voir Création d'une tâche de détection de périphérique , page 44.

   REMARQUE :
   - La taille de la plage est limitée à 16 385 (0x4001).
   - Les formats CIDR IPv6 et IPv6 sont également pris en charge.

3. Cliquez sur **Ajouter**.
4. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**.
   L'adresse IP ou la plage est globalement exclue, puis s'affiche dans la liste des plages d'exclusion. Ces périphériques sont globalement exclus, ce qui implique qu'ils ne participent à aucune activité exécutée par OpenManage Enterprise.

   REMARQUE : Un périphérique globalement exclu est clairement identifié comme « Globalement exclu » sur la page **Détails de la tâche**.

   Pour supprimer un périphérique de la liste d'exclusion globale :
   a. Cochez la case et cliquez sur **Supprimer de l'exclusion**.
   b. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**. Le périphérique est supprimé de la liste d'exclusion globale. Néanmoins, le périphérique supprimé de la liste d'exclusion globale n'est pas automatiquement surveillé par OpenManage Enterprise. Vous devez détecter ce périphérique pour qu'OpenManage Enterprise commence à le surveiller.

REMARQUE :
- L'ajout de périphériques déjà connus par la console (c'est-à-dire déjà détectés par la console) à la liste d'exclusion globale entraîne la suppression de ces périphériques d'OpenManage Enterprise.
- Les périphériques nouvellement inclus dans la liste d'exclusion globale continuent d'être affichés dans la grille Tous les périphériques jusqu'au prochain cycle de détection. Pour éviter d'effectuer des tâches sur ces périphériques, il est vivement recommandé de les exclure manuellement de la page Tous les périphériques, en cochant la case correspondant au périphérique, puis en cliquant sur **Exclure**.
- Les périphériques répertoriés dans la liste d'exclusion globale sont exclus de toutes les tâches de la console. Si l'IP d'un périphérique est dans la liste d'exclusion globale et qu'une tâche de détection est créée avec une plage de détection comprenant

cette IP, ce périphérique ne sera pas détecté. Cependant, aucune erreur ne sera signalée sur la console lors de la création de la tâche de détection. Si vous prévoyez qu'un périphérique doit être détecté et qu'il ne l'est pas, vous devez vérifier la liste d'exclusion globale pour voir s'il a été inclus dans cette liste.

.

Spécification du mode détection pour créer une tâche de détection de serveur

1. Dans le menu déroulant **Types de périphériques**, sélectionnez **SERVEUR**.
2. Lorsque vous y êtes invité, sélectionnez :
   - **Dell iDRAC** : pour détecter en utilisant iDRAC.
   - **Système d'exploitation de l'hôte** : pour détecter en utilisant un système d'exploitation VMware ESXi, Microsoft Windows Hyper-V ou Linux.
   - **Serveurs non Dell (via OOB)** : pour détecter des serveurs tiers en utilisant IPMI.
3. Cliquez sur **OK**.
   En fonction de votre sélection, les champs changent sous **Paramètres**.
4. Saisissez l'adresse IP, le nom d'hôte ou la plage d'adresses IP associée au protocole dans **IP/Nom d'hôte/Plage**.
5. Sous **Paramètres**, saisissez le nom d'utilisateur et le mot de passe du serveur à détecter.
6. Pour personnaliser les protocoles de détection en cliquant sur **Paramètres supplémentaires**, consultez Création d'un modèle de tâche de détection d'appareil personnalisée pour serveurs.
7. Planifier la tâche de détection. Voir Définitions de champs de tâche de planification , page 180.
8. Cliquez sur **Terminer**.
   Une tâche de détection est créée et affichée dans la liste des tâches de détection.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Création de protocole de tâche de détection d'appareils personnalisé pour les serveurs : paramètres supplémentaires pour les protocoles de détection

Dans la boîte de dialogue **Paramètres supplémentaires**, saisissez les détails du protocole approprié avec lequel vous souhaitez détecter le ou les serveurs :

REMARQUE : les protocoles appropriés sont automatiquement présélectionnés en fonction de vos entrées initiales.

1. Pour la **Détection à l'aide de WS-Man/Redfish (iDRAC, Serveur, et/ou Boîtier)**
   a. Dans la section Informations d'identification, saisissez le **Nom d'utilisateur** et le **Mot de passe**.
   b. Dans la section **Paramètres de connexion** :
      - Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
      - Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
      - Dans le champ **Port**, indiquez le numéro de port. Par défaut, le port 443 est utilisé pour se connecter au périphérique. Pour connaître les numéros de port pris en charge, voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32
      - Cochez la case **Activer le nom commun (CN)** si le nom commun de l'appareil est identique au nom de l'hôte utilisé pour accéder à OpenManage Enterprise.
      - Cochez la case **Activer la vérification d'autorité de certification (CA)** si nécessaire.
2. Pour la **Détection à l'aide d'IPMI (serveurs non Dell via OOB)**
   a. Dans la section Informations d'identification, saisissez le **Nom d'utilisateur** et le **Mot de passe**.
   b. Dans la section **Paramètres de connexion** :
      - Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
      - Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.

- Dans le champ **KgKey** , saisissez une valeur appropriée.

3. Pour la **Détection à l'aide de SSH (Linux, Windows, Hyper-V)**

   REMARQUE : Seul OpenSSH sur Windows et Hyper-V est pris en charge. Le SSH CygWin n'est pas pris en charge.

   a. Dans la section Informations d'identification, saisissez le **Nom d'utilisateur** et le **Mot de passe**.
   b. Dans la section **Paramètres de connexion** :
      - Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
      - Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
      - Dans le champ **Port**, indiquez le numéro de port. Par défaut, le port 22 est utilisé pour se connecter au périphérique. Pour connaître les numéros de port pris en charge, voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32
      - Cochez la case **Vérifier la clé d'hôte connue** pour valider l'hôte par rapport aux clés d'hôte connues.

        REMARQUE : Les clés d'hôte connues sont ajoutées via le service */DeviceService/HostKeys REST API*. Pour plus d'informations sur la gestion des clés d'hôte, reportez-vous au *Guide API RESTful OpenManage Enterprise*.
      - Cochez la case **Utiliser l'option SUDO** si les comptes sudo sont préférés.

        REMARQUE : Pour que les comptes sudo fonctionnent, le fichier `/etc/sudoer` du ou des serveurs doit être configuré pour utiliser NOPASSWD.

4. Pour la **Détection à l'aide de ESXi (VMware)**

   a. Dans la section Informations d'identification, saisissez le **Nom d'utilisateur** et le **Mot de passe**.
   b. Dans la section **Paramètres de connexion** :
      - Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
      - Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
      - Dans le champ **Port**, indiquez le numéro de port. Par défaut, le port 443 est utilisé pour se connecter au périphérique. Pour connaître les numéros de port pris en charge, voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32
      - Cochez la case **Activer le nom commun (CN)** si le nom commun de l'appareil est identique au nom de l'hôte utilisé pour accéder à OpenManage Enterprise.
      - Cochez la case **Activer la vérification d'autorité de certification (CA)** si nécessaire.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Spécification du mode de détection pour créer une tâche de détection de châssis

1. Dans le menu déroulant **Types de périphérique**, sélectionnez **CHASSIS**.
   En fonction de votre sélection, les champs changent sous **Paramètres**.
2. Saisissez l'adresse IP, le nom d'hôte ou la plage d'adresses IP dans **IP/Nom d'hôte/Plage**.
3. Sous **Paramètres**, saisissez le nom d'utilisateur et le mot de passe du serveur à détecter.
4. Saisissez le type de communauté.
5. Pour créer un modèle de détection personnalisé en cliquant sur **Paramètres supplémentaires**, voir Création de protocoles de tâche de détection d'appareils personnalisés pour les boîtiers : paramètres supplémentaires pour les protocoles de détection , page 52.

REMARQUE : À l'heure actuelle, pour n'importe quel châssis M1000e détecté, la date de la colonne HORODATAGE sous Journaux du matériel s'affiche en tant que JAN 12, 2013 dans CMC 5.1x et les versions antérieures. Toutefois, pour toutes les versions de châssis CMC VRTX et FX2, la bonne date s'affiche.

REMARQUE : Lorsqu'un serveur dans un châssis est découvert séparément, les informations sur les emplacements concernant le serveur ne sont pas affichées dans la section **Informations sur le châssis**. Cependant, lorsqu'elles sont découvertes par l'intermédiaire d'un châssis, les informations sur les emplacements sont affichées. Par exemple, un serveur MX740c dans un châssis MX7000.

Création de protocoles de tâche de détection d'appareils personnalisés pour les boîtiers : paramètres supplémentaires pour les protocoles de détection

Dans la boîte de dialogue **Paramètres supplémentaires** :

1. Cochez la case **Détection à l'aide de WS-Man/Redfish (iDRAC, Serveur, et/ou Boîtier)**.

   REMARQUE : Pour les châssis, la case **Détecter à l'aide de WS-Man/Redfish** est cochée par défaut. Signifie que le châssis peut être détecté à l'aide de ces deux protocoles. Les châssis M1000e, CMC VRTX et FX2 prennent en charge les commandes WS-Man. Le châssis MX7000 prend en charge le protocole Redfish.

2. Saisissez le nom d'utilisateur et le mot de passe du boîtier à détecter.
3. Dans la section **Paramètres de connexion** :
   a. Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
   b. Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
   c. Dans le champ **Port**, indiquez le numéro de port. Par défaut, le port 443 est utilisé pour se connecter au périphérique. Pour connaître les numéros de port pris en charge, voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
   d. Sélectionnez la case **Activer le nom commun (CN)** si le nom commun du périphérique est identique au nom de l'hôte utilisé pour accéder à OpenManage Enterprise.
   e. Cochez la case **Activer la vérification d'autorité de certification (CA)**.
4. Pour détecter les modules d'E/S, cochez la case **Détecter les modules d'E/S avec le châssis**.

   REMARQUE : Applicable uniquement pour les boîtiers CMC VRTX, M1000e et FX2 (modèles FN2210S, FN410T et FN410S). Pour le châssis MX7000, les modules d'E/S sont automatiquement détectés.

   REMARQUE : Seuls les modules d'E/S en mode Autonome, PMUX (MUX programmable) et VLT (Jonction de liaisons virtuelles) peuvent être détectés. Les modules en mode Commutateur entier et Empilé ne seront pas détectés.

   a. Sélectionnez **Utiliser les informations d'identification du boîtier** si les informations d'identification de l'utilisateur de l'agrégateur d'E/S M sont identiques à celles du boîtier.
   b. Sélectionnez **Utiliser des informations d'identification différentes** si les informations d'identification de l'utilisateur de l'agrégateur d'E/S M diffèrent de celles du boîtier, puis procédez comme suit :
      - Saisissez le **Nom d'utilisateur** et le **Mot de passe**.
      - Modifiez les valeurs par défaut des champs **Nouvelles tentatives**, **Délai d'expiration** et **Port**, si nécessaire.
      - Sélectionnez **Vérifier la clé d'hôte connue** pour valider l'hôte par rapport aux clés d'hôte connues.

        REMARQUE : Les clés d'hôte connues sont ajoutées via le service */DeviceService/HostKeys REST API*. Pour plus d'informations sur la gestion des clés d'hôte, reportez-vous au *Guide API RESTful OpenManage Enterprise*.
      - Sélectionnez **Utiliser l'option SUDO** si nécessaire.
5. Cliquez sur **Terminer**.
6. Exécutez les tâches dans Création d'une tâche de détection de périphérique , page 44.

Spécification du mode détection pour créer une tâche de détection de stockage Dell

1. Dans le menu déroulant **Types d'appareil**, sélectionnez **STOCKAGE DELL**.
2. Lorsque vous y êtes invité, sélectionnez :
   - PowerVault ME : pour détecter les appareils de stockage utilisant le protocole HTTPS, tels que le PowerVault ME.
   - Autres : pour détecter les appareils de stockage utilisant le protocole SNMP.

   En fonction de votre sélection, les champs changent sous **Paramètres**.
3. Saisissez l'adresse IP, le nom d'hôte ou la plage d'adresses IP dans **IP/Nom d'hôte/Plage**.
4. Sous **Paramètres**, en fonction de votre sélection initiale : saisissez le **Nom d'utilisateur** et le **Mot de passe** pour le stockage HTTPS ou saisissez la **version SNMP** et le **type de communauté** de l'appareil à détecter.

5. Cliquez sur **Paramètres supplémentaires** pour personnaliser le protocole de détection correspondant. Consultez Création de modèle de tâche personnalisée de détection d'appareils pour les appareils SNMP ou Création de protocole HTTPS de tâche de détection d'appareils personnalisé pour les périphériques de stockage : paramètres supplémentaires pour les protocoles de détection , page 53.
6. Exécutez les tâches dans Création d'une tâche de détection de périphérique , page 44.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Spécification du mode de détection pour créer une tâche de détection de commutateur de réseau

1. Dans le menu déroulant **Types d'appareils**, sélectionnez **COMMUTATEUR RÉSEAU**.
2. Saisissez l'adresse IP, le nom d'hôte ou la plage d'adresses IP dans **IP/Nom d'hôte/Plage**.
3. Dans la section **Paramètres**, saisissez la **version SNMP** et le **type de communauté** de l'appareil à détecter.
4. Cliquez sur **Paramètres supplémentaires** pour personnaliser le protocole de détection correspondant. Consultez Création de modèle de tâche personnalisée de détection d'appareils pour les appareils SNMP
5. Exécutez les tâches dans Création d'une tâche de détection de périphérique , page 44.

Création de protocole HTTPS de tâche de détection d'appareils personnalisé pour les périphériques de stockage : paramètres supplémentaires pour les protocoles de détection

Dans la boîte de dialogue **Paramètres supplémentaires** :

1. Saisissez le nom d'utilisateur et le mot de passe du PowerVault ME à détecter.
2. Dans la section **Paramètres de connexion** :
   a. Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
   b. Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.
   c. Dans la zone **Port**, indiquez le numéro de port. Par défaut, le port 443 est utilisé pour se connecter au périphérique. Pour connaître les numéros de port pris en charge, voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
   d. Sélectionnez la case **Activer le nom commun (CN)** si le nom commun du périphérique est identique au nom d'hôte utilisé pour accéder à OpenManage Enterprise.
   e. Cochez la case **Activer la vérification d'autorité de certification (CA)**.
3. Cliquez sur **Terminer**.
4. Exécutez les tâches dans Création d'une tâche de détection de périphérique , page 44.

Création de modèle de tâche personnalisée de détection de périphériques pour des périphériques SNMP

Par défaut, la case **Détection à l'aide de SNMP** est cochée pour vous permettre de détecter les périphériques de stockage, de mise en réseau, ou d'autres périphériques SNMP.

REMARQUE : Seuls les modules d'E/S en mode Autonome, PMUX (MUX programmable) et VLT (Jonction de liaisons virtuelles) peuvent être détectés. Les modules en mode Commutateur entier et Empilé ne seront pas détectés.

1. Sous **Informations d'identification**, sélectionnez la version SNMP, puis saisissez le type de communauté.
2. Dans la section **Paramètres de connexion** :
   a. Dans le champ **Nouvelles tentatives**, saisissez le nombre de tentatives répétées à réaliser pour détecter un serveur.
   b. Dans le champ **Délai d'expiration**, saisissez la durée au bout de laquelle une tâche doit cesser de s'exécuter.

c. Dans le champ **Port**, saisissez le numéro de port utilisé par la tâche pour exécuter la détection.

REMARQUE : Actuellement, les paramètres du **champ nouvelles tentatives** et du **champ délai d'expiration** n'ont pas d'impact fonctionnel sur les tâches de détection pour les périphériques SNMP. Par conséquent, ces paramètres peuvent être ignorés.

3. Cliquez sur **Terminer**.
4. Exécutez les tâches dans Création d'une tâche de détection de périphérique , page 44.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Spécification du mode de détection pour créer une tâche de détection MULTIPLE

1. Dans le menu déroulant **Type**, sélectionnez **MULTIPLE** pour détecter des périphériques à l'aide de plusieurs protocoles.
2. Saisissez l'adresse IP, le nom d'hôte ou la plage d'adresses IP dans **IP/Nom d'hôte/Plage**.
3. Pour créer un modèle de détection personnalisé en cliquant sur **Paramètres supplémentaires**, voir Création de protocole de tâche de détection d'appareils personnalisé pour les serveurs : paramètres supplémentaires pour les protocoles de détection , page 50.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

Suppression d'une tâche de détection de périphérique

REMARQUE : Un périphérique peut être supprimé même lorsque des tâches sont en cours d'exécution sur celui-ci. Si un périphérique est supprimé avant qu'une tâche en cours se termine, la tâche échoue.

Pour supprimer une tâche de détection de périphérique, procédez comme suit :

1. Cochez la case en regard de la tâche de détection à supprimer et cliquez sur **Supprimer**.
2. Lorsque vous êtes invité à indiquer si la tâche doit être supprimée, cliquez sur **OUI**.
   Les tâches de détection sont supprimées et un message s'affiche dans l'angle inférieur droit de l'écran.

REMARQUE : Si vous supprimez une tâche de détection, les périphériques associés à la tâche ne sont pas supprimés. Si vous voulez que les périphériques détectés par une tâche de détection soient retirés de la console, alors supprimez-les de la page **Tous les périphériques**.

REMARQUE : Une tâche de détection de périphérique ne peut pas être supprimée à partir de la page **Tâches**.

Information associée

Détection de périphériques pour la surveillance ou la gestion , page 41

8

Gestion des périphériques et des groupes de périphériques

En cliquant sur **OpenManage Enterprise** > **Périphériques**, vous pouvez afficher et gérer les groupes de périphériques et les périphériques découverts dans OpenManage Enterprise. Si vous êtes connecté en tant que gestionnaire de périphériques, seuls les groupes de périphériques et les arborescences associées qui se trouvent dans votre périmètre seront disponibles pour l'affichage et la gestion.

Le volet de gauche affiche les groupes de périphériques comme suit :

- Tous les périphériques : groupe racine de premier niveau contenant tous les groupes.
- Groupes du système : groupes par défaut créés par OpenManage Enterprise lors de l'expédition.
- Groupes personnalisés : groupes créés par des utilisateurs tels que les administrateurs et les gestionnaires de périphériques. vous pouvez créer des groupes « requête » ou « statiques » sous les groupes personnalisés.
- Groupes de plug-ins : groupes créés par des plug-ins.

Vous pouvez créer des groupes enfants sous ces groupes parents. Pour plus d'informations, reportez-vous à la section Groupes de périphériques.

Dans la partie supérieure du volet en cours, les graphiques circulaires affichent l'état de santé et les alertes de tous les périphériques par défaut. Toutefois, lorsqu'un groupe est sélectionné dans le volet de gauche, ces graphiques circulaires affichent l'état de santé et les alertes du groupe sélectionné. En outre, si un plug-in est installé, un troisième graphique circulaire peut afficher les données du plug-in installé. Pour plus d'informations sur le graphique circulaire, voir Graphique circulaire.

Le tableau après le graphique circulaire répertorie les périphériques et affiche l'état de santé, l'état de l'alimentation, le nom, l'adresse IP et l'ID. Par défaut, tous les périphériques sont répertoriés. Toutefois, lorsqu'un groupe est sélectionné dans le volet de gauche, seuls les périphériques de ce groupe s'affichent. Pour plus d'informations sur la liste des périphériques, voir Liste des périphériques.

Les **filtres avancés** peuvent être utilisés pour réduire davantage les périphériques affichés dans la liste des périphériques en fonction de leur état de santé, de l'état de l'alimentation, de l'état de la connexion, du nom, de l'adresse IP, de l'ID, du type de périphérique, de l'état géré, etc.

Lorsque vous sélectionnez un périphérique dans la liste, le volet de droite affiche l'aperçu des périphériques sélectionnés. Lorsque plusieurs périphériques sont sélectionnés, l'aperçu du dernier périphérique sélectionné s'affiche. Sous **Actions rapides**, les liens de gestion mis en corrélation avec l'appareil correspondant sont répertoriés. Pour effacer les sélections, cliquez sur **Effacer la sélection**.

REMARQUE :

- Après la mise à niveau d'OpenManage Enterprise vers la dernière version, la liste des périphériques sera mise à jour après la réexécution des tâches de découverte.
- Vous pouvez sélectionner un maximum de 25 périphériques par page et naviguer dans les pages pour sélectionner plusieurs périphériques et effectuer des tâches.
- Certaines des tâches liées aux périphériques que vous pouvez effectuer sur la page Tous les périphériques (telles que la mise à jour de firmware, l'actualisation de l'inventaire, l'actualisation de l'état, des actions de contrôle du serveur) peuvent également être effectuées sur les périphériques individuels depuis la page **Détails du périphérique** respective.

Sujets :

Organisation des périphériques dans des groupes

Dans un datacenter, pour gérer les périphériques de manière rapide et efficace, vous pouvez :

- Grouper les périphériques. Par exemple, vous pouvez grouper les périphériques selon leurs fonctions, systèmes d'exploitation, profils utilisateur ou emplacements, puis exécuter des requêtes pour gérer les périphériques.
- Filtrer les données relatives au périphérique lorsque vous procédez à la gestion des périphériques, à la mise à jour de firmware, à la détection des périphériques et à la gestion des stratégies et des rapports d'alerte.
- Vous pouvez gérer les propriétés d'un périphérique dans un groupe. Voir Affichage et configuration des périphériques individuels , page 68.

L'application OpenManage Enterprise fournit un rapport intégré qui présente les périphériques qu'elle surveille. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport de présentation des périphériques**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Pour afficher les données du tableau de bord concernant les périphériques ou groupes sélectionnés, effectuez une sélection dans le menu déroulant **Groupes de périphériques**.

REMARQUE : L'état d'intégrité d'un périphérique ou d'un groupe est indiqué par des symboles appropriés. L'état d'intégrité d'un groupe représente l'état d'un périphérique dans un groupe dont l'état d'intégrité est le plus critique. Par exemple, parmi les nombreux périphériques compris dans un groupe, si l'intégrité d'un serveur est définie sur Avertissement, alors l'intégrité du groupe est également définie sur Avertissement. L'état cumulé équivaut à l'état du périphérique qui présente un niveau élevé de gravité. Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc technique *Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération* disponible sur le Dell TechCenter.

Les groupes peuvent posséder un groupe parent et enfant. Un groupe ne peut pas définir ses groupes parents en tant que groupe enfant. Par défaut, OpenManage Enterprise comprend les groupes intégrés suivants.

Groupes du système : groupes par défaut créés par OpenManage Enterprise. Vous ne pouvez pas modifier ou supprimer un Groupe du système, mais vous pouvez l'afficher en fonction des privilèges dont vous disposez. Exemples de Groupes du système :

- **Appliances HCI** : périphériques hyper-convergents tels que les périphériques Dell EMC série XC et VxRAIL
- **Systèmes Hyperviseur** : serveurs Hyper-V et serveurs VMware ESXi
- **Systèmes modulaires** : châssis PowerEdge, PowerEdge FX2, châssis PowerEdge 1000e, châssis PowerEdge MX7000 et châssis PowerEdge VRTX.

  REMARQUE : Un châssis MX7000 peut être un châssis maître, autonome ou membre. Si un châssis MX7000 est un châssis maître et possède un châssis membre, ce dernier est détecté à l'aide de l'IP de son châssis maître. Un châssis MX7000 est identifié à l'aide de l'une des syntaxes suivantes :

  - **Groupe MCM** : indique le groupe de gestion multi-châssis (MCM) qui possède plusieurs châssis identifiés par la syntaxe suivante : `Group_<MCM group name>_<Lead_Chassis_Svctag>` où :
    - `<MCM group name>` : nom du groupe MCM
    - `<Lead_Chassis_Svctag>` : numéro de série du châssis maître. Le châssis, les traîneaux et les IOM de réseau forment ce groupe.
  - **Groupe de châssis autonomes** : identifié à l'aide de la syntaxe `<Chassis_Svctag>`. Le châssis, les traîneaux et les IOM de réseau forment ce groupe.
- **Périphériques réseau** : commutateurs de mise en réseau Dell Force10 et commutateurs Fibre Channel
- **Serveurs** : serveurs Dell iDRAC, serveurs Linux, serveurs autres que Dell, serveurs OEM et serveurs Windows.
- **Périphériques de stockage** : baies de stockage Dell Compellent, baies de stockage PowerVault MD et baies de stockage PowerVault ME
- **Groupes de détection** : groupes qui sont mappés sur la plage d'une tâche de détection. Le groupe ne peut pas être modifié ou supprimé, car il est contrôlé par la tâche de détection appliquant la condition inclure/exclure. Voir Détection de périphériques pour la surveillance ou la gestion , page 41.

REMARQUE : Pour développer tous les sous-groupes d'un groupe, effectuez un clic droit sur le groupe, puis cliquez sur **Développer tout**.

Groupes personnalisés : créés par les administrateurs pour des besoins spécifiques. Par exemple, les serveurs hébergeant les services de messagerie sont groupés. Les utilisateurs peuvent les afficher, les modifier et les supprimer en fonction des privilèges dont ils disposent et des types de groupes.

- **Groupes statiques** : créés manuellement par l'utilisateur en ajoutant des périphériques spécifiques dans un groupe. Ces groupes changent uniquement lorsqu'un utilisateur modifie manuellement les périphériques du groupe ou d'un sous-groupe. Les éléments du groupe restent statiques jusqu'à ce que le groupe parent soit modifié ou que le périphérique enfant soit supprimé.

- **Groupes de requête** : groupes définis de manière dynamique par le biais d'une correspondance entre les critères spécifiés par l'utilisateur. Les périphériques du groupe varient en fonction du résultat des périphériques détectés en fonction de la correspondance des critères. Par exemple, une requête est exécutée pour détecter les serveurs affectés au service financier. Cependant, les Groupes de requête possèdent une structure plate sans aucune hiérarchie.

REMARQUE : Groupes statiques et de requête :

- Ne peuvent pas posséder plus d'un groupe parent. Cela signifie qu'un groupe ne peut pas être ajouté en tant que sous-groupe dans son groupe parent.
- Lorsque des modifications sont apportées à un groupe statique (ajout ou suppression de périphériques) ou à un groupe de requêtes (lorsqu'une requête est mise à jour), la conformité du firmware/pilote des périphériques associés à ces groupes n'est pas actualisée automatiquement. Il est recommandé à l'utilisateur d'activer la conformité du firmware et/ou du pilote pour les périphériques nouvellement ajoutés/supprimés dans de telles instances.

REMARQUE : La création de Groupes personnalisés (de requête) supplémentaires dans la hiérarchie du groupe de périphériques impacte la performance globale d'OpenManage Enterprise. Pour une performance optimisée, OpenManage Enterprise capture l'état d'intégrité cumulé toutes les 10 secondes ; la présence d'un plus grand nombre de Groupes dynamiques affecte cette performance.

Sur la page **Tous les périphériques**, dans le volet de gauche, vous pouvez créer des groupes enfants dans le groupe parent statique ou de requête. Voir Création d'un groupe de périphériques statique , page 58 et Création d'un groupe de périphériques de requête , page 58.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Pour supprimer le groupe enfant d'un groupe statique ou de requête :

1. Cliquez avec le bouton droit sur le groupe statique ou de requête, puis cliquez sur **Supprimer**.
2. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**. Le groupe est supprimé et la liste dans le groupe est mise à jour.

Groupes de plug-ins : les groupes de plug-ins sont créés lorsque des plug-ins tels que Services et Power Manager sont installés. Les plug-ins, lorsqu'ils sont installés, ont leurs propres groupes de systèmes, et certains plug-ins, tels que le plug-in Power Manager, permettent à l'utilisateur de créer des groupes personnalisés à l'intérieur.

Tâches associées

Suppression de périphériques d'OpenManage Enterprise , page 64
Actualiser l'inventaire des appareils d'un seul appareil , page 72
Actualisation de l'intégrité du périphérique d'un groupe de périphériques , page 66

Création d'un groupe personnalisé (statique ou requête)

Dans **OpenManage Enterprise** > **Périphériques** (page Tous les périphériques), vous pouvez créer des groupes statiques ou de requête à l'aide de l'Assistant de création d'un groupe personnalisé.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

1. Pour activer l'Assistant de création d'un groupe personnalisé, vous pouvez procéder comme suit :
   - Dans les GROUPES PERSONNALISÉS du volet de gauche **OpenManage Enterprise** > **Périphériques**, cliquez avec le bouton droit ou cliquez sur le menu de trois points verticaux, puis cliquez sur **Créer un groupe personnalisé.**
   - À partir de la page Tous les périphériques, menu déroulant **Actions de groupe**, cliquez sur **Créer un groupe personnalisé**.
2. Dans l'Assistant de création du groupe personnalisé, sélectionnez l'un des groupes personnalisés suivants :
   a. **Groupe statique**.
   b. **Groupe de requête**
3. Cliquez sur **Créer**.
   En fonction de votre sélection (statique ou requête), l'Assistant de création du groupe statique ou l'Assistant de création du groupe de requête est activé.

Une fois qu'un groupe (statique ou requête) est créé, il est répertorié sous le GROUPE PERSONNALISÉ, les groupes statiques ou de requêtes.

Création d'un groupe de périphériques statique

Dans la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), vous pouvez créer des groupes statiques en utilisant l'Assistant de création du groupe statique. Les périphériques d'un groupe statique restent statiques jusqu'à ce que les périphériques du groupe soient ajoutés ou supprimés.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Pour activer l'Assistant de création du groupe statique, procédez comme suit :
   - Sous GROUPES PERSONNALISÉS, **Groupes statiques**, cliquez avec le bouton droit ou cliquez sur le menu de trois points verticaux, puis cliquez sur **Créer un nouveau groupe statique**.
   - Cliquez sur **Actions de groupe** > **Créer un groupe personnalisé** > **Groupe statique**.
2. Dans la boîte de dialogue **Assistant de création du groupe statique**, saisissez le nom et la description (facultatif) du groupe, puis sélectionnez un groupe parent sous lequel le nouveau groupe statique doit être créé.

   REMARQUE : Dans OpenManage Enterprise, les noms de groupes statiques ou dynamiques et les noms relatifs à la configuration du serveur doivent être uniques (non sensibles à la casse). Par exemple, *nom1* et *Nom1* ne peuvent pas être utilisés en même temps.
3. Cliquez sur **Suivant**.
4. Dans la boîte de dialogue Sélection de membres du groupe, sélectionnez les périphériques qui doivent être inclus dans le groupe statique.
5. Cliquez sur **Terminer**.

Le groupe statique est créé et répertorié sous le groupe parent dans le volet de gauche. Les groupes enfants s'affichent en retrait de leur groupe parent.

Création d'un groupe de périphériques de requête

Les groupes de requêtes sont des groupes dynamiques dont les périphériques sont définis par correspondance avec certains critères spécifiés par l'utilisateur. Les périphériques du groupe varient selon le résultat des périphériques détectés en fonction des critères de la requête. Sur la page Tous les périphériques (**OpenManage Enterprise** > **Devices**), vous pouvez créer des groupes de requêtes à l'aide de l'Assistant de création du groupe de requête.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Pour activer l'Assistant de création du groupe de requête, vous pouvez effectuer l'une des opérations suivantes :
   - Sous Groupes personnalisés, cliquez avec le bouton droit de la souris sur **Groupes de requêtes** ou cliquez sur le menu de trois points verticaux en regard des groupes de requêtes, puis cliquez sur **Créer un groupe de requête**.
   - Cliquez sur **Actions de groupe** > **Créer un groupe personnalisé** > **Groupe de requête**.
2. Dans la boîte de dialogue **Assistant de création du groupe de requête**, saisissez un **nom** et une **description** (facultatif) pour le groupe.
3. Cliquez sur **Suivant**.
4. Dans le menu déroulant **Sélectionner une requête existante à copier** de la boîte de dialogue **Sélection de critères de requête**, sélectionnez une requête, puis choisissez les autres critères de filtre. Voir Sélection d'un critère de requête , page 58.
5. Cliquez sur **Terminer**.
   Le groupe de requête est créé et répertorié sous la section Groupe de requête dans le volet de gauche.

Sélection d'un critère de requête

Définissez des filtres lorsque vous créez des critères de requête pour :

- Générer des rapports personnalisés. Voir Création de rapports , page 142.
- Créer des groupes de périphériques basés sur des requêtes sous GROUPES PERSONNALISÉS. Voir Création d'un groupe de périphériques de requête , page 58.

Pour définir un critère de requête, utilisez deux options :

- **Sélectionner une requête existante à copier** : par défaut, OpenManage Enterprise intègre une liste de modèles de requête que vous pouvez copier pour créer votre propre critère de requête. Vous pouvez utiliser au maximum 6 critères (filtres) lors de la définition d'une requête. Pour ajouter des filtres, sélectionnez des éléments dans le menu déroulant **Sélectionner un type**.
- **Sélectionner un type** : pour créer un critère de requête, utilisez les attributs répertoriés dans ce menu déroulant. Les éléments présents dans le menu dépendent des périphériques surveillés par OpenManage Enterprise. Lorsqu'un type de requête est sélectionné, seuls les opérateurs appropriés s'affichent, tels que =, >, < et null, en fonction du type de requête. Cette méthode est recommandée pour la définition des critères de requête lors de la création de rapports personnalisés.

  REMARQUE : Lorsque vous évaluez une requête avec plusieurs conditions, l'ordre d'évaluation est identique à celui de SQL. Pour spécifier un ordre particulier pour l'évaluation des conditions, ajoutez ou supprimez des parenthèses lors de la définition la requête.

REMARQUE : Une fois sélectionnés, les filtres d'un critère de requête existant sont uniquement copiés virtuellement pour créer un nouveau critère de requête. Les filtres par défaut associés à un critère de requête existant ne sont pas modifiés. Les filtres définis d'un critère de requête intégré sont utilisés comme point de départ pour la construction d'un critère de requête personnalisé. Par exemple :

1. *Requête1* est un critère de requête intégré composé du filtre prédéfini suivant : `Task Enabled=Yes`.
2. Pour copier les propriétés du filtre de *Requête1*, créer *Requête2*, puis personnaliser le critère de requête, ajoutez un autre filtre : `Task Enabled=Yes` ET `(Task Type=Discovery)`.
3. Ensuite, ouvrez *Requête1*. Son critère de filtre reste `Task Enabled=Yes`.

1. Dans la boîte de dialogue **Sélection de critères de requête**, sélectionnez des éléments du menu déroulant selon que vous souhaitez créer un critère de requête pour générer des groupes de requêtes ou des rapports.
2. Pour ajouter ou supprimer un filtre, cliquez respectivement sur le symbole plus ou sur la corbeille.
3. Cliquez sur **Terminer**.
   Un critère de requête est généré et sauvegardé dans la liste des requêtes existantes. Une entrée est créée dans le journal d'audit et s'affiche dans la liste des journaux d'audit. Voir Surveillance des journaux d'audit , page 127.

Information associée

Gestion de la conformité de la configuration du périphérique , page 110
Modification d'une ligne de base de conformité de la configuration , page 114
Suppression d'une ligne de base de conformité de la configuration , page 116

Modification d'un groupe statique

Dans la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**) les groupes statiques existants peuvent être renommés, repositionnés et les périphériques du groupe statique peuvent être ajoutés ou supprimés à l'aide de l'Assistant de modification du groupe statique.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Cliquez avec le bouton droit de la souris sur le groupe statique ou cliquez sur le menu de trois points verticaux en regard du groupe statique, puis cliquez sur **Modifier** pour activer l'Assistant de modification du groupe statique.
2. Dans l'Assistant de modification du groupe statique, vous pouvez modifier le nom, la description et le groupe parent.
3. Cliquez sur **Suivant**.
4. Dans l'écran Sélection des membres du groupe, vous pouvez cocher ou décocher les périphériques à ajouter ou exclure du groupe statique.
5. Cliquez sur **Terminer**.

Les modifications apportées au groupe statique sont implémentées.

Modification d'un groupe de requête

Sur la page Tous les périphériques (**OpenManage Enterprise** > **Tous les périphériques**), le groupe de requête existant peut être renommé, repositionné et les critères de requête à partir desquels les périphériques sont inclus dans le groupe de requête peuvent être modifiés à l'aide de l'Assistant Modifier le groupe de requête.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Sous GROUPES PERSONNALISÉS, cliquez avec le bouton droit de la souris sur le groupe de requête ou cliquez sur le menu de trois points verticaux en regard du groupe de requête, puis cliquez sur **Modifier**.
2. Dans l'Assistant Modifier le groupe de requête, modifiez le nom et la description en fonction de vos besoins.
3. Cliquez sur **Suivant**.
4. Dans le menu déroulant **Sélectionner une requête existante à copier** de la boîte de dialogue Sélection de critères de requête, sélectionnez une requête, puis choisissez les autres critères de filtre.
5. Cliquez sur **Terminer**.

Les modifications apportées au groupe de requête sont implémentées.

Attribution d'un nouveau nom à un groupe statique ou de requête

Pour renommer un groupe statique ou de requête sur la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**) :

1. Sous **GROUPES PERSONNALISÉS**, cliquez avec le bouton droit de la souris sur un groupe statique ou de requête, ou cliquez sur les trois points en regard du groupe que vous souhaitez renommer, puis sur **Renommer**. Ou sélectionnez un groupe, puis cliquez sur **Actions de groupe** > **Renommer le groupe**.
2. Dans la boîte de dialogue **Renommer le groupe**, saisissez le nouveau nom du groupe.
3. Cliquez sur **Terminer**.
   Le nom mis à jour est répertorié dans le volet de gauche.

Suppression d'un groupe de périphériques statique ou de requête

Sur la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), vous pouvez supprimer un groupe statique ou de requête existant comme suit :

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Cette procédure s'applique uniquement à la suppression d'un groupe statique ou de requête, mais les périphériques du groupe ne sont pas supprimés de la page Tous les périphériques. Pour supprimer des périphériques d'OpenManage Enterprise, reportez-vous à la section Suppression de périphériques d'OpenManage Enterprise , page 64.

1. Sous **GROUPES PERSONNALISÉS**, cliquez avec le bouton droit de la souris sur un groupe statique ou de requête, ou cliquez sur le menu de trois points verticaux en regard du groupe, puis cliquez sur **Supprimer**. OU sélectionnez le groupe que vous souhaitez supprimer, puis dans le menu déroulant **Actions de groupe** cliquez sur **Supprimer le groupe**.
2. Lorsque le programme vous invite à confirmer, cliquez sur **Oui**.

Le groupe est supprimé des GROUPES PERSONNALISÉS.

Clonage d'un groupe statique ou de requête

Les groupes statiques ou de requête existants peuvent être clonés et ajoutés aux GROUPES PERSONNALISÉS.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

1. Cliquez avec le bouton droit de la souris sur le groupe statique ou de requête, ou cliquez sur le menu vertical de trois points en regard du groupe statique ou de requête, puis cliquez sur **Cloner**.
2. Dans la boîte de dialogue **Cloner le groupe**, saisissez un nom et une description pour le groupe. En outre, pour le groupe statique, sélectionnez le groupe parent sous lequel le clone statique doit être créé.
3. Cliquez sur **Terminer**.
   Le groupe cloné est créé et répertorié sous le groupe parent dans le volet de gauche.

Ajout de périphériques à un nouveau groupe

Vous pouvez créer un nouveau groupe et y ajouter des périphériques à partir du tableau répertoriant les périphériques disponibles sur la page Tous les périphériques.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Dans le menu **OpenManage Enterprise**, cliquez sur **Périphériques**.
   La page Tous les périphériques s'affiche.
2. Dans la liste des périphériques, cochez la case correspondant au(x) périphérique(s), puis cliquez sur **Actions de groupe** > **Ajouter au nouveau groupe**.
   a. Dans la boîte de dialogue **Assistant Ajouter des périphériques au nouveau groupe**, saisissez le **nom**, la **description** (facultatif), puis sélectionnez le **groupe parent** sous lequel le nouveau groupe enfant sera créé. Pour plus d'informations sur les groupes, voir Groupes de périphériques.
   b. Pour ajouter d'autres périphériques au groupe, cliquez sur **Suivant**. Sinon, passez à l'étape 3.
3. Dans la boîte de dialogue **Sélection des membres du groupe**, sélectionnez d'autres périphériques dans la liste **Ajouter des périphériques**.
   Après avoir sélectionné les périphériques dans l'onglet **Tous les périphériques**, les périphériques sélectionnés sont répertoriés dans **Tous les périphériques sélectionnés**.
4. Cliquez sur **Terminer**.
   Un nouveau groupe est créé et les périphériques sont ajoutés au groupe sélectionné.
   REMARQUE : Pour créer des groupes ou ajouter des périphériques à un groupe, vous devez suivre la relation parent-enfant des groupes. Voir Groupes de périphériques.

Ajout de périphériques à un groupe existant

Vous pouvez ajouter des périphériques à un groupe existant à partir du tableau répertoriant les périphériques disponibles sur la page Tous les périphériques.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Dans le menu **OpenManage Enterprise**, cliquez sur **Périphériques**.
   La page Tous les périphériques s'affiche.
2. Dans la liste des périphériques, cochez la case correspondant au(x) périphérique(s), puis cliquez sur **Actions de groupe** > **Ajouter à un groupe existant**.
3. Dans la boîte de dialogue **Ajouter les périphériques sélectionnés à un groupe existant**, saisissez ou sélectionnez des données. Pour plus d'informations sur les groupes, voir Groupes de périphériques.
4. Cliquez sur **Terminer**.
   Les périphériques sont ajoutés au groupe existant sélectionné.
   REMARQUE : Pour créer des groupes ou ajouter des périphériques à un groupe, vous devez suivre la relation parent-enfant des groupes. Voir Groupes de périphériques.

Actualisation de l'intégrité sur le groupe

Les étapes suivantes décrivent la façon dont vous pouvez actualiser l'intégrité et l'état en ligne d'un groupe sélectionné.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Pour les appareils intrabande découverts à l'aide d'ESXi et des systèmes d'exploitation Linux, l'état d'intégrité ( ) s'affiche comme étant inconnu ( ).

1. Accédez à la page Tous les périphériques en cliquant sur **OpenManage Enterprise** > **Périphériques**.

2. Dans le volet de gauche, sélectionnez le groupe sur lequel vous souhaitez actualiser l'intégrité.
   Après la sélection du groupe, la liste des périphériques répertorie les périphériques du groupe sélectionné.
3. Cliquez sur le menu déroulant **Actualiser l'intégrité**, puis cliquez sur **Actualiser l'intégrité sur le groupe**. L'Assistant d'intégrité s'affiche.
4. Dans l'Assistant d'intégrité, le **Nom de la tâche** affiche le nom de tâche généré par l'appliance pour la tâche d'actualisation de l'intégrité. Si nécessaire, vous pouvez modifier le nom de la tâche.
5. Le menu déroulant **Sélectionner un groupe** affiche le groupe que vous avez sélectionné.
6. Dans le menu déroulant Planification, vous pouvez sélectionner l'une des options suivantes :
   a. **Exécuter maintenant** : permet d'exécuter immédiatement l'option Actualiser l'intégrité sur le groupe sélectionné.
   b. **Exécuter plus tard** : vous pouvez sélectionner Exécuter plus tard, puis sélectionner la date et l'heure d'exécution de la tâche Actualiser l'intégrité sur le groupe.
   c. **Exécuter selon la planification** : vous pouvez sélectionner cette option, puis choisir la fréquence quotidienne ou hebdomadaire, et sélectionner une heure si vous voulez actualiser l'intégrité du groupe sur une base quotidienne ou hebdomadaire à une heure donnée.

Une tâche permettant d'actualiser l'intégrité et l'état en ligne du groupe est créée. Vous pouvez afficher les détails de la tâche sur la page Tâches (**OpenManage Enterprise** > **Surveiller** > **Tâches**).

Liste des périphériques

La liste des périphériques affiche les propriétés des périphériques telles que leur adresse IP et leur numéro de série. Vous pouvez sélectionner un maximum de 25 périphériques par page et naviguer dans les pages pour sélectionner plusieurs périphériques et effectuer des tâches. Pour plus d'informations sur les tâches que vous pouvez réaliser sur la page Tous les périphériques, voir Page tous les périphériques : actions de la liste de périphériques , page 63.

REMARQUE : Par défaut, la liste des périphériques affiche tous les périphériques pris en compte lors de la génération du graphique circulaire. Pour afficher une liste des périphériques relevant d'un état d'intégrité spécifique, cliquez sur la bande de couleur correspondante dans le graphique circulaire, ou cliquez sur le symbole d'état d'intégrité. Les périphériques qui appartiennent uniquement à la catégorie sélectionnée sont répertoriés.

- **État d'intégrité** indique l'état de fonctionnement du périphérique. Les états d'intégrité (Normal, Critique et Avertissement) sont identifiés par des symboles de couleur. Voir États d'intégrité du périphérique , page 40
- **État d'alimentation** indique si le périphérique est sous tension ou hors tension.
- L'**État de la connexion** indique l'état de la connexion des périphériques détectés pour OpenManage Enterprise en tant que : Connecté, Déconnecté ou Déconnecté (Échec de l'authentification)
- **Nom** indique le nom du périphérique.
- **Adresse IP** indique l'adresse IP de l'iDRAC installé sur le périphérique.
- **ID** indique le numéro de série du périphérique.
- **Modèle** indique le numéro de modèle.
- **Type** indique le type de périphérique (Serveur, Châssis, Solution de stockage Dell et Commutateur de mise en réseau).
- **Nom du châssis** indique le nom du châssis.
- **Nom du logement** indique le nom du logement pour les périphériques de châssis.
- La colonne **État géré** indique si le périphérique est surveillé, géré ou proxy. Voir Détection de périphériques pour la surveillance ou la gestion , page 41.

Pour filtrer des données du tableau, cliquez sur **Filtres avancés** ou sur le symbole Filtre. Pour exporter des données au format de fichier HTML, CSV ou PDF, cliquez sur le symbole Exporter dans le coin supérieur droit.

REMARQUE : Dans la liste des périphériques, cliquez sur le nom ou l'adresse IP du périphérique pour afficher ses données de configuration, puis sur modifier. Voir Affichage et configuration des périphériques individuels , page 68.

REMARQUE : Le volet actuel affiche le graphique circulaire du groupe de périphériques sélectionné. À l'aide du graphique circulaire, vous pouvez afficher la liste de périphériques qui appartiennent à d'autres états d'intégrité dans ce groupe. Pour afficher les périphériques d'autres états d'intégrité, cliquez sur la couleur correspondante du graphique circulaire. Les données dans le tableau changent. Pour plus d'informations sur l'utilisation du graphique circulaire, voir la rubrique Graphique circulaire.

Page tous les périphériques : actions de la liste de périphériques

Sur la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**) vous pouvez réaliser diverses actions sur les périphériques.

Les boutons d'action sont contextuels à la sélection de groupe dans l'arborescence sur la gauche ainsi qu'aux appareils sélectionnés dans la grille. Par conséquent, si l'action est associée au groupe (par exemple des actions de groupe telles que l'exécution de l'inventaire sur le groupe et l'actualisation de l'intégrité du groupe), par défaut le groupe sélectionné est utilisé. Toutes les actions de périphérique concernent par défaut les périphériques sélectionnés. Toutefois, quelques actions, telles que la détection, sont toujours applicables sans aucune sélection. En outre, le type d'actions disponibles par périphérique dépend du type de périphérique sélectionné.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

- Dans le menu déroulant **Actions de groupe**, vous pouvez effectuer les opérations suivantes :
  - Créer des groupes de périphériques personnalisés. Voir Création d'un groupe personnalisé (statique ou requête) , page 57.
  - Créer des groupes statiques. Voir Création d'un groupe de périphériques statique , page 58.
  - Créer des groupes de requêtes. Voir Création d'un groupe de périphériques de requête , page 58
  - Modifier les groupes statiques ou de requête. Voir Modification d'un groupe statique , page 59 et Modification d'un groupe de requête , page 59.
  - Cloner des groupes. Voir Clonage d'un groupe statique ou de requête , page 60.
  - Renommer le groupe. Voir Attribution d'un nouveau nom à un groupe statique ou de requête , page 60.
  - Supprimer des groupes. Voir Suppression d'un groupe de périphériques statique ou de requête , page 60.
  - Ajouter des périphériques à un nouveau groupe. Voir Ajout de périphériques à un nouveau groupe , page 61.
  - Ajouter des périphériques à un groupe existant. Voir Ajout de périphériques à un groupe existant , page 61.
- Dans le menu déroulant **Détection**, vous pouvez effectuer les opérations suivantes :
  - Détecter et intégrer des périphériques. Voir Détection de périphériques pour la surveillance ou la gestion , page 41 et Intégration de périphériques , page 45.
  - Exclure les périphériques. Voir Exclusion de périphériques d'OpenManage Enterprise , page 64.
  - Modifier les plages d'exclusion. Voir Exclusion globale des plages , page 49.
- Dans le menu déroulant **Inventaire**, vous pouvez effectuer les opérations suivantes :
  - Exécuter l'inventaire sur un groupe de périphériques. Reportez-vous à la section Créer et exécuter une tâche d'inventaire.
  - Exécuter l'inventaire sur les périphériques. Voir Exécution de l'inventaire sur les périphériques , page 64.
- Dans le menu déroulant **Actualiser l'intégrité**, vous pouvez effectuer les opérations suivantes :
  - Actualiser l'intégrité sur le groupe. Voir Actualisation de l'intégrité sur le groupe , page 61.
  - Actualiser l'intégrité sur les périphériques. Voir Actualisation de l'intégrité sur les périphériques , page 66.
- Dans le menu déroulant **Plus d'actions**, vous pouvez effectuer les opérations suivantes :
  - Allumer la LED. Voir Création d'une tâche pour activer les voyants de périphérique , page 133.
  - Désactiver la LED. Voir Création d'une tâche pour activer les voyants de périphérique , page 133.
  - Mettre sous tension le(s) périphérique(s). Voir Création d'une tâche pour gérer les périphériques d'alimentation , page 134.
  - Mettre hors tension le(s) périphérique(s). Voir Création d'une tâche pour gérer les périphériques d'alimentation , page 134.
  - Faire un arrêt normal du ou des périphériques. Voir Création d'une tâche pour gérer les périphériques d'alimentation , page 134.
  - Exécuter un cycle d'alimentation du système (démarrage à froid). Voir Création d'une tâche pour gérer les périphériques d'alimentation , page 134.
  - Réinitialiser le système (démarrage à chaud). Voir Création d'une tâche pour gérer les périphériques d'alimentation , page 134.
  - Exécuter la commande à distance CLI IPMI sur un périphérique. Voir Exécution de commandes RACADM et IPMI distantes sur des périphériques individuels , page 72.
  - Exécuter la commande à distance CLI RACADM sur un périphérique. Voir Exécution de commandes RACADM et IPMI distantes sur des périphériques individuels , page 72.
  - Supprimer le(s) périphérique(s) d'OpenManage Enterprise. Voir Suppression de périphériques d'OpenManage Enterprise , page 64.
  - Exporter les données sur tous les périphériques. Voir Exportation de toutes les données ou des données sélectionnées , page 68
  - Exporter les données sur les périphériques sélectionnés. Voir Exportation de toutes les données ou des données sélectionnées , page 68

Suppression de périphériques d'OpenManage Enterprise

Les étapes suivantes expliquent comment supprimer et stocker en externe les périphériques découverts dans OpenManage Enterprise.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Vous ne pouvez pas supprimer un périphérique sur lequel un profil est affecté, à moins d'annuler l'affectation du profil. Pour plus d'informations, voir Annulation de l'attribution de profils , page 108.
- Un périphérique peut être supprimé même lorsque des tâches sont en cours d'exécution sur celui-ci. Les tâches initiées sur un périphérique échouent si le périphérique est supprimé avant la fin de l'exécution de ces tâches.

Pour supprimer les périphériques découverts :

1. Accédez à la page Tous les périphériques en cliquant sur **OpenManage Enterprise** > **Périphériques**.
2. Dans la liste des périphériques, cochez la case correspondant aux périphériques que vous souhaitez supprimer.
3. Cliquez sur le menu déroulant **Plus d'actions**, puis cliquez sur **Supprimer des périphériques**.
4. À l'invite indiquant que les périphériques seront supprimés d'OpenManage Enterprise et stockés en externe, cliquez sur **Oui**.

Les périphériques sélectionnés sont entièrement supprimés d'OpenManage Enterprise. Après la suppression du périphérique, toutes les informations d'intégration propres à ce périphérique sont supprimées. Les informations d'identification de l'utilisateur sont supprimées automatiquement si elles ne sont pas partagées avec d'autres périphériques. Si OpenManage Enterprise a été défini en tant que destination d'interruption sur le périphérique qui a été supprimé, vous devez supprimer l'adresse IP de la console OpenManage Enterprise en tant que destination d'interruption du périphérique.

Information associée

Organisation des périphériques dans des groupes , page 55

Exclusion de périphériques d'OpenManage Enterprise

Les périphériques sont découverts et regroupés dans OpenManage Enterprise pour une gestion efficace des tâches répétitives, telles que les mises à jour de firmware, les mises à jour de configuration, la génération d'inventaire et la surveillance des alertes. Toutefois, vous pouvez également exclure les périphériques de toutes les activités de détection, surveillance et gestion d'OpenManage Enterprise. Les étapes suivantes expliquent comment exclure les périphériques déjà découverts d'OpenManage Enterprise.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Accédez à la page Tous les périphériques en cliquant sur **OpenManage Enterprise** > **Périphériques**.
2. Dans le volet de gauche, sélectionnez le groupe du système ou le groupe personnalisé duquel le périphérique doit être exclu.
3. Dans la liste des périphériques, cochez la case correspondant au(x) périphérique(s), puis à partir du menu déroulant **Détection**, cliquez sur **Exclure les périphériques**.
4. À l'invite indiquant que les périphériques seront entièrement supprimés et ajoutés à la liste d'exclusion globale, cliquez sur **Oui**.

Les périphériques sont exclus, ajoutés à la liste d'exclusion globale et ne sont plus surveillés par OpenManage Enterprise.

REMARQUE : Pour supprimer le périphérique de l'exclusion globale et permettre à nouveau à OpenManage Enterprise de contrôler le périphérique, vous devez supprimer les périphériques de la plage d'exclusion globale, puis les redécouvrir.

Exécution de l'inventaire sur les périphériques

Les étapes suivantes décrivent la façon dont vous pouvez lancer la collecte d'inventaire sur les périphériques découverts.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

1. Accédez à la page Tous les périphériques en cliquant sur **OpenManage Enterprise** > **Périphériques**.

2. Dans la liste de périphériques, cochez la case correspondant aux périphériques.
3. Dans le menu déroulant **Inventaire**, cliquez sur **Exécuter l'inventaire sur les périphériques**.

Une tâche d'inventaire est créée pour la collecte d'inventaire des périphériques sélectionnés. Vous pouvez afficher l'état de cette tâche sur la page Inventaire (**OpenManage Enterprise** > **Surveiller** > **Inventaire**).

Mise à jour des firmwares et des pilotes du périphérique à l'aide des lignes de base

Vous pouvez mettre à jour la version du firmware et/ou du pilote du ou des périphériques sur la page Tous les périphériques, ou à partir de la page Conformité du firmware/pilote (voir la section Mise à jour des firmwares et/ou des pilotes en utilisant le rapport de conformité de ligne de base , page 84). La mise à jour à partir de la page Tous les périphériques est recommandée lors de la mise à jour du firmware et/du pilote d'un seul périphérique.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les mises à jour des pilotes s'appliquent uniquement aux périphériques associés aux versions 64 bits de Windows.
- Les mises à jour des pilotes sur les périphériques ne peuvent pas être restaurées.
- Si la mise à jour de firmware est effectuée à l'aide de l'option **« Programmer le prochain redémarrage du serveur »**, la vérification de l'inventaire et de la ligne de base doit être exécutée manuellement après l'installation du package sur le périphérique distant.
- Si le périphérique n'est pas associé à une configuration de base, le menu déroulant **Configuration de base** est vide. Pour associer un périphérique à une configuration de base, voir Création de la configuration de base du firmware.
- Si vous sélectionnez plusieurs périphériques, seuls les périphériques qui sont associés à la ligne de base sélectionnée sont répertoriés dans le tableau.

1. Dans la liste des **Périphériques** de la page Tous les périphériques, sélectionnez le ou les périphériques, puis cliquez sur **Plus d'actions** > **Mettre à jour**.

   REMARQUE : Lorsque vous sélectionnez un (des) périphérique(s), assurez-vous qu'ils sont associés à une ou plusieurs configurations de base du firmware. Sinon, les périphériques ne sont pas affichés dans le rapport de conformité, et par conséquent ne peuvent pas être mis à jour.

2. Dans la boîte dialogue **Mise à jour du périphérique** :
   a. Dans la section **Sélectionner une source de mise à jour**, sélectionnez l'une des actions suivantes :
      - Dans le menu déroulant **Ligne de base**, sélectionnez la ligne de base. Une liste des périphériques associés à la ligne de base sélectionnée s'affiche. Le niveau de conformité de chaque périphérique est affiché dans la colonne « conformité ». En fonction du niveau de conformité, vous pouvez mettre à jour la version du firmware et/ou du pilote. Pour plus d'informations sur la description du champ de cette page, voir Affichage du rapport de conformité du firmware de périphérique.
        i. Cochez les cases correspondantes aux périphériques qui doivent être mis à jour.
        ii. Cliquez sur **Suivant**.
      - Vous pouvez également mettre à jour le firmware et/ou les pilotes à l'aide d'un package de mise à jour individuel. Cliquez sur **Package individuel**, puis suivez les instructions à l'écran. Cliquez sur **Suivant**.

   b. Dans la section **Calendrier** :

   - Sous **Planifier une mise à jour**, cliquez sur **Informations supplémentaires** pour afficher les informations importantes et sélectionnez l'une des options suivantes :
     a. **Mettre à jour maintenant** : applique les mises à jour de firmware/pilote immédiatement.
     b. **Programmer plus tard** : pour spécifier la date et l'heure de mise à jour de la version du pilote et/ou du firmware. Ce mode est recommandé si vous ne souhaitez pas perturber les tâches en cours.
   - Sous **Options de serveur**, sélectionnez l'une des options de redémarrage suivantes :
     a. Pour redémarrer le serveur immédiatement après la mise à jour du firmware/pilote, choisissez **Redémarrer le serveur immédiatement**, puis, dans le menu déroulant, sélectionnez l'une des options suivantes :
        i. **Redémarrage normal sans arrêt forcé**
        ii. **Redémarrage normal avec arrêt forcé**
        iii. **Cycle d'alimentation** pour une réinitialisation matérielle du périphérique.

b. Sélectionnez **Programmer le prochain redémarrage du serveur** pour déclencher la mise à jour du firmware/pilote lors du prochain redémarrage du serveur. Si cette option est sélectionnée, la vérification de l'inventaire et de la ligne de base doit être exécutée manuellement après l'installation du package sur le périphérique distant.

3. Cliquez sur **Terminer**.

Une tâche de mise à jour de firmware/pilote est créée et indiquée dans la liste des tâches. Voir Utilisation des tâches pour le contrôle de périphériques , page 129.

Actualisation de l'intégrité du périphérique d'un groupe de périphériques

Par défaut, l'intégrité de tous les périphériques et groupes de périphériques est automatiquement actualisée toutes les heures par l'appliance, mais vous pouvez également le faire à tout moment. Les étapes suivantes expliquent comment actualiser l'intégrité et l'état de la connexion du groupe de périphériques sélectionné sur la page Tous les périphériques.

1. Dans le volet de gauche, sélectionnez le groupe auquel le périphérique appartient.
   Les périphériques associés au groupe sont alors répertoriés.
2. Cochez la case correspondant au(x) périphérique(s), puis cliquez sur **Actualiser l'intégrité sur le groupe**.
   Une tâche est créée et répertoriée dans la liste des tâches, et son état est **Nouveau** dans la colonne ÉTAT DE LA TÂCHE.

Le dernier état de fonctionnement du ou des périphérique(s) sélectionné(s) est collecté et affiché sur le Tableau de bord et les autres sections pertinentes d'OpenManage Enterprise. Pour télécharger un inventaire des périphériques, voir Exportation de l'inventaire d'un seul périphérique , page 67.

Information associée

Organisation des périphériques dans des groupes , page 55

Actualisation de l'intégrité sur les périphériques

Par défaut, l'intégrité de tous les périphériques et groupes de périphériques est automatiquement actualisée toutes les heures par l'appliance, mais vous pouvez également le faire à tout moment. Les étapes suivantes expliquent comment actualiser l'intégrité et l'état de la connexion des périphériques sélectionnés sur la page Tous les périphériques.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Pour les appareils intrabande découverts à l'aide d'ESXi et des systèmes d'exploitation Linux, l'état d'intégrité ( ) s'affiche comme étant inconnu ( ).

1. Accédez à la page Tous les périphériques en cliquant sur **OpenManage Enterprise** > **Périphériques**.
2. Sélectionnez les périphériques dans la liste des périphériques sur lesquels vous souhaitez actualiser l'intégrité.
3. Cliquez sur le menu déroulant **Actualiser l'intégrité**, puis cliquez sur **Actualiser l'intégrité sur les périphériques**.

Une tâche d'intégrité est lancée pour les périphériques sélectionnés. Vous pouvez afficher l'état de la tâche d'intégrité sur la page Tâches (**OpenManage** > **Surveiller** > **Tâches**).

Restauration d'une version du firmware du périphérique

Vous pouvez effectuer une restauration de la version de micrologiciel d'un périphérique qui est postérieure à la version de micrologiciel de la ligne de base à laquelle il est associé. Cette fonction est disponible uniquement lorsque vous affichez et configurez les propriétés d'un périphérique individuel. Voir la section Affichage et configuration des périphériques individuels , page 68. Vous pouvez effectuer une mise à niveau ou restaurer la version du micrologiciel d'un périphérique individuel. Vous pouvez restaurer la version du micrologiciel d'un seul périphérique à la fois.

REMARQUE :

- La restauration est applicable uniquement pour le firmware. Les pilotes de périphériques mis à jour ne peuvent pas être restaurés à la version précédente.

- La restauration n'est applicable que pour les périphériques mis à jour à partir de la console OME (elle s'applique aux deux lignes de base et pour la mise à jour de DUP unique).
- Si l'un des iDRAC installés n'est pas à l'état « prêt », une tâche de mise à jour du firmware peut signaler un échec, même si le firmware est appliqué avec succès. Vérifiez l'iDRAC qui n'est pas à l'état prêt, puis appuyez sur F1 pour continuer pendant le démarrage du serveur.

Tout firmware d'appareil mis à jour à l'aide de l'interface GUI d'iDRAC n'est pas répertorié dans la liste ci-dessous et ne peut pas être mis à jour. Pour plus d'informations sur la création de lignes de base, voir Création d'une ligne de base de firmware/pilote , page 81.

1. Dans le volet de gauche, sélectionnez le groupe, puis cliquez sur le nom du périphérique dans la liste.
2. Sur la page **<Nom du périphérique>**, cliquez sur **Firmware/pilotes**.
3. Dans le menu déroulant **Ligne de base**, sélectionnez la ligne de base à laquelle l'appareil appartient.
   Tous les appareils associés à la ligne de base sélectionnée sont répertoriés. Pour plus d'informations concernant la description dans le tableau, voir Affichage du rapport de conformité de la ligne de base , page 83.
4. Cochez la case correspondant au périphérique dont la version du firmware doit être restaurée et qui est identifié par .
5. Cliquez sur **Restaurer le micrologiciel**.
6. Dans la boîte de dialogue **Restauration du micrologiciel**, les informations suivantes s'affichent :
   - **NOM DU COMPOSANT** : composant sur le périphérique dont la version du micrologiciel est postérieure à la version de la ligne de base.
   - **VERSION ACTUELLE** : version actuelle du composant.
   - **VERSION DE RESTAURATION** : version du micrologiciel suggérée à laquelle le composant peut être rétrogradé.
   - **SOURCE DE LA RESTAURATION** : cliquez sur **Parcourir** pour sélectionner une source à partir de l'emplacement où la version du micrologiciel peut être téléchargée.
7. Cliquez sur **Terminer**. La version du micrologiciel est restaurée.
   REMARQUE : Actuellement, la fonction de restauration suit uniquement les numéros de version à partir desquels le micrologiciel est restauré. La restauration ne prend pas en compte la version du micrologiciel installée par la fonction de restauration (en restaurant la version).

Exportation de l'inventaire d'un seul périphérique

Vous pouvez exporter les données d'inventaire d'un seul périphérique à la fois et uniquement au format .csv.

1. Dans le volet de gauche, sélectionnez le groupe de périphériques. Une liste des périphériques du groupe s'affiche dans la liste Périphériques.
   Un diagramme circulaire indique l'état du périphérique dans le volet en cours. Voir Graphique circulaire. Un tableau répertorie les propriétés des périphériques sélectionnés. Voir Liste des périphériques.
2. Dans la liste des périphériques, cochez la case correspondant au périphérique, puis cliquez sur **Exporter l'inventaire**.
3. Dans la boîte de dialogue **Enregistrer sous**, enregistrez l'inventaire dans un emplacement connu.
   REMARQUE : Lorsqu'elles sont exportées au format .csv, certaines des données affichées dans l'interface graphique utilisateur ne sont pas énumérées avec une chaîne descriptive.

Effectuer plus d'actions sur le châssis et les serveurs

À l'aide du menu déroulant **Plus d'actions**, vous pouvez effectuer les actions suivantes sur la page Tous les périphériques. Sélectionnez le ou les périphérique(s), puis cliquez sur l'un des éléments suivants :

- **Activer la DEL** : activez la DEL du périphérique pour identifier le périphérique parmi un groupe de périphériques dans un datacenter.
- **Désactiver la DEL** : désactivez la DEL du périphérique.
- **Mise sous tension** : allumez le ou les périphérique(s).
- **Mise hors tension** : éteignez le ou les périphérique(s).
- **Arrêt normal** : cliquez pour arrêter le système cible.
- **Exécuter un cycle d'alimentation sur le système (redémarrage à froid)** : cliquez pour éteindre et redémarrer le système.
- **Réinitialiser le système (redémarrage à chaud)** : cliquez sur ce bouton pour arrêter, puis redémarrer le système d'exploitation en forçant la désactivation du système cible.
- **Proxy** : affiché uniquement pour le châssis MX7000. Indique que le périphérique est détecté via un châssis maître MX7000 en cas de Gestion multi-châssis (MCM).
- **CLI IPMI** : cliquez sur ce bouton pour exécuter une commande IMPI. Voir Création d'une tâche de commande distante pour gérer les périphériques , page 134.

- **CLI RACADM** : cliquez sur ce bouton pour exécuter une commande RACADM. Voir Création d'une tâche de commande distante pour gérer les périphériques , page 134.
- **Mise à jour du micrologiciel** : voir Mise à jour des firmwares et des pilotes du périphérique à l'aide des lignes de base , page 65.
- **Intégration** : voir Intégration de périphériques , page 45.
- **Exporter tout et Exporter la sélection** : voir Exportation de toutes les données ou des données sélectionnées , page 68.

Informations matérielles affichées pour le châssis MX7000

- **Blocs d'alimentation du châssis** : informations sur les blocs d'alimentation secteur (PSU) utilisés dans les traîneaux et autres composants.
- **Logements de châssis** : informations sur les logements disponibles dans le châssis et les composants installés dans les logements, le cas échéant.
- **Contrôleur de châssis** : Chassis Management Controller (CMC) et sa version.
- **Ventilateurs** : informations sur les ventilateurs utilisés dans le châssis et leur état de fonctionnement.
- **Température** : état de la température et valeurs seuil du châssis.
- **FRU** : composants ou unités remplaçables sur site qui peuvent être installés dans le châssis.

Exportation de toutes les données ou des données sélectionnées

Vous pouvez exporter des données :

- Des périphériques d'un groupe de périphériques que vous avez affichés et pour lesquels vous avez effectué une analyse stratégique et statistique.
- D'un maximum de 1 000 périphériques.
- Liées à des alertes système, des rapports, des journaux d'audit, des inventaires de groupe, des listes de périphériques, des informations de garantie, OpenManage Enterprise Services, etc.
- Aux formats de fichier suivants : HTML, CSV et PDF.

REMARQUE :

- Évitez d'exporter au format PDF des tableaux « étendus » possédant des colonnes avec de longues chaînes ou un trop grand nombre de colonnes. En raison d'une limitation dans la bibliothèque PDFMaker, la section la plus à droite de ces données exportées est tronquée ou coupée.
- L'inventaire d'un seul appareil peut être exporté uniquement au format .csv. Voir Exportation de l'inventaire d'un seul périphérique , page 67
- En ce qui concerne les rapports, vous pouvez exporter uniquement les rapports sélectionnés et non tous les rapports. Voir Exportation des rapports sélectionnés , page 143.

.

1. Pour exporter des données, sélectionnez **Exporter tout** ou **Exporter la sélection**.
   Une tâche est créée et les données sont exportées vers l'emplacement sélectionné.
2. Téléchargez les données et effectuez des analyses statistiques et stratégiques, si nécessaire.
   Les données sont ouvertes ou enregistrées avec succès en fonction de votre sélection.

   REMARQUE : Si vous exportez des données au format .csv, vous devez disposer des informations d'identification de niveau administrateur pour ouvrir le fichier.

Affichage et configuration des périphériques individuels

REMARQUE : Dans Liste des périphériques, cliquez sur le nom ou l'adresse IP d'un périphérique pour afficher les données de configuration de périphérique, puis modifiez la configuration de périphérique, comme le décrit cette rubrique.

En cliquant sur **OpenManage Enterprise** > **Appareils** > **Sélection d'un appareil dans la liste d'appareils** > **Afficher les détails**, vous pouvez effectuer les actions suivantes :

- Afficher les informations sur l'intégrité et l'état d'alimentation, l'adresse IP du périphérique et le numéro de série.
- Afficher les informations générales à propos du périphérique et effectuer les tâches de contrôle du périphérique et de dépannage.
- Afficher les informations sur le périphérique telles que le RAID, le bloc d'alimentation, le système d'exploitation, la carte réseau, la mémoire, le processeur et le boîtier de stockage. OpenManage Enterprise intègre un rapport présentant un aperçu du NIC, du BIOS,

du disque physique et du disque virtuel utilisés sur les périphériques surveillés par OpenManage Enterprise. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports**.

- Mettre à jour ou restaurer les versions de firmware des composants d'un périphérique qui sont associés à la ligne de base du firmware. Voir Gestion des firmwares et des pilotes de périphérique , page 77.

  REMARQUE : La mise à jour d'un périphérique à l'aide du workflow Package individuel ne prend en charge que les packages Dell Update Packages basés sur un exécutable (EXE). Lors de la mise à jour d'un CMC FX2, le package DUP exécutable doit être installé dans l'un des sleds du châssis.
- Accuser la réception, exporter, supprimer ou ignorer les alertes relatives à un périphérique. Voir Gestion des alertes des périphériques.
- Afficher et exporter les données des fichiers log de matériel d'un périphérique. Voir Gestion des journaux du matériel du périphérique individuel , page 71.
- Afficher et gérer l'inventaire de configuration du périphérique dans un souci de conformité de la configuration. Une comparaison de conformité est lancée lors de l'exécution de l'inventaire de configuration des périphériques.
- Afficher le niveau de conformité d'un périphérique par rapport à la ligne de base de conformité de la configuration à laquelle il est associé. Voir Gestion de la conformité de la configuration du périphérique , page 110.

Présentation du périphérique

- Sur la page **<nom du périphérique>**, sous **Présentation**, l'intégrité, l'état d'alimentation et le numéro de série du périphérique s'affichent. Cliquez sur l'adresse IP pour ouvrir la page de connexion de l'iDRAC. Consultez le *Guide de l'utilisateur de l'iDRAC* disponible sur le site de support Dell.
  - **Informations** : informations de périphérique, telles que le numéro de série, les emplacements DIMM, le nom DNS de l'iDRAC, les processeurs, le châssis, le système d'exploitation et le nom du datacenter. Plusieurs adresses IP de gestion en corrélation avec l'appareil sont répertoriées. Vous pouvez cliquer dessus pour activer les interfaces correspondantes.
  - **Alertes récentes** : alertes récemment générées pour le périphérique.
  - **Activité récente** : liste des tâches récemment exécutées sur le périphérique. Cliquez sur **Afficher tout** pour afficher toutes les tâches. Voir Utilisation des tâches pour le contrôle de périphériques , page 129.
  - **Console distante** : cliquez sur **Lancer l'iDRAC** pour démarrer l'application iDRAC. Cliquez sur **Lancer la console virtuelle** pour démarrer la console virtuelle. Cliquez sur le symbole **Actualiser l'aperçu** pour actualiser la page **Présentation**.
  - **Sous-système du serveur** : affiche l'état d'intégrité des autres composants du périphérique, tels que le bloc d'alimentation, le ventilateur, l'UC et la batterie.

    REMARQUE : Le temps nécessaire pour collecter les données de sous-systèmes des composants de capteur détectés à l'aide d'IPMI dépend de la connectivité réseau, du serveur cible et du firmware cible. Si vous rencontrez des problèmes de délai d'expiration lors de la collecte des données de capteur, redémarrez le serveur cible.
  - La section **Dernière mise à jour** indique la date de la dernière mise à jour de l'état d'inventaire du périphérique. Cliquez sur le bouton **Actualiser** pour mettre à jour l'état. Une tâche d'inventaire est lancée et l'état est mis à jour sur la page.
- La fonctionnalité **Contrôle de l'alimentation** permet de mettre sous ou hors tension, de contrôler le cycle d'alimentation et d'éteindre un périphérique.
- À l'aide de l'**Utilitaire de résolution des problèmes** :
  - Exécutez et téléchargez le rapport de diagnostics. Voir Exécution et téléchargement des rapports de diagnostic , page 70.
  - Réinitialisez l'iDRAC.
  - Extrayez et téléchargez le rapport de Services (SupportAssist). Voir Extraction et téléchargement des rapports de Services (SupportAssist) , page 71.
- Actualisez l'état du périphérique.
- Affichez l'inventaire de périphériques.
- Exportez l'inventaire des périphériques qui est collecté en cliquant sur **Actualiser l'inventaire**. Voir Exportation de toutes les données ou des données sélectionnées , page 68.
- Exécutez les commandes RACADM et IPMI distantes sur le périphérique. Voir Exécution de commandes RACADM et IPMI distantes sur des périphériques individuels , page 72.

OpenManage Enterprise intègre un rapport offrant un aperçu des périphériques surveillés par OpenManage Enterprise. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport de présentation des périphériques**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

Informations sur le matériel du périphérique

OpenManage Enterprise intègre un rapport présentant les composants et leur conformité avec la ligne de base de conformité du firmware. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Conformité du firmware selon le rapport sur les composants**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

- **Informations sur les cartes du périphérique** : informations au sujet des cartes utilisées dans le périphérique.
- **Logiciels installés** : liste des firmwares et des logiciels installés sur les différents composants du périphérique.
- **Processeur** : informations sur le processeur telles que les emplacements pour carte, la famille, la vitesse, les cœurs et le modèle.
- **Informations sur le contrôleur RAID** : contrôleurs RAID et PERC utilisés sur les périphériques de stockage. L'état cumulé équivaut à l'état du RAID qui présente un niveau élevé de gravité. Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc *Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération* disponible sur Dell TechCenter.
- **Informations NIC** : informations sur les cartes réseaux utilisées dans le périphérique.
- **Informations sur la mémoire** : informations sur les modules DIMM utilisés dans le périphérique.
- **Disque de baie** : informations sur les lecteurs installés sur le périphérique. OpenManage Enterprise intègre un rapport sur les disques durs ou disques virtuels disponibles sur les périphériques surveillés par OpenManage Enterprise. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport de disque physique**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.
- **Contrôleur de stockage** : contrôleur de stockage installé sur le périphérique. Cliquez sur le symbole plus pour afficher les données du contrôleur individuel.
- **Informations sur les blocs d'alimentation** : informations sur les blocs d'alimentation installés sur le périphérique.
- **Système d'exploitation** : système d'exploitation installé sur le périphérique.
- **Licences** : état d'intégrité des différentes licences installées sur le périphérique.
- **Boîtier de stockage** : état du boîtier de stockage et version d'EMM.
- **Disque flash virtuel** : liste des lecteurs flash virtuels et leurs spécifications techniques.
- **FRU** : liste des unités remplaçables sur site (FRU) que seuls les techniciens de terrain peuvent gérer et réparer. OpenManage Enterprise intègre un rapport sur les unités remplaçables sur site (FRU) installées sur les périphériques surveillés par OpenManage Enterprise. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Rapport sur les FRU**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.
- **Informations sur la gestion des périphériques** : informations sur l'adresse IP de l'iDRAC installé uniquement s'il s'agit d'un périphérique serveur.
- **Informations client** : affiche les périphériques invités surveillés par OpenManage Enterprise. L'UUID est l'ID universellement unique (Universally Unique Identifier) du périphérique. La colonne **ÉTAT DU CLIENT** indique l'état de fonctionnement du périphérique invité.

Exécution et téléchargement des rapports de diagnostic

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. VoirContrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche liée au firmware exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

1. Sur la page **<Nom du périphérique>**, depuis le menu déroulant **Dépanner**, sélectionnez **Exécuter des diagnostics**.
2. Dans la boîte de dialogue **Type de diagnostic à distance**, depuis le menu déroulant **Type de diagnostic à distance**, sélectionnez l'une des options suivantes pour générer un rapport.
   - **Express** : le plus vite possible.
   - **Étendu** : à vitesse nominale.
   - **Exécution longue** : à un rythme lent.

   REMARQUE : Consultez le livre blanc technique *Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands* (Exécution à distance de diagnostics automatiques à l'aide des commandes WS-Man et RACADM) à l'adresse https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.
3. Pour générer le rapport de diagnostic maintenant, sélectionnez **Exécuter maintenant**.
4. Cliquez sur **OK**. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**.

AVERTISSEMENT : L'exécution d'un rapport de diagnostic redémarre automatiquement le serveur.

Une tâche est créée et s'affiche sur la page **Tâches**. Pour afficher des informations sur cette tâche, cliquez sur **Afficher les détails** dans le volet de droite. Voir Afficher les listes de tâches , page 129. L'état de la tâche est également affiché dans la section **Activité récente**. Une fois la tâche exécutée avec succès, l'état de la tâche indique **Diagnostic terminé** et le lien **Télécharger** s'affiche dans la section **Activité récente**.

5. Pour télécharger le rapport, cliquez sur le lien **Télécharger**, puis téléchargez le fichier de rapport de diagnostic <*Servicetag-jobid*>.TXT.
   - Sinon, cliquez sur **Dépanner** > **Télécharger le rapport de diagnostic**, puis téléchargez le fichier.
6. Dans la boîte de dialogue **Télécharger les fichiers de diagnostics à distance**, cliquez sur le lien du fichier .TXT, puis téléchargez le rapport.
7. Cliquez sur **OK**.

Extraction et téléchargement des rapports de Services (SupportAssist)

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche liée au firmware exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

1. Sur la page **<Nom du périphérique>**, dans le menu déroulant **Dépannage**, sélectionnez **Extraire le rapport SupportAssist**.
2. Dans la boîte de dialogue **Extraire le rapport SupportAssist** :
   a. Saisissez le nom du fichier dans lequel le rapport SupportAssist doit être enregistré.
   b. Cochez les cases qui correspondent aux types de journaux dont le rapport SupportAssist doit être extrait.
3. Cliquez sur **OK**.
   Une tâche est créée et s'affiche sur la page **Tâches**. Pour afficher des informations sur cette tâche, cliquez sur **Afficher les détails** dans le volet de droite. Voir Afficher les listes de tâches , page 129. L'état de la tâche est également affiché dans la section **Activité récente**. Une fois la tâche exécutée avec succès, l'état de la tâche indique **Diagnostic terminé** et le lien **Télécharger** s'affiche dans la section **Activité récente**.
4. Pour télécharger le rapport, cliquez sur le lien **Télécharger**, puis téléchargez le fichier de rapport SupportAssist <*Numéro de série*>.<*Heure*>.TXT.
   - Vous pouvez également cliquer sur **Dépannage** > **Télécharger le rapport SupportAssist**.
5. Dans la boîte de dialogue **Télécharger les fichiers SupportAssist**, cliquez sur le lien du fichier .TXT, puis téléchargez le rapport. Chaque lien représente le type de journal que vous avez sélectionné.
6. Cliquez sur **OK**.

Gestion des journaux du matériel du périphérique individuel

REMARQUE : Les journaux de matériel sont disponibles pour les serveurs YX4X, les châssis MX7000 et les traîneaux. Pour en savoir plus, voir Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

- Sur la page **<Nom du périphérique>**, cliquez sur **Journaux du matériel**. Tous les messages d'événement et d'erreur générés pour le périphérique sont répertoriés. Pour obtenir la description des champs, voir Surveillance des journaux d'audit , page 127.
- Pour un châssis, les données en temps réel sur les journaux du matériel sont récupérées à partir du châssis.
- Pour ajouter un commentaire, cliquez sur **Ajouter un commentaire**.
- Dans la boîte de dialogue, saisissez le commentaire, puis cliquez sur **Enregistrer**. Le commentaire est enregistré et identifié par un symbole dans la colonne **COMMENTAIRE**.
- Pour exporter les données du journal sélectionnées vers un fichier .CSV, cochez les cases correspondantes, puis cliquez sur **Exporter** > **Exporter les données sélectionnées**.
- Pour exporter tous les journaux d'une page, cliquez sur **Exporter** > **Exporter la page actuelle**.

Exécution de commandes RACADM et IPMI distantes sur des périphériques individuels

Les commandes RACADM et IPMI peuvent être envoyées à l'iDRAC d'un périphérique à partir de la page « Nom de périphérique » pour gérer à distance le périphérique correspondant.

REMARQUE :

- L'utilisation du CLI RACADM n'autorise qu'une seule commande à la fois.
- Les caractères spéciaux suivants ne sont pas pris en charge dans les paramètres RACADM et IPMI CLI : **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * et **'**.

1. Cochez la case correspondant au périphérique puis cliquez sur **Afficher les détails**.
2. Sur la page **<Nom du périphérique>**, cliquez sur **Ligne de commande distante**, puis sélectionnez **CLI RACADM** ou **CLI IPMI**.

   REMARQUE : L'onglet CLI RACADM ne s'affiche pas pour les serveurs suivants car la tâche correspondante n'est pas disponible dans le pack de périphérique : MX740c, MX840c et MX5016S.

3. Dans la boîte de dialogue **Envoyer une commande distante**, saisissez la commande. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne. Pour afficher les résultats dans la même boîte de dialogue, cochez la case **Ouvrir les résultats après l'envoi**.

   REMARQUE : Saisissez une commande IPMI à l'aide de la syntaxe suivante : `-I lanplus <command>` . Pour mettre fin à la commande, saisissez « Exit ».

4. Cliquez sur **Envoyer**.
   Une tâche est créée et affichée dans la boîte de dialogue. La tâche est également répertoriée dans les Détails de la tâche. Voir Afficher les listes de tâches , page 129.
5. Cliquez sur **Terminer**.
   La section **Alertes récentes** affiche l'état de progression de la tâche.

Lancement de l'application de gestion iDRAC d'un périphérique

1. Cochez la case correspondant au périphérique.
   État de fonctionnement du périphérique, nom, type, adresse IP et le numéro de service s'affichent.
2. Dans le volet de droite, cliquez sur **Lancer l'application de gestion**.
   La page Connexion iDRAC s'affiche. Connectez-vous avec les informations d'identification iDRAC.

   Pour de plus amples informations concernant l'utilisation de l'iDRAC, rendez-vous sur Dell.com/idracmanuals.

   REMARQUE : Vous pouvez également démarrer l'application de gestion en cliquant sur l'adresse IP dans la liste des périphériques. Voir Liste des périphériques , page 62.

Démarrer la console virtuelle

Le lien de la **console virtuelle** fonctionne sur la licence iDRAC Enterprise des serveurs YX4X. Sur les serveurs YX2X et YX3X, le lien fonctionne sur la version 2.52.52.52 et les versions ultérieures de la licence iDRAC Enterprise. Si vous cliquez sur le lien alors que le type actuel du plug-in pour la console virtuelle est Active X, un message vous invitant à mettre à jour la console vers HTML5 pour bénéficier d'une meilleure expérience utilisateur s'affiche. Pour en savoir plus, voir Création d'une tâche pour modifier le type de plug-in de la console virtuelle , page 135 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

1. Cochez la case correspondant au périphérique.
   État de fonctionnement du périphérique, nom, type, adresse IP et le numéro de service s'affichent.
2. Dans le volet de droite, cliquez sur **Lancer la console virtuelle**.
   La page de la console distante sur le serveur s'affiche.

Actualiser l'inventaire des appareils d'un seul appareil

Par défaut, l'inventaire des composants logiciels et matériels dans les périphériques ou groupes de périphériques est automatiquement collecté toutes les 24 heures (par exemple, à midi tous les jours). Cependant, vous pouvez procéder comme suit pour collecter le rapport d'inventaire d'un appareil à tout moment :

1. Sélectionnez la case à cocher correspondant à l'appareil sur la page Tous les appareils (**OpenManage Enterprise** > **Appareils**) et cliquez sur **Afficher les détails** dans le volet de droite. La page Présentation des appareils s'affiche.
2. Cliquez sur **Actualiser l'inventaire** pour lancer une tâche d'inventaire.
   Vous pouvez afficher l'état de la tâche d'inventaire sur la page Inventaire (**OpenManage Enterprise** > **Surveiller** > **Inventaire**). Sélectionnez la tâche d'inventaire, puis cliquez sur **Afficher les détails** pour afficher l'inventaire collecté de l'appareil sélectionné. Pour plus d'informations sur l'affichage des données de l'inventaire actualisé, voir Affichage et configuration des périphériques individuels , page 68. Pour télécharger un inventaire des périphériques, voir Exportation de l'inventaire d'un seul périphérique , page 67.

Information associée

Organisation des périphériques dans des groupes , page 55

9

Gestion de l'inventaire des périphériques

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

En cliquant sur le menu **OpenManage Enterprise** > **Surveiller** > **Inventaire**, vous pouvez générer un rapport d'inventaire des périphériques pour mieux gérer votre datacenter, réduire la maintenance, maintenir un stock minimal et réduire les coûts opérationnels. À l'aide de la fonction Planifications d'inventaire dans OpenManage Enterprise, vous pouvez planifier des tâches pour qu'elles s'exécutent à un moment prédéfini, puis générer des rapports. Vous pouvez planifier des tâches d'inventaire sur les serveurs PowerEdge de 12e génération et versions ultérieures, les périphériques de mise en réseau, les châssis PowerEdge, les matrices EqualLogic, les matrices Compellent et les périphériques PowerVault.

Sur cette page, vous pouvez créer, modifier, exécuter, arrêter ou supprimer des planifications d'inventaire. La liste des tâches de planification d'inventaire existantes s'affiche.

- **NOM** : le nom de la planification d'inventaire.
- **PLANIFICATION** : indique si la tâche est planifiée pour s'exécuter immédiatement ou ultérieurement.
- **DERNIÈRE EXÉCUTION** : indique l'heure à laquelle la tâche a été exécutée pour la dernière fois.
- **ÉTAT** : indique si la tâche est en cours d'exécution, terminée ou en échec.

REMARQUE : Sur les pages **Détection** et **Planifications d'inventaire**, l'état d'une tâche planifiée est identifié par **En file d'attente** dans la colonne **ÉTAT**. Cependant, le même état est indiqué comme **Planifié** sur la page **Tâches**.

Pour afficher l'aperçu des informations d'une tâche, sélectionnez la ligne correspondant à la tâche. Le volet de droite affiche les données de la tâche et les groupes cible associés à la tâche d'inventaire. Pour afficher les informations relatives à la tâche, cliquez sur **Afficher les détails**. La page **Détails de la tâche** affiche plus d'informations. Voir Affichage des informations d'une tâche individuelle , page 133.

Tâches associées

Exécution immédiate d'une tâche d'inventaire , page 75
Création d'une tâche d'inventaire , page 75
Suppression d'une tâche d'inventaire , page 76
Création d'une tâche d'inventaire , page 74

Sujets :

Création d'une tâche d'inventaire

Les étapes suivantes décrivent la façon dont vous pouvez lancer la collecte d'inventaire sur les groupes découverts.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- La collecte de l'inventaire sur les traîneaux de stockage du châssis n'est pas prise en charge dans OpenManage Enterprise s'ils sont gérés via la gestion des périphériques du châssis.

1. Pour lancer l'Assistant d'inventaire, procédez comme suit :

a. Sur la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), sélectionnez un groupe dans le volet de gauche et, dans le menu déroulant **Inventaire**, cliquez sur **Exécuter l'inventaire sur le groupe** .
b. Sur la page Inventaire (**OpenManage Enterprise** > **Surveiller** > **Inventaire**), cliquez sur **Créer**.

2. Dans la boîte de dialogue **Inventaire**, un nom par défaut de tâche d'inventaire est rempli dans le champ **Nom de tâche d'inventaire**. Pour le modifier, entrez un nom pour la tâche d'inventaire.
3. Dans le menu déroulant **Sélectionner des groupes**, sélectionnez les groupes de périphériques sur lesquels l'inventaire doit être exécuté.

   Si vous avez lancé la tâche d'inventaire à partir de la page Tous les périphériques après la sélection d'un groupe, Sélectionner des groupes sera renseigné avec le nom du groupe sélectionné. Pour en savoir plus sur les groupes de périphériques, voir Organisation des périphériques dans des groupes , page 55.
4. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard.

   Voir Définitions de champs de tâche de planification , page 180.
5. Les **options supplémentaires** suivantes peuvent être sélectionnées lors de l'exécution de la tâche d'inventaire :
   - Cochez la case **Collecter l'inventaire de configuration** pour générer un inventaire de la ligne de base de conformité de la configuration.
   - Cochez la case **Collecter l'inventaire des pilotes** pour collecter les informations relatives à l'inventaire des pilotes à partir du serveur Windows. Vous pouvez également installer le collecteur d'inventaire et Dell System Update sur le serveur Windows, si ces composants ne sont pas disponibles sur le serveur.

   REMARQUE :
   - « Collecter l'inventaire des pilotes » s'applique uniquement aux périphériques détectés en tant que serveurs Windows 64 bits.
   - La collecte d'inventaire des périphériques Windows n'est prise en charge qu'à l'aide d'OpenSSH. Les autres implémentations SSH sur Windows, comme le SSH CygWin, ne sont pas prises en charge.

   Pour plus d'informations sur les lignes de base de conformité de la configuration, voir Gestion de la conformité de la configuration du périphérique , page 110.
6. Cliquez sur **Terminer**.
7. La tâche est créée et répertoriée dans la file d'attente.
   Une tâche d'inventaire est créée et s'affiche dans la liste des tâches d'inventaire. La colonne **Planification** indique si la tâche est Planifiée ou Non planifiée. Voir la section Exécution immédiate d'une tâche d'inventaire , page 75.

Information associée

Gestion de l'inventaire des périphériques , page 74

Exécution immédiate d'une tâche d'inventaire

REMARQUE : Vous ne pouvez pas exécuter une nouvelle fois une tâche qui est déjà en cours d'exécution.

1. Dans la liste de tâches de planification d'inventaire existantes, cochez la case correspondant à la tâche d'inventaire que vous souhaitez exécuter immédiatement.
2. Cliquez sur **Exécuter maintenant**.

   La tâche démarre immédiatement et un message s'affiche dans l'angle inférieur droit.

Information associée

Gestion de l'inventaire des périphériques , page 74

Création d'une tâche d'inventaire

Vous pouvez arrêter la tâche uniquement si elle est en cours d'exécution. Il est impossible d'arrêter les tâches d'inventaire qui sont terminées ou qui ont échoué. Pour arrêter une session :

1. Dans la liste de tâches de planification d'inventaire existantes, cochez la case correspondant à la tâche de planification d'inventaire que vous souhaitez arrêter.
2. Cliquez sur **Arrêter**.
   La tâche est arrêtée et un message s'affiche dans l'angle inférieur droit.

Information associée

Gestion de l'inventaire des périphériques , page 74

Suppression d'une tâche d'inventaire

REMARQUE : Vous ne pouvez pas supprimer une tâche en cours d'exécution.

1. Dans la liste de tâches de planification d'inventaire existantes, cochez la case correspondant à la tâche d'inventaire que vous souhaitez supprimer.
2. Cliquez sur **Supprimer**.
   La tâche est supprimée et un message s'affiche dans le coin inférieur droit.

Information associée

Gestion de l'inventaire des périphériques , page 74

Modification d'une tâche de planification d'inventaire

1. Cliquez sur **Modifier**.
2. Dans la boîte de dialogue **Planification d'inventaire**, modifiez le nom de la tâche d'inventaire dans **Nom de tâche d'inventaire**. Voir la section Création d'une tâche d'inventaire , page 74.
   La tâche de planification d'inventaire est mise à jour et s'affiche dans le tableau.

10

Gestion des firmwares et des pilotes de périphérique

Sur la page **OpenManage Enterprise** > **Configuration** > **Conformité du firmware/pilote**, vous pouvez gérer les firmwares de tous les périphériques « gérés ». Vous pouvez également mettre à jour les pilotes des appareils basés sur Windows 64 bits.

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des privilèges d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- La version de firmware et de pilote du périphérique, si elle est antérieure à la version de la ligne de base, n'est pas mise à jour automatiquement. Par conséquent, l'utilisateur doit lancer la mise à jour.
- Il est recommandé d'effectuer les mises à jour du firmware et du pilote pendant les périodes de maintenance pour empêcher les périphériques ou l'environnement de passer à l'état hors ligne durant les heures de bureau.
- Pour gérer le firmware et/ou le pilote d'un périphérique, vous devez définir l'état d'intégration du système sur « Géré » ou « Géré avec des alertes ». Voir Intégration de périphériques , page 45
- Actuellement, le catalogue contient des pilotes uniquement pour les périphériques Windows 64 bits.

La fonctionnalité Firmware/Pilote permet d'effectuer les opérations suivantes :

- Utilisez un catalogue de firmwares et de pilotes à partir de Dell.com directement ou après l'avoir enregistré sur un chemin d'accès au réseau. Voir Ajout d'un catalogue à l'aide de Dell.com , page 78 ou Création d'un catalogue de firmwares en utilisant le réseau local.
- Créez une ligne de base de firmwares et pilotes à l'aide des catalogues disponibles. Ces lignes de base servent de points de référence pour comparer la version de firmware et de pilote des périphériques avec celle du catalogue. Reportez-vous à Création de la configuration de base d'un firmware.
- Exécutez un rapport de conformité pour vérifier si les périphériques associés à la ligne de base sont conformes aux versions de firmware et de pilote de la ligne de base. Voir la rubrique Vérification de la conformité des firmwares. La colonne **CONFORMITÉ** affiche les éléments suivants :
  - **OK**  : si la version de firmware et/ou de pilote du périphérique cible est identique à la ligne de base.
  - **Mise à niveau** : si le périphérique cible dispose d'une ou plusieurs versions antérieures à la version de firmware ou de pilote de la ligne de base. Voir Mise à jour de la version du firmware du périphérique.
  - **Critique**  : si le périphérique n'est pas conforme à la ligne de base, indique qu'il s'agit d'une mise à niveau critique et que le firmware et le pilote du périphérique doivent être mis à niveau pour garantir un bon fonctionnement.
  - **Avertissement**  : si le firmware et/ou le pilote du périphérique n'est pas conforme à la ligne de base et que le firmware peut être mis à niveau pour améliorer les fonctionnalités.
  - **Rétrograder**  : si le firmware et/ou pilote du périphérique est ultérieur à la version de la ligne de base.
  - Exportez le rapport de conformité à des fins statistiques et d'analyse.
  - Mettez à jour la version de firmware et/ou de pilote du périphérique à l'aide de la ligne de base. Consultez Mise à jour des firmwares et des pilotes du périphérique à l'aide des lignes de base , page 65.

REMARQUE :

- Lorsqu'une la conformité d'une ligne de base de firmware/pilote avec de nombreux appareils est vérifiée, les alertes d'avertissement CDEV9000 sur la page Alertes sont consignées pour un seul appareil non conforme aléatoire de cette ligne de base.
- Déployer des serveurs supplémentaires pour augmenter la fonctionnalité de calcul en période de forte charge de travail. L'état de conformité des firmwares ou des pilotes des commutateurs réseau, des IOA modulaires et des appareils de stockage Dell s'affiche comme **Inconnu**, car ils ne peuvent pas être mis à jour à l'aide du catalogue Dell. Il est recommandé d'effectuer des mises à jour individuelles des firmwares ou des pilotes pour ces périphériques en utilisant leur package de mise à jour individuel. Pour effectuer des mises à jour individuelles des firmwares ou des pilotes, sélectionnez un périphérique sur la page Tous les périphériques, puis cliquez sur **Afficher les détails** > **Firmwares/Pilotes** et sélectionnez l'option Package individuel. Pour plus d'informations sur la

liste des appareils non pris en charge, reportez-vous à Rapports de ligne de base de conformité du firmware et du pilote : appareils dont l'état de conformité est « Inconnu » , page 184.

Vous pouvez également mettre à jour la version du firmware d'un périphérique depuis la :

- Page Tous les périphériques. Voir Mise à jour de la version du firmware du périphérique.
- Page Détails du périphérique. Dans la liste des périphériques, cliquez sur le nom ou l'adresse IP du périphérique pour afficher ses données de configuration, puis sur Modifier. Voir Affichage et configuration des périphériques individuels , page 68.

  REMARQUE : La mise à jour d'un périphérique à l'aide du workflow Package individuel ne prend en charge que les packages Dell Update Packages basés sur un exécutable (EXE). Lors de la mise à jour d'un CMC FX2, le package DUP exécutable doit être installé dans l'un des sleds du châssis.

  Le résumé de toutes les lignes de base s'affiche dans le volet actuel, et la conformité d'une ligne de base sélectionnée s'affiche dans le volet de droite sous forme de graphique circulaire. Un graphique circulaire et une liste d'éléments dans la ligne de base changent en fonction de la ligne de base que vous sélectionnez dans la liste des lignes de base. Voir Graphique circulaire.

Sujets :

Gestion des catalogues de firmwares et de pilotes

Les catalogues sont des lots de firmwares et de pilotes basés sur les types de périphériques. Tous les catalogues disponibles (modules de mise à jour) sont validés et publiés sur le site Dell.com. Vous pouvez utiliser le catalogue directement à partir du répertoire en ligne ou il peut être téléchargé vers un partage réseau.

À l'aide de ces catalogues, vous pouvez créer des lignes de base de firmware/pilote pour les périphériques détectés et vérifier leur conformité. Cela permet de réduire l'effort supplémentaire des administrateurs et gestionnaires de périphériques et réduit également la durée de mise à jour et de maintenance.

Les utilisateurs administrateurs peuvent afficher et accéder à tous les catalogues d'OpenManage Enterprise, mais les gestionnaires de périphériques peuvent uniquement afficher et gérer les catalogues qu'ils ont créés et qu'ils possèdent. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Pour obtenir des définitions de champ sur la page de gestion de catalogue, voir Définitions des champs de la section Gestion du catalogue , page 184. Les sources de catalogues auxquelles vous pouvez actuellement accéder sont :

REMARQUE :

- La gestion du catalogue de firmware à l'aide de Dell.com ou d'un chemin de réseau local est limitée uniquement au catalogue Enterprise Server.
- Les catalogues dont l'emplacement de base pointe vers « Downloads.dell.com » peuvent être utilisés sans Dell Update Packages (DUP) lors de l'importation du catalogue dans OpenManage Enterprise version 3.5 à partir d'un partage réseau. Au cours du processus de mise à niveau du firmware, les DUP seront téléchargés directement depuis https://downloads.dell.com.

- **Dernières versions de composant sur Dell.com** : répertorie les dernières versions de firmware et de pilote (Windows 64 bits) des périphériques. Par exemple, BIOS, iDRAC, le bloc d'alimentation ainsi que les disques durs qui sont rigoureusement testés, puis mis sur le marché et publiés sur le site Dell.com. Voir Création d'un catalogue de firmwares en utilisant Dell.com.
- **Chemin d'accès au réseau** : emplacement vers lequel les catalogues de firmwares et de pilotes sont téléchargés par le Dell Repository Manager (DRM) et enregistrés sur un partage réseau. Voir Création d'un catalogue de firmwares en utilisant le réseau local.

Ajout d'un catalogue à l'aide de Dell.com

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche liée au firmware exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions

antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

1. Sur la page **Gestion des catalogues**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une mise à jour de catalogue** :
   a. Dans le champ **Nom**, saisissez un nouveau nom de catalogue de firmwares.
   b. Pour la **Source de catalogue**, sélectionnez l'option **Dernières versions de composant sur Dell.com**.
   c. Dans le champ **Mise à jour du catalogue**, sélectionnez **Manuellement** ou **Automatiquement**.
   d. Si l'option **Automatiquement** est sélectionnée dans le champ **Mise à jour du catalogue**, il convient de définir le paramètre **Fréquence de mise à jour** sur **Tous les jours** ou **Toutes les semaines**, suivi de l'heure dans le format de 12 heures (AM/PM).
   e. Cliquez sur **Terminer**.

   Le bouton **Terminer** s'affiche uniquement lorsque vous avez renseigné tous les champs de la boîte de dialogue.

   Un nouveau catalogue de micrologiciels est créé et répertorié dans le tableau de catalogues sur la page **Gestion des catalogues**.
3. Pour revenir à la page **Conformité du firmware/pilote**, cliquez sur **Retour à la conformité du firmware/pilote**.

Ajout d'un catalogue au réseau local

Le catalogue contenant le firmware et les pilotes (Windows 64 bits) peut être téléchargé à l'aide du Dell Repository Manager (DRM) et enregistré sur un partage réseau.

1. Sur la page **Gestion des catalogues**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une mise à jour de catalogue** :
   a. Dans le champ **Nom**, saisissez un nouveau nom de catalogue.
   b. Pour la Source de catalogue, sélectionnez l'option **Chemin d'accès au réseau**.
   Le menu déroulant **Type de partage** s'affiche.
   c. Sélectionnez une des options suivantes :

   REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche liée au firmware exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

   - NFS
     i. Dans la zone **Adresse de partage**, saisissez l'adresse IP du système sur lequel le catalogue de micrologiciels est stocké sur le réseau.
     ii. Dans la zone **Chemin d'accès au fichier du catalogue**, saisissez le chemin d'accès complet de l'emplacement du fichier du catalogue. Exemple de chemin : *nfsshare\catalog.xml*
   - CIFS
     i. Dans la zone **Adresse de partage**, saisissez l'adresse IP du système sur lequel le catalogue de micrologiciels est stocké sur le réseau.
     ii. Dans la zone **Chemin d'accès au fichier du catalogue**, saisissez le chemin d'accès complet de l'emplacement du fichier du catalogue. Exemple de chemin : *Firmware\m630sa\catalog.xml*
     iii. Dans la zone **Domaine**, saisissez le nom de domaine du périphérique.
     iv. Dans la zone **Nom d'utilisateur**, saisissez le nom de l'utilisateur du périphérique où le catalogue est stocké.
     v. Dans la zone **Mot de passe**, saisissez le mot de passe du périphérique pour accéder au partage. Saisissez le nom d'utilisateur et le mot de passe du dossier partagé sur lequel le fichier catalog.xml est stocké.
   - HTTP
     i. Dans la zone **Adresse de partage**, saisissez l'adresse IP du système sur lequel le catalogue de micrologiciels est stocké sur le réseau.
     ii. Dans la zone **Chemin d'accès au fichier du catalogue**, saisissez le chemin d'accès complet de l'emplacement du fichier du catalogue. Exemple de chemin : *compute/catalog.xml*.
   - HTTPS
     i. Dans la zone **Adresse de partage**, saisissez l'adresse IP du système sur lequel le catalogue de micrologiciels est stocké sur le réseau.
     ii. Dans la zone **Chemin d'accès au fichier du catalogue**, saisissez le chemin d'accès complet de l'emplacement du fichier du catalogue. Exemple de chemin : *compute/catalog.xml*.
     iii. Dans la zone **Nom d'utilisateur**, saisissez le nom de l'utilisateur du périphérique où le catalogue est stocké.
     iv. Dans la zone **Mot de passe**, saisissez le mot de passe du périphérique où le catalogue est stocké.

v. Cochez la case **Vérification du certificat**.

L'authenticité du périphérique où le fichier de catalogue est stocké est validée, et un certificat de sécurité est généré et affiché dans la boîte de dialogue **Informations sur le certificat**.

d. Après avoir saisi l'**Adresse de partage** et le **Chemin d'accès au fichier de catalogue**, le lien **Tester maintenant** s'affiche. Pour valider une connexion au catalogue, cliquez sur **Tester maintenant**. Si la connexion au catalogue est établie, le message *Connexion réussie* s'affiche. Si la connexion à l'adresse de partage ou au chemin d'accès au fichier de catalogue échoue, le message d'erreur *Échec de la connexion au chemin d'accès* s'affiche. Il s'agit d'une étape facultative.

e. Dans le champ **Mise à jour du catalogue**, sélectionnez **Manuellement** ou **Automatiquement**.
Si le champ **Mise à jour du catalogue** est défini sur **Automatiquement**, sélectionnez **Tous les jours** ou **Toutes les semaines** comme fréquence de mise à jour et saisissez l'heure au format 12 heures.

3. Cliquez sur **Terminer**. Le bouton **Terminer** s'affiche uniquement lorsque vous avez renseigné tous les champs de la boîte de dialogue. Un nouveau catalogue de micrologiciels est créé et répertorié dans le tableau de catalogues sur la page **Gestion des catalogues**.
4. Pour revenir à la page **Conformité du firmware/pilote**, cliquez sur **Retour à la conformité du firmware/pilote**.

Tâches associées

Suppression d'un catalogue , page 81

Informations sur le certificat SSL

Les fichiers de catalogues pour les mises à jour du firmware et du pilote peuvent être téléchargés à partir du site de support de Dell, de Dell EMC Repository Manager ou d'un site Web au sein du réseau de votre organisation.

Si vous choisissez de télécharger le fichier de catalogue à partir du site Web au sein du réseau de votre organisation, vous pouvez accepter ou refuser le certificat SSL. Vous pouvez afficher les détails du certificat SSL dans la fenêtre **Informations sur le certificat**. Les informations comprennent la période de validité, l'autorité émettrice et le nom de l'entité pour laquelle le certificat est émis.

REMARQUE : La fenêtre **Informations sur le certificat** ne s'affiche que si vous créez le catalogue à partir de l'Assistant **Création de ligne de base**.

Actions

Accepter	Accepte le certificat SSL et vous permet d'accéder au site Web.
Annuler	Ferme la fenêtre **Informations sur le certificat** sans accepter le certificat SSL.

Mise à jour d'un catalogue

Les catalogues de firmwares et de pilotes existants peuvent être mis à jour à partir du site Dell.com (emplacement de base).

Pour mettre à jour un catalogue :

1. Sur la page Gestion de catalogue, sélectionnez un catalogue.
2. Cliquez sur le bouton **Rechercher les mises à jour** qui est situé dans le volet de droite de la page **Gestion de catalogue**.
3. Cliquez sur **OUI**.
Si le catalogue sélectionné était un catalogue en ligne, il est remplacé par la version la plus à jour disponible sur le site Dell.com. Pour les catalogues des réseaux locaux, tous les firmwares et pilotes récents disponibles à l'emplacement de base sont pris en compte dans le calcul de la conformité de ligne de base.

Modification d'un catalogue

1. Sur la page **Gestion de catalogue**, sélectionnez un catalogue.
Les détails du catalogue s'affichent dans le volet de droite **<nom de catalogue>**.
2. Cliquez sur **Modifier** dans le volet de droite.
3. Dans l'Assistant **Modifier la mise à jour de catalogue**, modifiez les propriétés.

   Les propriétés que vous ne pouvez pas modifier sont grisées. Pour en savoir plus sur les définitions de champ, voir Ajout d'un catalogue à l'aide de Dell.com , page 78 et Ajout d'un catalogue au réseau local , page 79.

4. Saisissez l'**Adresse de partage** et le **Chemin d'accès au fichier du catalogue**, le lien **Tester maintenant** s'affiche. Pour valider une connexion au catalogue, cliquez sur **Tester maintenant**. Si la connexion au catalogue est établie, le message `Connection Successful` (Connexion réussie) s'affiche. Si la connexion à l'adresse de partage ou au chemin d'accès au fichier de catalogue échoue, le message d'erreur `Connection to path failed` s'affiche. Il s'agit d'une étape facultative.
5. Dans le champ **Mise à jour du catalogue**, sélectionnez **Manuellement** ou **Automatiquement**.
   Si le champ **Mise à jour du catalogue** est défini sur **Automatiquement**, sélectionnez **Tous les jours** ou **Toutes les semaines** comme fréquence de mise à jour et saisissez l'heure au format 12 heures.
6. Cliquez sur **Terminer**.
   Une tâche est créée et exécutée immédiatement. L'état de la tâche est indiqué dans la colonne **EMPLACEMENT DE LA LOGITHÈQUE** de la page **Gestion du catalogue**.

Suppression d'un catalogue

1. Sur la page **Gestion du catalogue**, sélectionnez les catalogues, puis cliquez sur **Supprimer**.
   Les catalogues sont supprimés de la liste.
2. Pour revenir à la page **Conformité du firmware/pilote**, cliquez sur **Retour à la conformité du firmware/pilote**.

REMARQUE : Les catalogues ne peuvent pas être supprimés s'ils sont associés à une ligne de base.

Information associée

Ajout d'un catalogue au réseau local , page 79

Création d'une ligne de base de firmware/pilote

Une ligne de base est un ensemble de périphériques ou de groupes de périphériques qui sont associés à un catalogue de firmware/pilotes. Une ligne de base est créée pour l'évaluation de la conformité du firmware et des pilotes pour les périphériques de cette ligne de base, par rapport aux versions spécifiées dans le catalogue. Pour créer une ligne de base :

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- L'utilisateur gestionnaire de périphériques peut uniquement afficher et gérer les lignes de base du firmware/pilote que le gestionnaire de périphériques en question a créées et qu'il possède. En outre, lors de la création de lignes de base, les groupes ou les périphériques cibles (capables de mettre à jour le firmware) qui sont uniquement dans le périmètre du gestionnaire de périphériques s'affichent.
- Après une mise à niveau depuis la version 3.5 ou une version antérieure, les lignes de base de firmware/pilote créées par les gestionnaires de périphériques à partir de n'importe quelle version antérieure d'OpenManage Enterprise sont uniquement affectées à l'administrateur. Par conséquent, les gestionnaires de périphériques doivent recréer les lignes de base du firmware/pilote à partir des versions précédentes postérieures à la mise à niveau.
- Un périphérique non conforme dont la version de firmware et/ou de pilote est antérieure à la version du catalogue n'est pas automatiquement mis à jour. Vous devez mettre à jour la version du firmware. Il est recommandé d'effectuer les mises à jour de firmware du périphérique pendant les périodes de maintenance pour empêcher les périphériques ou l'environnement de passer à l'état hors ligne durant les heures de bureau.

1. Sous **Firmware**, cliquez sur **Créer une configuration de base**.
2. Dans la boîte de dialogue **Créer une mise à jour de la ligne de base** :
   a. Dans la section **Informations sur la configuration de base** :
      i. Dans le menu déroulant **Catalogue**, sélectionnez un catalogue.
      ii. Pour ajouter un catalogue à cette liste, cliquez sur **Ajouter**. Voir Gestion des catalogues de firmwares.
      iii. Dans la zone **Nom de la ligne de base**, saisissez un nom pour la ligne de base, puis saisissez sa description.
      iv. Cliquez sur **Suivant**.
   b. Dans la section **Cible** :
      - Pour sélectionner le(s) périphérique(s) cible(s) :

i. Sélectionnez l'option **Sélectionner des périphériques**, puis cliquez sur le bouton **Sélectionner des périphériques.**
ii. Dans la boîte de dialogue **Sélectionner des périphériques**, tous les périphériques surveillés par OpenManage Enterprise, les IOM et les périphériques du groupe statique ou de requête s'affichent dans leurs groupes respectifs.
iii. Dans le volet de gauche, cliquez sur le nom de la catégorie. Les périphériques de cette catégorie s'affichent dans le volet en cours.
iv. Cochez la case correspondant au(x) périphérique(s). Les périphériques sélectionnés sont répertoriés dans l'onglet **Périphériques sélectionnés**.

- Pour sélectionner le(s) groupe(s) de périphériques cibles :
  i. Sélectionnez l'option **Sélectionner des groupes**, puis cliquez sur le bouton **Sélectionner des groupes.**
  ii. Dans la boîte de dialogue **Sélectionner des groupes**, tous les périphériques surveillés par OpenManage Enterprise, les IOM et les périphériques du groupe statique ou de requête s'affichent dans les catégories respectives.
  iii. Dans le volet de gauche, cliquez sur le nom de la catégorie. Les périphériques de cette catégorie s'affichent dans le volet en cours.
  iv. Cochez la case correspondant au(x) groupe(s). Les groupes sélectionnés sont répertoriés sous l'onglet **Groupes sélectionnés**.

3. Cliquez sur **Terminer**.
   Un message s'affiche, indiquant qu'une tâche est générée pour créer la configuration de base.

   Dans le tableau Ligne de base, des données à propos du périphérique et de la tâche de ligne de base s'affichent. Pour en savoir plus sur les définitions de champ, voir Définitions de champs de ligne de base du micrologiciel , page 180.

Suppression des lignes de base de conformité de la configuration

Vous pouvez supprimer les lignes de base de conformité de la configuration sur la page **Configuration** > **Conformité de la configuration** et délier les appareils des lignes de base associées.

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

Pour supprimer les lignes de base de conformité de la configuration :

1. Sélectionnez la ou les lignes de base dans la liste des lignes de base sur la page Conformité de la configuration.
2. Cliquez sur **Supprimer**, puis sur **Oui** à l'invite de commande.

Les lignes de base de configuration supprimées sont retirées de la page Conformité de la configuration.

Modification d'une ligne de base

Vous pouvez modifier la ligne de base sur la page **Configurations** > **Conformité du firmware/pilote** en procédant comme suit :

1. Sélectionnez une ligne de base, puis cliquez sur **Modifier** dans le volet de droite.
2. Modifiez les données comme indiqué dans Création de la configuration de base du micrologiciel.
   Les informations mises à jour s'affichent dans la liste de configurations de base.
3. Pour revenir à la page **Conformité du firmware/pilote**, cliquez sur **Retour à la conformité du firmware/pilote**.

Vérification de la conformité d'un firmware et d'un pilote de périphérique

Sur la page **Configuration** > **Conformité du firmware/pilote**, vous pouvez vérifier la conformité des firmwares et des pilotes des périphériques de ligne de base par rapport au catalogue associé, afficher le rapport et mettre à jour les firmwares et les pilotes des périphériques non conformes.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

- Les firmwares et les pilotes (Windows 64 bits) pour les périphériques non conformes dans la ligne de base ne sont pas automatiquement mis à jour, cela doit être fait par l'utilisateur. Il est recommandé d'effectuer les mises à jour des firmwares et des pilotes du périphérique pendant les périodes de maintenance pour empêcher les périphériques ou l'environnement de passer à l'état hors ligne durant les heures de bureau.
- Pour collecter les informations relatives à l'inventaire, le collecteur d'inventaire et Dell System Update doivent être disponibles sur le serveur Windows. Si ces composants ne sont pas disponibles sur le serveur, lancez une tâche d'inventaire et sélectionnez **Collecter l'inventaire des pilotes**. La tâche de détection collecte également les informations relatives à l'inventaire des pilotes, mais seule la tâche d'inventaire installe les composants nécessaires sur le serveur. Pour collecter les informations relatives à l'inventaire des pilotes, créez ou modifiez une tâche d'inventaire, puis cochez la case **Collecter l'inventaire des pilotes**. Pour plus d'informations, voir Création d'une tâche d'inventaire , page 74 et Modification d'une tâche de planification d'inventaire , page 76.

1. Cochez la case correspondant à la ou aux lignes de base, puis cliquez sur **Vérifier la conformité**.
   La tâche de conformité de la ligne de base est exécutée.

   REMARQUE : Si les périphériques ne sont associés à aucun catalogue, la conformité n'est pas vérifiée. Une tâche est créée uniquement pour les périphériques qui sont associés et répertoriés dans le tableau Conformité. Pour associer un périphérique à un catalogue, voir la rubrique Création d'une configuration de base pour les firmwares.

   Dans le tableau Ligne de base, des données à propos du périphérique et de la tâche de ligne de base s'affichent. Pour en savoir plus sur les définitions de champ, voir Définitions de champs de ligne de base du micrologiciel , page 180.
2. Pour afficher le rapport de conformité et mettre à niveau la version de firmware et de pilote du ou des périphériques, cliquez sur **Afficher le rapport** dans le volet de droite.

   Voir la rubrique Affichage du rapport sur la conformité de firmware d'un périphérique.

   REMARQUE : La restauration n'est pas prise en charge pour les pilotes.

Affichage du rapport de conformité de la ligne de base

Sur la page **Configuration** > **Conformité du firmware/pilote**, l'état de conformité des lignes de base est indiqué. Un graphique circulaire fournit un récapitulatif de la conformité des lignes de base à leurs catalogues respectifs. Lorsque plusieurs périphériques sont associés à une ligne de base, l'état du périphérique le moins conforme à la ligne de base est indiqué comme correspondant au niveau de conformité de cette ligne de base. Par exemple, le niveau de conformité d'une ligne de base avec un seul périphérique dont la conformité est « critique » est indiqué par « critique »  même si la plupart des périphériques sont conformes.

Vous pouvez afficher la conformité du firmware et du pilote d'un périphérique individuel associé à une ligne de base et choisir de mettre à niveau ou rétrograder la version de firmware et/ou pilote sur ce périphérique. Pour afficher le rapport de conformité de la ligne de base :

- Cochez la case correspondant à la configuration de base et cliquez sur **Afficher le rapport** dans le volet de droite.

  Sur la page **Rapport de conformité**, la liste des périphériques associés à la configuration de base et leur niveau de conformité respectif s'affiche. Par défaut, les appareils présentant les états **Critique** et **Avertissement** s'affichent.

  REMARQUE : Chaque périphérique à son propre état, mais l'état le plus grave est considéré comme l'état du groupe. Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération) disponible sur le Dell TechCenter.
- **CONFORMITÉ** : indique le niveau de conformité d'un périphérique par rapport à la configuration de base. Pour plus d'informations sur les symboles utilisés pour les niveaux de conformité du firmware/pilote du périphérique, voir la section Gestion des firmwares et des pilotes de périphérique , page 77.
- **TYPE** : type de périphérique pour lequel le rapport de conformité est généré.
- **NOM/COMPOSANTS DE PÉRIPHÉRIQUE** : par défaut, le numéro de service du périphérique s'affiche.
  1. Pour afficher des informations sur les composants du périphérique, cliquez sur le symbole **>**.

     Une liste des composants et de leur conformité par rapport au catalogue s'affiche.

     REMARQUE : Pour tous les appareils (à l'exception du châssis MX7000) qui sont entièrement conformes à la ligne de base du firmware associée, le symbole **>** n'est pas affiché.
  2. Cochez une ou plusieurs cases correspondant aux périphériques dont l'état de conformité du firmware est « Critique » et nécessite une mise à jour.

3. Cliquez sur **Rendre conforme**. Reportez-vous à la section Mise à jour de la version du firmware du périphérique et du pilote du système d'exploitation en utilisant le rapport de conformité de ligne de base.

- **NUMÉRO DE SERVICE** : permet d'afficher les informations complètes à propos d'un périphérique sur la page **<nom du périphérique>**. Pour plus d'informations concernant les tâches que vous pouvez effectuer de cette page, voir la rubrique Affichage et configuration des périphériques individuels , page 68.
- **REDÉMARRAGE REQUIS** : indique si le périphérique doit être redémarré après la mise à jour du micrologiciel.
- **Informations** : ce symbole, correspondant à chaque composant de périphérique, est un lien vers la page du site de support à partir de laquelle le firmware/pilote peut être mis à jour. Cliquez ici pour ouvrir la page Détails du pilote correspondante sur le site de support.
- **VERSION ACTUELLE** : indique la version actuelle du micrologiciel du périphérique.
- **VERSION DE LA LIGNE DE BASE** : indique la version correspondante de firmware et de pilote du périphérique disponible dans le catalogue associé.
- Pour exporter le rapport de conformité vers un fichier Excel, cochez les cases correspondant au périphérique, puis sélectionner dans **Exporter**.
- Pour revenir à la page **Micrologiciels**, cliquez sur **Retour aux micrologiciels**.
- Pour procéder à un tri des données sur la base d'une colonne, cliquez sur le titre de la colonne.
- Pour rechercher un périphérique dans le tableau, cliquez sur **Filtres avancés**, puis sélectionnez ou saisissez les données dans les cases des filtres. Reportez-vous à Filtres avancés dans Présentation de l'interface graphique d'OpenManage Enterprise–Tech Release , page 36.

Mise à jour des firmwares et/ou des pilotes en utilisant le rapport de conformité de ligne de base

À l'issue de l'exécution du rapport de conformité du firmware ou du pilote, si la version du firmware ou du pilote du périphérique est antérieure à la version du catalogue, la page Rapport de conformité indique que l'état du firmware ou du pilote du périphérique est défini sur Mettre à niveau (ou).

La version de firmware et de pilote des périphériques de ligne de base associés n'est pas mise à jour automatiquement. Par conséquent, l'utilisateur doit lancer la mise à jour. Il est recommandé d'effectuer les mises à jour du firmware et/ou du pilote du périphérique pendant les périodes de maintenance pour empêcher les périphériques ou l'environnement de passer à l'état hors ligne durant les heures de bureau.

Les gestionnaires de périphériques peuvent uniquement mettre à jour les firmware et les pilotes des périphériques dans leur périmètre.

REMARQUE : La collecte de l'inventaire et la mise à jour de firmware sur le traîneau de stockage du châssis ne sont pas prises en charge dans OpenManage Enterprise s'ils sont gérés via la gestion des périphériques du châssis.

Conditions préalables :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Vous devez créer une règle de pare-feu de trafic entrant pour permettre la communication avec le port 22.
- Si les partages HTTP et HTTPS ont été configurés à l'aide des paramètres de proxy, assurez-vous que ces URL locales sont incluses dans la liste des exceptions de proxy avant de lancer les tâches de mise à jour.
- Une seule tâche de mise à jour peut être lancée sur l'ordinateur cible à un moment donné.

REMARQUE :

- La fonction Réinitialiser l'iDRAC n'est pas prise en charge pour les périphériques d'un châssis MCM qui se trouvent à l'état d'intégration « Proxy » ni pour mettre à jour uniquement les pilotes des périphériques. Pour plus d'informations sur les états d'intégration, reportez-vous à la section Intégration de périphériques , page 45.
- Déployer des serveurs supplémentaires pour augmenter la fonctionnalité de calcul en période de forte charge de travail.L'état de conformité des firmwares ou des pilotes des commutateurs réseau, des IOA modulaires et des appareils de stockage Dell s'affiche comme « Inconnu », car ils ne peuvent pas être mis à jour à l'aide du catalogue Dell. Il est recommandé d'effectuer des mises à jour individuelles des firmwares ou des pilotes pour ces périphériques en utilisant leur package de mise à jour individuel. Pour effectuer des mises à jour individuelles des firmwares ou des pilotes, sélectionnez un périphérique sur la page Tous les périphériques, puis cliquez sur **Afficher les détails** > **Firmwares/Pilotes** et sélectionnez l'option Package individuel. Pour plus d'informations sur la liste des périphériques non pris en charge, reportez-vous à Rapports de ligne de base de conformité du firmware et du pilote : appareils dont l'état de conformité est « Inconnu » , page 184

Si le groupe de gestion multi-châssis (MCM) est géré à l'aide d'une version d'OpenManage Enterprise-Modular antérieure à la version 1.30.00, vous devez tenir compte des points suivants avant de mettre à jour le firmware et/ou les pilotes des traineaux et du châssis MX7000 :

- Les firmwares du châssis et du traineau doivent être mis à jour séparément.
- Le châssis maître doit être mis à jour séparément à l'étape finale, après la mise à jour de tous les châssis membres.
- Le firmware ne peut être mis à jour que pour un maximum de 9 châssis membres à la fois.
- La mise à jour de firmware est prise en charge sur un maximum de 43 traineaux à la fois, quel que soit l'état d'intégration (Géré ou Proxy).

Les mises à jour de pilote sont disponibles uniquement sur les périphériques détectés en tant que serveurs Windows 64 bits. Avant de mettre à jour les pilotes, procédez comme suit :

- N'oubliez pas que la restauration des mises à jour de pilote n'est pas prise en charge.
- Les mises à jour des pilotes intrabandes ne sont prises en charge que sur Windows avec OpenSSH. Les mises à jour de pilotes sur les SSH tiers hébergés sur Windows, telles que le SSH Cygwin, ne sont pas pris en charge.
- Pour collecter les informations relatives à l'inventaire, le collecteur d'inventaire et Dell System Update doivent être disponibles sur le serveur Windows. Si ces composants ne sont pas disponibles sur le serveur, lancez une tâche d'inventaire et sélectionnez **Collecter l'inventaire des pilotes**. La tâche de détection collecte également les informations relatives à l'inventaire des pilotes, mais seule la tâche d'inventaire installe les composants nécessaires sur le serveur. Pour collecter les informations relatives à l'inventaire des pilotes, créez ou modifiez une tâche d'inventaire, puis cochez la case **Collecter l'inventaire des pilotes**. Pour plus d'informations, voir Création d'une tâche d'inventaire , page 74 et Modification d'une tâche de planification d'inventaire , page 76.

Pour mettre à jour le firmware et/ou le pilote d'un périphérique en utilisant le rapport de conformité de ligne de base :

1. Sur la page **Configuration** > **Conformité du firmware/pilote**, cochez la case correspondant à la ligne de base à laquelle le périphérique est associé, puis cliquez sur **Afficher le rapport** dans le volet de droite.

   Sur la page **Rapport de conformité**, la liste des périphériques associés à la ligne de base et leur niveau de conformité respectif s'affiche. Pour obtenir la description des champs, voir Affichage du rapport de conformité de la ligne de base , page 83.
2. Cochez la case correspondant au périphérique dont le firmware ou le pilote doit être mis à jour. Vous pouvez sélectionner plusieurs périphériques qui ont des propriétés similaires.
3. Cliquez sur **Rendre conforme**.
4. Dans la boîte de dialogue **Rendre les périphériques conformes**, vous pouvez effectuer les opérations suivantes :
   - Sous **Planifier une mise à jour**, cliquez sur **Informations supplémentaires** pour afficher les informations importantes et sélectionnez l'une des options suivantes :
     a. **Mettre à jour maintenant** : applique les mises à jour de firmware/pilote immédiatement.
     b. **Programmer plus tard** : sélectionnez cette option pour spécifier la date et l'heure de mise à jour de la version du pilote et/ou du firmware. Ce mode est recommandé si vous ne souhaitez pas perturber les tâches en cours.
   - Sous **Options de serveur**, sélectionnez l'une des options de redémarrage suivantes :
     a. Pour redémarrer le serveur immédiatement après la mise à jour du firmware/pilote, choisissez **Redémarrer le serveur immédiatement**, puis, dans le menu déroulant, sélectionnez l'une des options suivantes :
        i. **Redémarrage normal sans arrêt forcé**
        ii. **Redémarrage normal avec arrêt forcé**
        iii. **Cycle d'alimentation** pour une réinitialisation matérielle du périphérique.
     b. Sélectionnez **Programmer le prochain redémarrage du serveur** pour déclencher la mise à jour du firmware/pilote lors du prochain redémarrage du serveur.

        REMARQUE : Si les tâches de mise à jour du firmware/pilote sont créées à l'aide de l'option « Programmer le prochain redémarrage du serveur », la vérification de l'inventaire et de la ligne de base doit être exécutée manuellement après l'installation du package sur le périphérique distant.
   - **Effacer la file d'attente des tâches** : sélectionnez cette option pour supprimer toutes les tâches (planifiées, terminées et ayant échoué) sur le périphérique cible avant le lancement de la tâche de mise à jour.

     REMARQUE : Cette fonction n'est pas prise en charge pour la mise à jour des pilotes.
   - **Réinitialiser l'iDRAC** : sélectionnez cette option pour lancer un redémarrage de l'iDRAC avant le lancement de la tâche de mise à jour.

     REMARQUE : Cette fonction n'est pas prise en charge pour la mise à jour des pilotes.
5. Cliquez sur **Mettre à jour**.

Une tâche de mise à jour de firmware/pilote est créée pour mettre à jour le firmware et/ou le pilote du périphérique. Vous pouvez afficher l'état de la tâche sur la page **Surveiller** > **Tâches**.

11

Gérer des modèles de déploiement d'appareil

Le modèle de déploiement d'appareil dans OpenManage Enterprise vous permet de définir les propriétés de configuration, telles que les propriétés réseau, de démarrage, du BIOS, etc. pour les serveurs et les châssis.

Le modèle de déploiement est une consolidation des paramètres de configuration système appelés attributs. Le modèle de déploiement permet de configurer rapidement et automatiquement plusieurs serveurs ou châssis sans risque d'erreur humaine.

Les modèles vous permettent d'optimiser vos ressources de datacenter et de réduire la durée du cycle lors de la création de clones et les déploiements. Par ailleurs, les modèles améliorent vos opérations stratégiques dans une infrastructure convergée qui utilise des infrastructures software-defined.

Vous pouvez utiliser les modèles de déploiement prédéfinis ou importer les modèles de déploiement à partir d'un appareil de référence ou d'un fichier de modèle existant. Pour afficher la liste des modèles existants, cliquez sur **Configuration** > **Modèles** dans le menu OpenManage Enterprise.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Un gestionnaire de périphériques peut afficher et effectuer des tâches sur les modèles par défaut, ainsi que sur les modèles personnalisés détenus par le gestionnaire de périphériques.

Sujets :

Créer un modèle de déploiement à partir d'un appareil de référence

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

Vous pouvez créer ou modifier un modèle de déploiement en utilisant un appareil de référence ou en procédant à une importation depuis un modèle de déploiement existant. Pour créer un modèle en utilisant un périphérique de référence :

1. Dans le menu **OpenManage Enterprise**, cliquez sur **Configuration** > **Modèles** > **Créer un modèle**, puis sélectionnez **À partir d'un périphérique de référence**.
2. Dans la boîte dialogue **Créer un modèle** :
   a. Dans la section **Informations sur le modèle**, saisissez le nom et la description du modèle de déploiement.
   b. Sélectionnez le type de modèle de déploiement :
      - **Cloner le serveur de référence** : permet de cloner la configuration d'un serveur existant.
      - **Cloner le châssis de référence** : permet de cloner la configuration d'un châssis existant.
      - **Cloner l'IOA de référence** : permet de cloner la configuration d'un agrégateur d'E/S M.

        REMARQUE : Les attributs du modèle IOA ne peuvent pas être modifiés. Seuls le **nom** et la **description** d'un modèle IOA peuvent être modifiés.

   c. Cliquez sur **Suivant**.
   d. Dans la section **Périphérique de référence**, cliquez sur **Sélectionner un périphérique** pour sélectionner l'appareil dont les propriétés de configuration doivent être utilisées pour la création du modèle de déploiement. Pour en savoir plus sur la sélection des périphériques, voir Sélection de périphériques et de groupes de périphériques cibles.

      REMARQUE : seul un périphérique peut être sélectionné en tant que périphérique de référence.

      REMARQUE : Seuls les modèles d'IOA extraits lors de la détection du boîtier peuvent être clonés. Voir Création de protocole de tâche de détection d'appareils personnalisé pour les serveurs : paramètres supplémentaires pour les protocoles de détection , page 50
   e. Dans la section **Éléments de configuration**, cochez les cases correspondant aux éléments de périphériques qui doivent être clonés. Pour créer un modèle de déploiement en utilisant un serveur en tant qu'appareil, vous pouvez choisir de cloner les propriétés de serveur telles que le contrôleur iDRAC, le BIOS, Lifecycle Controller et les filtres d'événements. Par défaut, tous les éléments sont sélectionnés.
   f. Cliquez sur **Terminer**.
   Une fois que la création a été correctement effectuée, la tâche s'affiche dans la liste. Une tâche de création de modèle de déploiement est démarrée et l'état est affiché dans la colonne **ÉTAT**.

   Les informations relatives à la tâche s'affichent également sur la page **Surveiller** > **Tâches**. Pour afficher davantage de détails sur une tâche, sélectionnez-la et cliquez sur **Afficher les détails** dans le volet en cours. Les détails de l'exécution de la tâche s'affichent sur la page **Détails de la tâche**. Dans le volet **Résultats**, cliquez sur **Afficher les détails** pour afficher les informations détaillées de l'exécution de la tâche.

Créer un modèle de déploiement en important un fichier de modèle

REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.

1. Dans le menu **OpenManage Enterprise**, cliquez sur **Configuration** > **Modèles** > **Créer un modèle**, puis sélectionnez **Importer à partir d'un fichier**.
2. Dans la boîte de dialogue **Importer un modèle** :
   a. Saisissez un nom pour le nouveau modèle de déploiement.
   b. Cliquez sur **Sélectionner un fichier**, puis sélectionnez le fichier d'un modèle.
   c. Sélectionnez **Serveur**, **Châssis** ou **IOA** pour indiquer le type de modèle.
3. Cliquez sur **Terminer**.
   Les propriétés d'un fichier de modèle existant sont importées et un modèle de déploiement est créé.

- Pour afficher les informations relatives à un modèle de déploiement, cochez la case, puis cliquez sur **Afficher les détails** dans le volet de droite. Sur la page **Détails du modèle**, vous pouvez déployer ou modifier un modèle de déploiement. Voir Déployer des modèles de déploiement d'appareil , page 90 et Créer un modèle de déploiement à partir d'un appareil de référence , page 86.
- Pour modifier un modèle de déploiement :
  1. Cochez la case correspondante, puis cliquez sur **Modifier**.

2. Dans la boîte de dialogue **Modifier le modèle**, modifiez le nom du modèle de déploiement, puis cliquez sur **Terminer**. Les informations mises à jour s'affichent dans la liste des modèles de déploiement.

Afficher les informations relatives à un modèle de déploiement

Une liste de modèles de déploiement d'appareils prédéfinis, créés par l'utilisateur ou clonés est affichée dans **Configuration** > **Modèles**.

1. Dans la liste des modèles de déploiement, cochez la case correspondant au modèle de d'appareil obligatoire.
2. Dans le volet actuel, cliquez sur **Afficher les détails**.
   Sur la page **Détails du modèle**, les informations suivantes s'affichent : nom du modèle de déploiement, description, appareil de référence à partir duquel le modèle de déploiement a été créé et dernière date de mise à jour par l'utilisateur OpenManage Enterprise.
3. Cliquez avec le bouton droit de la souris sur un élément pour développer ou réduire tous les éléments enfants dans la section **Détails de la configuration**, afin d'afficher l'ensemble des attributs utilisés pour créer le modèle de déploiement. Vous pouvez également développer des éléments enfants individuels spécifiques à un élément parent. Par exemple, si vous avez choisi d'utiliser les éléments d'iDRAC et du BIOS pour le clonage sur le périphérique cible, seuls les attributs associés à ces éléments s'affichent.

Modifier un modèle de déploiement de serveur

Les modèles de déploiement intégrés ne peuvent pas être modifiés. Seuls les modèles de déploiement créés par l'utilisateur et personnalisés peuvent être modifiés. Vous pouvez modifier les attributs d'un modèle de déploiement que vous l'ayez créé en utilisant un fichier de modèle de référence ou un appareil de référence. Lors de la modification d'un modèle, la sélection ou la désélection des attributs ne modifie pas les attributs stockés dans le modèle et tous les attributs font toujours partie du modèle s'il est exporté. Cela a une incidence sur ce qui est déployé.

1. Sur la page **Configuration** > **Modèles**, cochez la case du modèle personnalisé qui convient, puis cliquez sur **Modifier**.
2. Dans la boîte de dialogue **Modifier un modèle** :
   a. Dans la section **Informations sur le modèle**, modifiez le nom du modèle de déploiement et la description. Le type de modèle ne peut pas être modifié.
   b. Cliquez sur **Suivant**.
   c. Dans la section **Modifier des composants**, les attributs du modèle de déploiement s'affichent dans :
      - **Vue guidée** : cette vue des attributs affiche uniquement les attributs communs, regroupés par fonction. Les attributs des catégories suivantes sont affichés :
        i. Dans la section **Paramètres du BIOS**, sélectionnez l'une des options suivantes :
           - **Manuellement** : vous permet de définir manuellement les propriétés du BIOS suivantes :
             - **Profil du système** : dans le menu déroulant, sélectionnez cette option pour indiquer le type d'optimisation des performances à atteindre dans le profil du système.
             - **Ports USB accessibles par l'utilisateur** : depuis le menu déroulant, sélectionnez cette option pour indiquer les ports auxquels l'utilisateur peut accéder.
             - Par défaut, l'utilisation du processeur logique et la facilité de gestion intrabande sont activés.
           - **Optimisation en fonction de la charge applicative** : dans le menu déroulant Sélectionnez le profil de charge applicative, indiquez le type d'optimisation des performances de la charge applicative que vous souhaitez obtenir sur le profil.
        ii. Cliquez sur **Démarrer** et définissez le mode d'amorçage :
           - Si vous sélectionnez le BIOS en tant que le mode d'amorçage, effectuez les opérations suivantes :
             - Pour réessayer la séquence de démarrage, cochez la case **Activé**.
             - Faites glisser les éléments pour définir la séquence de démarrage et la séquence de disque dur.
           - Si vous sélectionnez le mode de démarrage UEFI en tant que, faites glisser les éléments pour définir la séquence de démarrage UEFI. Si nécessaire, cochez la case pour activer la fonctionnalité de démarrage sécurisé.
        iii. Cliquez sur **Mise en réseau**. Tous les réseaux associés au modèle de déploiement s'affichent sous **Interfaces réseau**.
           - Pour associer un pool facultatif d'identités au modèle de déploiement, sélectionnez le pool à partir du menu déroulant **Pool d'identités**. Les réseaux associés au pool d'identités sélectionné s'affichent. Si le modèle de déploiement est modifié dans la vue avancée, la sélection du pool d'identités est désactivée pour ce modèle de déploiement.
             - Pour afficher les propriétés du réseau, développez le réseau.
             - Pour modifier les propriétés, cliquez sur le symbole stylo correspondant.
               - Sélectionnez le protocole à utiliser pour le démarrage. Sélectionnez-le uniquement si le protocole est pris en charge par votre réseau.

- Sélectionnez le réseau balisé ou non balisé à associer au réseau
- Les bandes passantes maximale, minimale et de partition s'affichent à partir du modèle de déploiement (profil) créé plus tôt.

▪ Cliquez sur **Terminer**. Les paramètres réseau du modèle de déploiement sont enregistrés.

- **Vue avancée** : cette vue répertorie tous les attributs de modèle de déploiement qui peuvent être modifiés (y compris ceux affichés dans la Vue guidée). Cette vue vous permet de spécifier non seulement des valeurs d'attribut (comme dans la Vue guidée), mais également si chaque attribut est inclus ou non lorsque le modèle de déploiement est déployé sur un appareil cible.

  Les attributs sont regroupés de façon pratique pour l'affichage. Les attributs spécifiques au fournisseur sont regroupés sous Autres attributs. Chaque attribut s'affiche avec une case à cocher précédant son nom. La case à cocher indique si l'attribut sera inclus ou non lorsque le modèle de déploiement est déployé sur un appareil cible. En raison des dépendances d'attributs, si vous modifiez le paramètre pour savoir si un attribut particulier est déployé, cela peut générer des résultats inattendus sur l'appareil cible ou provoquer l'échec du déploiement. Chaque groupe dispose également d'une case à cocher située à gauche de son nom. L'une des trois icônes suivantes peut être affichée dans les cases à cocher des groupes :

  i. Coche – Indique que tous les attributs du groupe sont sélectionnés pour le déploiement.
  ii. Tiret – Indique que certains des attributs sont sélectionnés pour le déploiement.
  iii. Vide – Indique qu'aucun attribut du groupe n'est sélectionné pour le déploiement.

  REMARQUE :
  - Pour utiliser cette option, vous devez procéder avec prudence et disposer d'une connaissance suffisante des attributs et des dépendances d'attributs, car certains attributs dépendent de la valeur d'un autre attribut, qui détermine leur comportement.
  - Vous pouvez cliquer sur les icônes de groupe pour basculer entre les paramètres de déploiement de tous les attributs du groupe.
  - Les attributs contenant des informations sécurisées, comme les mots de passe, sont masqués et apparaissent « vides » lors du chargement initial tandis que les modifications apportées à ces valeurs d'attributs sécurisés sont masquées.
  - Le pool d'identités associé à un modèle de déploiement ne peut pas être modifié s'il est déjà associé à un profil.

3. Cliquez sur **Suivant**.
   Dans la section **Résumé**, les attributs que vous modifiez à l'aide des modes Avancé et Guidé s'affichent.
4. Cette section est en lecture seule. Vérifiez les paramètres, puis cliquez sur **Terminer**.
   Les attributs du modèle mis à jour sont enregistrés dans le modèle de déploiement.

Modifier un modèle de déploiement de châssis

La modification des modèles de déploiement de châssis est possible avec OpenManage Enterprise. Lors de la modification d'un modèle, la sélection ou la désélection des attributs ne modifie pas les attributs stockés dans le modèle et tous les attributs font toujours partie du modèle s'il est exporté. Cela a une incidence sur ce qui est déployé.

REMARQUE :
- Pour modifier des modèles de déploiement de châssis, vous devez posséder les privilèges d'un administrateur ou d'un gestionnaire d'appareils. Pour plus de détails, consultez Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les mots de passe utilisateur ne peuvent pas être définis sur le châssis MX7000 et les modèles de déploiement CMC (Chassis Management Controller).

Pour modifier un modèle de déploiement de châssis :

1. Sélectionnez **OpenManage Enterprise** > **Configuration** > **Modèles** pour obtenir la liste des modèles de déploiement.
2. Cochez la case correspondant au modèle de boîtier requis, puis cliquez sur **Modifier**. Assurez-vous que le modèle de déploiement est identifié comme "Personnalisé".
3. Modifiez le **Nom du modèle** et sa **Description** dans la section **Informations sur le modèle**. Vous ne pouvez pas modifier le **Type de modèle**.
4. Cliquez sur **Suivant**.
5. Dans la section **Modifier les composants**, sous **Vue avancée**, vous pouvez cocher ou décocher les attributs à inclure ou non au modèle de déploiement.
6. Cliquez sur **Suivant**.
7. Vous pouvez vérifier les modifications apportées aux attributs, sous **Résumé**. Un cercle apparaît en regard des attributs modifiés.

8. Cliquez sur **Terminer** pour enregistrer les modifications apportées au modèle de déploiement de châssis.

Modifier un modèle de déploiement IOA

Les attributs du modèle de déploiement IOA ne peuvent pas être modifiés. Seuls le **nom** et la **description** d'un modèle de déploiement IOA peuvent être modifiés.

REMARQUE :

Les attributs de modèle IOA ne doivent pas être modifiés en dehors de l'appliance, étant donné que le modèle est considéré comme un fichier corrompu lors du déploiement.

Modifier les propriétés réseau d'un modèle de déploiement

Sur la page **Configuration** > **Modèles**, vous pouvez modifier la configuration réseau des modèles de déploiement contenant les attributs de carte NIC applicables.

Après avoir sélectionné un modèle de déploiement, cliquez sur **Modifier le réseau** pour activer l'Assistant Modifier le réseau, puis procédez comme suit :

REMARQUE : Les paramètres VLAN sur les traîneaux MX7000 en proxy dans le périmètre sont autorisés pour un gestionnaire de périphériques, même si le châssis MX7000 est hors du périmètre.

1. Cliquez sur **Attribution d'un pool d'E/S**, puis, dans la liste **Pool d'identités**, sélectionnez un pool d'identités pour le modèle de déploiement. Cliquez sur **Suivant**.
2. Dans la section **Bande passante**, modifiez les valeurs des paramètres **Bande passante minimale (%)** et **Bande passante maximale (%)** des cartes NIC associées, puis cliquez sur **Suivant**.

   REMARQUE : Les paramètres de bande passante s'appliquent uniquement aux cartes NIC partitionnées.

3. Dans la section **VLAN** (applicable uniquement pour les systèmes modulaires) :
   a. Sélectionnez une option **Association de cartes NIC** appropriée.
   b. Cochez la case **Propager immédiatement les paramètres VLAN** pour propager immédiatement les paramètres VLAN modifiés sur les serveurs système modulaires associés sans nécessité de redémarrage du serveur. Cliquez sur **Afficher les détails** pour afficher les périphériques qui seraient affectés.

      REMARQUE :
      - L'option **Propager immédiatement les paramètres VLAN** est appliquée uniquement si le modèle de déploiement a déjà été déployé.
      - Avant de propager les paramètres VLAN, assurez-vous que les profils réseau sont déjà créés pour les serveurs du système modulaire dans la structure.
      - Si la case **Propager immédiatement les paramètres VLAN** est cochée, une tâche nommée **Propagation VLAN** est créée pour appliquer les modifications. L'état de la tâche peut être vérifié sur la page **Surveiller** > **Tâches**.

   c. Cochez la case **Utiliser une vérification stricte** pour faire correspondre les VLAN présentant des caractéristiques similaires. Si cette option est désactivée, seuls le nom du VLAN et la QoS sont utilisés pour la mise en correspondance.

      REMARQUE : Cette option s'applique uniquement aux sleds de systèmes modulaires.

   d. Si nécessaire, apportez des modifications aux attributs **Réseau non marqué** et **Réseau marqué** des cartes NIC associées.
4. Cliquez sur **Terminer** pour appliquer les modifications.

Déployer des modèles de déploiement d'appareil

Vous pouvez déployer un modèle de déploiement qui inclut un ensemble d'attributs de configuration sur des appareils spécifiques. Le déploiement d'un modèle de déploiement d'appareil sur les appareils permet d'uniformiser la configuration de ces derniers.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Si un gestionnaire de périphériques déploie des modèles, seuls les groupes cibles et les périphériques qui sont dans le périmètre du gestionnaire de périphériques et qui sont capables de faire l'objet d'un déploiement s'affichent.

Avant de commencer à déployer un modèle de déploiement de périphérique, assurez-vous que :

- Vous avez créé un modèle de déploiement d'appareil ou cloné un exemple de modèle de déploiement. Voir Créer un modèle de déploiement à partir d'un appareil de référence , page 86.
- Les périphériques cibles remplissent les conditions spécifiées à la rubrique Configuration matérielle minimale requise pour le déploiement d'OpenManage Enterprise , page 21.
- La licence OpenManage Enterprise Advanced est installée sur tous les appareils cibles.

PRÉCAUTION : Assurez-vous que seuls les périphériques appropriés sont sélectionnés pour le déploiement. Après avoir déployé un modèle de déploiement sur un appareil vierge et recyclé, il n'est pas toujours possible de rétablir la configuration d'origine de l'appareil.

REMARQUE : Lors du déploiement d'un modèle de châssis MX7000 :

- Le périphérique cible peut uniquement être le châssis MX7000 maître.
- Si un châssis MX7000 est supprimé du groupe, il doit être redétecté dans OpenManage Enterprise.
- Les utilisateurs sur le châssis MX7000 sont remplacés par les utilisateurs configurés dans le modèle.
- Les paramètres d'Active Directory importés sont remplacés par les valeurs du profil de châssis.

1. Dans la liste des modèles de déploiement de la page **Configuration** > **Modèles**, cochez la case correspondant au modèle de déploiement que vous souhaitez déployer, puis cliquez sur **Déployer le modèle**.
2. Dans la boîte de dialogue **Déployer le modèle : <nom_du_modèle>**, sous **Cible** :
   a. Cliquez sur **Sélectionner**, puis sélectionnez le ou les périphériques dans la boîte de dialogue **Tâche cible**. Voir Sélection de périphériques et de groupes de périphériques cibles.
   b. Lors du déploiement du modèle de déploiement d'appareil, les modifications de configuration peuvent nécessiter un redémarrage forcé du serveur. Si vous ne souhaitez pas redémarrer le serveur, sélectionnez l'option **Ne pas forcer le redémarrage du système d'exploitation hôte**.
   Une tentative de redémarrage normal du serveur est effectuée lorsque l'option **Ne pas forcer le redémarrage du système d'exploitation hôte** est sélectionnée. Si le redémarrage échoue, vous devez exécuter de nouveau la tâche de déploiement du modèle.
   c. Cochez la case **Utiliser une vérification stricte** pour faire correspondre les VLAN présentant des caractéristiques similaires. Si cette option est désactivée, seuls le nom du VLAN et la QoS sont utilisés pour la mise en correspondance.
      REMARQUE : Cette option s'affiche uniquement si les périphériques cibles sélectionnés sont des traineaux de systèmes modulaires.
   d. Cliquez sur **Suivant**.
3. Si le périphérique cible est un serveur, dans la section **Démarrer à partir de l'image ISO du réseau** :
   a. Cochez la case **Amorcer à partir de l'image ISO du réseau**.
   b. Sélectionnez **CIFS** ou **NFS** comme type de partage, puis saisissez les informations dans les champs, par exemple le chemin d'accès au fichier d'image ISO et l'emplacement de partage où ce fichier est stocké. Utilisez les info-bulles pour entrer la syntaxe correcte.
   c. Sélectionnez les options du menu déroulant **Durée de liaison de l'image ISO** pour définir le nombre d'heures pendant lesquelles le fichier ISO du réseau reste mappé sur le ou les périphériques cibles. Par défaut, cette valeur est définie sur quatre heures.
   d. Cliquez sur **Suivant**.
4. Dans la section **IP de gestion de l'iDRAC**, modifiez les paramètres IP du périphérique cible si nécessaire, puis cliquez sur **Suivant**.
   REMARQUE :
   - Le déploiement du modèle échoue si les paramètres DHCP sont attribués lors du déploiement du modèle sur un périphérique cible initialement découvert à l'aide d'une adresse IP statique.
   - Si le paramètre IP n'est pas configuré sur le traîneau MX7000 détecté, l'opération Amorcer à partir d'une image ISO de réseau n'est pas exécutée pendant le déploiement de modèles.
5. Dans la section **Attributs cibles**, les attributs d'identités non virtuelles propres à chaque appareil cible sélectionné, tels que les attributs d'emplacement et l'adresse IP, peuvent être modifiés avant de déployer le modèle de déploiement. Lorsque le modèle est

déployé, ces attributs cibles modifiés sont implémentés uniquement sur les périphériques spécifiques. Pour modifier les attributs d'identité non virtuels propres au périphérique :

a. Sélectionnez un périphérique cible dans la liste qui répertorie les périphériques cibles précédemment sélectionnés.
b. Développez les catégories d'attributs, puis sélectionnez ou désélectionnez les attributs qui doivent être inclus ou exclus lors du déploiement du modèle sur le périphérique cible.
c. Cliquez sur **Suivant**.

6. Dans la section **Identités virtuelles**, cliquez sur **Réserver des identités**.
Les identités virtuelles attribuées pour les cartes d'interface réseau de l'appareil cible sélectionné s'affichent. Pour afficher toutes les identités attribuées du pool d'identités de l'appareil cible sélectionné, cliquez sur **Afficher tous les détails de la carte d'interface réseau**.
REMARQUE : Si des identités sont déjà attribuées en dehors de l'appliance, ces identités ne seront utilisées dans un nouveau déploiement que si elles sont désactivées. Pour en savoir plus, voir Pools d'identités , page 96
7. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
8. Cliquez sur **Terminer**. Passez en revue le message d'avertissement, puis cliquez sur **OUI**.
Une tâche de configuration de périphérique est créée. Voir Utilisation des tâches pour le contrôle de périphériques , page 129.

Déployer des modèles de déploiement IOA

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Avant de commencer à déployer un modèle de déploiement IOA, assurez-vous que :

- Vous avez créé un modèle de déploiement IOA pour le déploiement. Voir Créer un modèle de déploiement à partir d'un appareil de référence , page 86.
- Les périphériques cibles remplissent les conditions spécifiées à la rubrique Configuration matérielle minimale requise pour le déploiement d'OpenManage Enterprise , page 21.
- La version du firmware de l'appareil cible est la même que dans le modèle de déploiement IOA.
- Seuls les déploiements de modèles transversaux suivants sont pris en charge :

Tableau 14. Déploiements de modèles transversaux pris en charge

Mode de modèle de déploiement IOA	Modes de modèle IOA pris en charge de la cible
Autonome	Autonome, PMUX
PMUX (MUX programmable)	PMUX, Autonome
VLT	VLT

PRÉCAUTION : Assurez-vous que seuls les périphériques appropriés sont sélectionnés pour le déploiement. Après avoir déployé un modèle de déploiement sur un appareil vierge et recyclé, il n'est pas toujours possible de rétablir la configuration d'origine de l'appareil.

1. Dans la liste des modèles de déploiement de la page **Configuration** > **Modèles**, cochez la case correspondant au modèle IOA que vous souhaitez déployer, puis cliquez sur **Déployer le modèle**.
2. Dans la boîte de dialogue **Déployer le modèle : <nom_du_modèle>**, sous **Cible** :
   a. Cliquez sur **Sélectionner**, puis sélectionnez le ou les périphériques dans la boîte de dialogue **Tâche cible**. Voir Sélection de périphériques et de groupes de périphériques cibles.
   b. Cliquez sur **OK**.
3. Dans la boîte de dialogue **Noms de l'hôte**, vous pouvez modifier le **Nom de l'hôte** de l'appareil IOA cible. Cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Options avancées**, sélectionnez **Mode de prévisualisation** pour simuler le déploiement, ou sélectionnez **Continuer en cas d'avertissement** pour déployer le modèle et ignorer les avertissements rencontrés. Cliquez sur **Suivant**.
5. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
6. Cliquez sur **Terminer**. Passez en revue le message d'avertissement, puis cliquez sur **OUI**.
Une tâche de configuration de périphérique est créée sous Tâches. Voir Utilisation des tâches pour le contrôle de périphériques , page 129.

Cloner des modèles de déploiement

1. Dans le menu **OpenManage Enterprise**, sous **Configuration**, cliquez sur **Modèles**.
   Une liste des modèles de déploiement disponibles s'affiche.
2. Cochez la case correspondant au modèle que vous souhaitez cloner.
3. Cliquez sur **Cloner**.
4. Saisissez le nom du nouveau modèle de déploiement, puis cliquez sur **Terminer**.
   Le modèle de déploiement cloné est créé et s'affiche dans la liste des modèles de déploiement.

Configuration de déploiement automatique sur les serveurs ou châssis qu'il reste à détecter

Les modèles de déploiement existants dans OpenManage Enterprise peuvent être attribués aux serveurs et châssis attendant d'être détectés. Ces modèles de déploiement sont automatiquement déployés sur les différents appareils lorsqu'ils sont détectés et intégrés.

Pour accéder à la page **Déployer automatiquement**, cliquez sur **OpenManage Enterprise** > **Configuration** > **Déployer automatiquement**.

Les cibles de déploiement automatique et leur **identificateur** respectif (numéro de série ou ID de nœud), **nom de modèle**, **type de modèle**, **état**, et **État d'amorçage à partir de l'image ISO du réseau** (pour les serveurs) s'affichent.

La liste de cibles de **Déploiement automatique** peut être personnalisée à l'aide des champs **Filtres avancés** disponibles en haut de la liste.

La section sur le côté droit de la page Déployer automatiquement affiche les informations **Créé sur** et **Créé par** de la cible de déploiement automatique sélectionnée. Lorsque plusieurs éléments sont sélectionnés, les informations sur le dernier élément sélectionné s'affichent dans cette section.

Une fois qu'une cible de déploiement automatique est détectée, son entrée à partir de la page Déploiement automatique est automatiquement supprimée et déplacée vers la page Tous les périphériques. En outre, un profil est créé sur la page Profils qui contient les paramètres de configuration du périphérique.

Les actions suivantes peuvent être effectuées sur la page Déployer automatiquement :

- **Créer** des modèles pour le déploiement automatique. Voir Création de cibles de déploiement automatique , page 93
- **Supprimer** des modèles qui ne sont pas nécessaires. VoirSuppression des cibles de déploiement automatique , page 94
- **Exporter** les modèles de déploiement automatique sous différents formats. Voir Export des informations de la cible de déploiement automatique en différents formats , page 95

REMARQUE :

- Seuls les administrateurs peuvent effectuer les tâches de création, suppression et exportation sur les modèles de déploiement automatique. Les gestionnaires de périphériques peuvent uniquement « exporter » les modèles de déploiement automatique. Pour plus d'informations, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Création de cibles de déploiement automatique

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

Pour créer des cibles de déploiement automatique :

1. Cliquez sur **OpenManage Enterprise** > **Configuration** > **Déployer automatiquement** > **Créer**
   L'Assistant **Modèle de déploiement automatique** s'affiche.
2. Sur la page **Informations sur le modèle**, sélectionnez le type de modèle de déploiement (serveur ou châssis).
3. Dans le menu déroulant **Modèle**, sélectionnez un modèle approprié. Si le modèle sélectionné possède des attributs d'identité n'étant pas associés à un pool d'identités virtuel, le message suivant s'affiche : *Le modèle sélectionné possède des attributs d'identité, mais ils n'ont pas été associés à un pool d'identités virtuel. Le déploiement de ce modèle ne modifiera pas les adresses réseau virtuel sur les appareils cibles.*
4. Cliquez sur Suivant.

La page **Informations sur la cible** s'affiche.

5. Sur la page **Informations sur la cible**, les appareils cibles peuvent être sélectionnés en utilisant l'une des méthodes suivantes :
   - **Saisie manuelle** : saisissez le numéro de série ou ID de nœud pour identifier les appareils cibles. Les identificateurs peuvent être saisis dans n'importe quel ordre, cependant, ils doivent être séparées par des virgules. Cliquez sur Valider pour vérifier l'exactitude des valeurs. Il est obligatoire de valider les identificateurs.
   - **Importation au format CSV** : cliquez sur **Importer CSV** pour parcourir les dossiers correspondants et sélectionnez le fichier .csv comportant les informations de l'appareil cible. Un récapitulatif du nombre d'entrées correctement importées et du nombre d'entrées non valides est affiché. Pour obtenir une vue plus détaillée du résultat de l'importation, cliquez sur **Afficher les détails**.

     Les entrées du fichier CSV doivent respecter le format suivant : les ID doivent être répertoriés un par ligne dans la première colonne, en commençant par la deuxième ligne. Pour un fichier CSV de modèle, cliquez sur **Télécharger un exemple de fichier CSV**.
6. Cliquez sur **Suivant**.
7. Sur la page **Informations sur le groupe cible**, spécifiez un sous-groupe sous le **Groupe statique** si celui-ci est disponible. Pour plus d'informations sur le regroupement d'appareils, consultez Organisation des périphériques dans des groupes , page 55. Les appareils cibles seront placés sous le groupe cible spécifié lors de leur détection.
8. Cliquez sur **Suivant**.
9. Si l'appareil cible est un serveur, sur la page **Démarrer à partir de l'image ISO du réseau** :
   - Cochez la case **Amorcer à partir de l'image ISO du réseau**.
   - Sélectionnez **CIFS** ou **NFS**.
   - Saisissez le **Chemin d'accès de l'ISO** de l'emplacement sur lequel le fichier image ISO est stocké. Utilisez les info-bulles pour entrer la syntaxe correcte.
   - Renseignez les champs **Adresse IP de partage**, **Groupe de travail**, **Nom d'utilisateur**, et **Mot de passe**.
   - Sélectionnez les options du menu déroulant **Durée de liaison de l'image ISO** pour définir le nombre d'heures pendant lesquelles le fichier ISO du réseau reste mappé sur le ou les périphériques cibles. Par défaut, cette valeur est définie sur quatre heures.
   - Cliquez sur **Suivant**.
10. Sur la page **Identités virtuelles**, cliquez sur **Réserver des identités**.
    Les identités virtuelles attribuées pour les cartes d'interface réseau de l'appareil cible sélectionné s'affichent. Pour afficher toutes les identités attribuées du pool d'identités de l'appareil cible sélectionné, cliquez sur **Afficher tous les détails de la carte d'interface réseau**.
11. Dans la section **Attributs cibles**, les attributs d'identités non virtuelles propres à chaque appareil cible sélectionné, tels que les attributs d'emplacement et l'adresse IP, peuvent être modifiés avant de déployer le modèle de déploiement. Lorsque le modèle est déployé, ces attributs cibles modifiés sont implémentés uniquement sur les périphériques spécifiques. Pour modifier les attributs d'identité non virtuels propres au périphérique :
    a. Sélectionnez un périphérique cible dans la liste qui répertorie les périphériques cibles précédemment sélectionnés.
    b. Développez les catégories d'attributs, puis sélectionnez ou désélectionnez les attributs qui doivent être inclus ou exclus lors du déploiement du modèle sur le périphérique cible.
    c. Cliquez sur **Suivant**.
12. Cliquez sur **Terminer**.
    Un message d'alerte *Le déploiement d'un modèle peut entraîner une perte de données et un redémarrage de l'appareil. Êtes-vous sûr de vouloir déployer le modèle ?* s'affiche.
13. Cliquez sur **Oui**.
    Une nouvelle cible de déploiement automatique est créée et répertoriée sur la page **Déployer automatiquement**.

Suppression des cibles de déploiement automatique

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

REMARQUE : Si un modèle, associé aux cibles de déploiement automatique, est supprimé de la page **OpenManage Enterprise** > **Configuration** > **Modèles**, les entrées de déploiement automatique associées sont également supprimées indépendamment de leur état actuel.

Pour supprimer les cibles de déploiement automatique à partir de la liste **Déployer automatiquement** :

1. Accédez à la page Déployer automatiquement en cliquant sur **OpenManage Enterprise** > **Configuration** > **Déployer automatiquement**.
2. Sélectionnez les cibles de déploiement automatique dans la liste.

3. Cliquez sur **Supprimer** puis sur **Oui** pour confirmer.
   Les cibles de déploiement automatique sélectionnées pour suppression sont supprimées de la page Déployer automatiquement.

Export des informations de la cible de déploiement automatique en différents formats

1. Accédez à la page Déployer automatiquement en cliquant sur **OpenManage Enterprise** > **Configuration** > **Déployer automatiquement**.
2. Sélectionnez la cible de déploiement automatique dans la liste et cliquez sur **Exporter**.
3. Dans la boîte de dialogue **Exporter tout**, sélectionnez le format HTML, CSV ou PDF. Cliquez sur **Terminer**.
   Une tâche est créée et les données de cibles de déploiement automatique sont exportées au format sélectionné.

Présentation du déploiement sans état

Pour déployer un modèle de déploiement d'appareil avec des attributs d'identités virtuelles sur les appareils cibles, procédez comme suit :

1. **Créez un modèle d'appareil** : cliquez sur la tâche **Créer un modèle** sous l'onglet **Déployer** pour créer un modèle de déploiement. Vous pouvez choisir de créer un modèle à partir d'un fichier de configuration ou d'un périphérique de référence.
2. **Créez un pool d'identités** : cliquez sur la tâche **Créer** sous l'onglet **Pools d'identités** pour créer un pool d'un ou plusieurs types d'identité d'identités.
3. **Attribuez des identités virtuelles à un modèle d'appareil :** sélectionnez un modèle de déploiement dans le volet **Modèles**, puis cliquez sur **Modification de réseau** pour attribuer un pool d'identités au modèle de déploiement. Vous pouvez également sélectionner le réseau balisé et non balisé, puis attribuer la bande passante maximum et minimum aux ports.
4. **Déployez le modèle de déploiement sur les appareils cibles** : utilisez la tâche **Déployer le modèle** sous l'onglet **Déployer** pour déployer le modèle de déploiement et les identités virtuelles sur les appareils cibles.

Gestion des pools d'identités — Déploiement sans état

Les interfaces d'E/S d'un serveur, telles que cartes réseau ou adaptateurs HBA, possèdent des attributs d'identité uniques attribués par le fabricant des interfaces. Ces attributs d'identité uniques forment collectivement l'identité d'E/S d'un serveur. Les identités d'E/S permettant d'identifier un serveur sur un réseau, mais également de déterminer la façon dont le serveur communique avec une ressource réseau à l'aide d'un protocole spécifique. OpenManage Enterprise vous permet de générer et d'attribuer automatiquement des attributs d'identité virtuels aux interfaces d'E/S d'un serveur.

Les serveurs déployés à l'aide d'un modèle de déploiement d'appareil qui contient des identités d'E/S virtuelles sont considérés comme sans état. Les déploiements sans état vous permettent de créer un environnement de serveur dynamique et flexible. Par exemple, le déploiement d'un serveur avec des identités d'E/S virtuelles dans un environnement de démarrage à partir du réseau SAN vous permet d'effectuer rapidement les opérations suivantes :

- Remplacer un serveur défaillant en transférant l'identité d'E/S du serveur vers un autre serveur de secours.
- Déployer des serveurs supplémentaires pour augmenter la fonctionnalité de calcul en période de forte charge applicative.

La page **OpenManage Enteprise** > **Configuration** > **Pools d'identités** vous permet de créer, modifier, supprimer ou exporter des pools d'E/S virtuelles.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Les restrictions basées sur le périmètre ne s'appliquent pas aux pools d'identités. Par conséquent, tous les pools d'identification peuvent être affichés et utilisés par tous les types d'utilisateurs Toutefois, une fois que le gestionnaire de périphériques attribue des identités, il est le seul à pouvoir les consulter et les utiliser.

Créer un pool d'identités - Informations de pool

Les pools d'identité sont utilisés lors du déploiement d'un serveur basé sur un modèle pour virtualiser l'identité du réseau pour les éléments suivants :

- Ethernet
- iSCSI
- Fibre Channel Over Ethernet (FCoE)
- Fibre Channel (FC)

Vous pouvez créer un maximum de 5 000 pools d'identité dans chacune de ces catégories.

Le processus de déploiement de serveur récupère la prochaine identité disponible dans le pool et l'utilise tout en fournissant un serveur à partir de la description du modèle. Vous pouvez ensuite migrer le profil d'un serveur sur un autre sans perdre l'accès au réseau ou aux ressources de stockage dans votre environnement.

Vous pouvez modifier le nombre d'entrées dans le pool. Cependant, vous ne pouvez pas définir un nombre d'entrées inférieur à celui affecté ou réservé. Vous pouvez également supprimer les entrées qui ne sont pas attribuées ni réservées.

REMARQUE : La modification du pool d'identités échoue lorsque les plages d'identités se chevauchent. L'échange n'est pas autorisé si vous avez des pools d'identité configurés pour Ethernet, FCoE et iSCSI et si vous essayez de modifier et d'échanger l'adresse de départ qui chevauche la plage existante. Pour échanger l'adresse MAC de départ, vous devez la sortir de la plage conflictuelle, une section à la fois.

Nom du pool	Saisissez un nom pour le pool d'identités. Le nom de pool peut contenir un maximum de 255 caractères.
Description	Saisissez une description pour le pool d'identités. La description peut contenir un maximum de 255 caractères.

Actions

Suivant	Affiche l'onglet **Ethernet**.
Terminer	Enregistre les modifications et affiche la page **Pools d'identités**.
Annuler	Ferme l'assistant **Créer un pool d'identités** sans enregistrer les modifications.

Pools d'identités

Un pool d'identités est un ensemble d'un ou plusieurs types d'identités virtuelles nécessaires à la communication réseau. Un pool d'identités peut contenir une combinaison des types d'identités virtuelles suivants :

- Identités Ethernet

  Les identités définies par l'adresse MAC (Media Access Control). Les adresses MAC sont requises pour les communications Ethernet (LAN).

- Identités iSCSI

  Identités définies par le nom IQN (iSCSI Qualified Name). Des identités IQN sont requises pour la prise en charge du démarrage à partir d'un SAN à l'aide du protocole iSCSI.

- Identités Fibre Channel (FC)

  Identités définies par le nom WWNN (World Wide Node Name) et le nom WWPN (World Wide Port Name). Un nom WWNN identité est attribué à un nœud (périphérique) dans une structure FC et peut être partagé par certains ou tous les ports d'un périphérique. Un nom WWPN identité est attribué à chaque port d'une structure FC et est propre à chaque port. Les identités WWNN et WWPN sont requises pour la prise en charge du démarrage à partir d'un SAN et pour l'accès aux données via les protocoles FC et FCoE (Fibre Channel over Ethernet).

- Identités Fibre Channel Over Ethernet (FCoE)

  Identités qui fournissent une identité virtuelle unique pour les opérations FCoE. Ces identités sont définies à la fois par les adresses MAC et FC (c'est-à-dire le nom WWNN et le nom WWPN). Les identités WWNN et WWPN sont requises pour la prise en charge du démarrage à partir d'un SAN et pour l'accès aux données via les protocoles FC et FCoE (Fibre Channel over Ethernet).

OpenManage Enterprise utilise les pools d'identités pour attribuer automatiquement des identités virtuelles au modèle de déploiement d'appareil utilisé pour déployer un serveur.

REMARQUE :

- Pour les identités qui appartiennent à un pool d'identités existant, mais qui ont été déployées en dehors d'OpenManage Enterprise, une nouvelle tâche d'inventaire de la configuration doit être lancée pour les identifier et les désigner comme étant « attribuées » dans l'appliance.
- Les identités virtuelles qui sont déjà attribuées ne seront pas utilisées pour un nouveau déploiement, à moins d'effacer ces identités.

Création de pools d'identités

Vous pouvez créer un pool d'identités qui contient un ou plusieurs types d'identités virtuelles. Le pool commun créé par l'administrateur peut être utilisé par tous les gestionnaires de périphériques. En outre, l'administrateur peut voir toutes les identités sous lesquelles il est utilisé. Les gestionnaires de périphériques peuvent voir tous les pools d'identités et effectuer toutes les opérations qu'ils contiennent (comme spécifié par RBAC). Toutefois, sous Utilisation, les gestionnaires de périphériques ne peuvent voir que les identités associées aux périphériques dans leur périmètre.

Pour créer un pool de types d'identités virtuelles :

1. Sur la page **Configuration**, cliquez sur **Pools d'identités**.
2. Cliquez sur **Créer**.
3. Dans la boîte de dialogue **Créer un pool d'identités**, sous **Informations sur le pool** :
   a. Saisissez un nom unique pour le pool d'identités virtuelles et une description appropriée.
   b. Cliquez sur **Suivant**.
4. Dans la section **Ethernet** :
   a. Cochez la case **Inclure les adresses MAC Ethernet virtuelles** pour inclure les adresses MAC.
   b. Saisissez une adresse MAC de début et indiquez le nombre d'identités MAC virtuelles à créer.
5. Dans la section **iSCSI** :
   a. Cochez la case **Inclure des adresses MAC iSCSI** pour inclure les adresses MAC iSCSI.
   b. Saisissez l'adresse MAC de début et indiquez le nombre d'adresses MAC iSCSI à créer.
   c. Sélectionnez **Configurer un initiateur iSCSI**, puis saisissez le préfixe IQN.
   d. Sélectionnez **Activer le pool d'adresses IP de l'initiateur iSCSI**, puis saisissez les détails du réseau.

      REMARQUE : Le pool d'adresses IP de l'initiateur iSCSI ne prend pas en charge les adresses IPv6.

6. Dans la section **FCoE** :
   a. Cochez la case **Inclure des identités FCoE** pour inclure des identités FCoE.
   b. Saisissez l'adresse MAC de début et indiquez le nombre d'identités FCoE à créer.

      REMARQUE : Les adresses WWPN et WWNN sont générées en préfixant respectivement 0x2001 et 0x2000 pour les adresses MAC.

7. Dans la section **Fibre Channel** :
   a. Cochez la case **Inclure des identités FC** pour inclure des identités FC.
   b. Saisissez les octets de postfix (six octets) et le nombre d'adresses WWPN et WWNN à créer.

      REMARQUE : Les adresses WWPN et WWNN sont générées en préfixant le postfix fourni par 0x2001 et 0x2000, respectivement.

Le pool d'identités virtuelles est créé et répertorié sous l'onglet **Pools d'identités**.

Créer un pool d'identités - Fibre Channel

Vous pouvez ajouter des adresses Fibre Channel (FC) au pool d'identités. Le FC comprend des adresses WWPN/WWNN.

Inclure des identités FC	Cochez la case pour ajouter des adresses FC au pool d'identités.
Postfix (6 octets)	Saisissez le postfix dans l'un des formats suivants : • `AA:BB:CC:DD:EE:FF`

- AA-BB-CC-DD-EE-FF
- AABB.CCDD.EEFF

Le postfix peut comporter un maximum de 50 caractères. Cette option s'affiche uniquement si la case **Inclure des identités FC** est cochée.

Nombre d'adresses WWPN/WWNN

Sélectionnez le nombre d'adresses WWPN ou WWNN. L'adresse peut être comprise entre 1 et 5 000.

Cette option s'affiche uniquement si la case **Inclure des identités FC** est cochée.

Actions

Précédent

Affiche l'onglet **FCoE**.

Terminer

Enregistre les modifications et affiche la page **Configuration**.

Annuler

Ferme l'assistant **Créer un pool d'identités** sans enregistrer les modifications.

Créer un pool d'identités - iSCSI

Vous pouvez configurer le nombre requis d'adresses MAC iSCSI dans l'onglet iSCSI.

REMARQUE : Les attributs iSCSI sont appliqués uniquement lorsque l'option DHCP pour l'initiateur iSCSI est désactivée dans le modèle source.

Inclure des adresses MAC iSCSI virtuelles

Cochez la case pour ajouter des adresses MAC iSCSI au pool d'identités.

Adresse MAC virtuelle de début

Saisissez l'adresse MAC de début du pool d'identités dans l'un des formats suivants :

- AA:BB:CC:DD:EE:FF
- AA-BB-CC-DD-EE-FF
- AABB.CCDD.EEFF

La longueur maximale d'une adresse MAC est de 50 caractères. Cette option s'affiche uniquement si la case **Inclure des adresses MAC iSCSI** est cochée.

Nombre d'adresses MAC iSCSI

Saisissez le nombre d'adresses MAC iSCSI. L'adresse MAC peut être comprise entre 1 et 5000. Cette option s'affiche uniquement si la case **Inclure des adresses MAC iSCSI** est cochée.

Configurer un initiateur iSCSI

Cochez cette case pour configurer l'initiateur iSCSI. Cette option s'affiche uniquement si la case **Inclure des adresses MAC iSCSI** est cochée.

Préfixe IQN

Saisissez le préfixe IQN du pool d'identités iSCSI. La longueur du préfixe IQN peut comporter un maximum de 200 caractères. Le système génère automatiquement le pool d'adresses IQN en ajoutant le numéro généré pour le préfixe. Par exemple : <IQN Prefix>.<number>

Cette option s'affiche uniquement si la case **Configurer un initiateur iSCSI** est cochée.

REMARQUE : Le nom qualifié iSCSI (IQN) configuré avec les pools d'identités n'est pas déployé sur le système cible si le mode de démarrage est défini sur « BIOS ».

REMARQUE : Si le nom de l'initiateur iSCSI s'affiche dans une ligne distincte du champ **Pools d'identités** > **Utilisation** > **IQN iSCSI**, cela indique que l'IQN iSCSI est activé uniquement sur cette partition NIC.

Activer le pool d'adresses IP de l'initiateur iSCSI

Cochez la case pour configurer un pool d'identités d'initiateur iSCSI. Cette option s'affiche uniquement si la case **Inclure des adresses MAC iSCSI** est cochée.

Plage d'adresses IP

Saisissez la plage d'adresses IP pour le pool d'initiateurs iSCSI dans l'un des formats suivants :

- A.B.C.D - W.X.Y.Z
- A.B.C.D/E

Masque de sous-réseau	Sélectionnez l'adresse du masque de sous-réseau du pool iSCSI dans la liste déroulante.
Passerelle	Saisissez l'adresse de la passerelle du pool iSCSI.
Serveur DNS principal	Saisissez l'adresse du serveur DNS principal.
Serveur DNS secondaire	Saisissez l'adresse du serveur DNS secondaire.

REMARQUE : La **plage d'adresses IP**, la **Passerelle**, le **serveur DNS principal** et le **Serveur DNS secondaire** doivent être des adresses IPv4 valides.

Actions

Précédent	Affiche l'onglet **Ethernet**.
Suivant	Affiche l'onglet **FCoE**.
Terminer	Enregistre les modifications et affiche la page **Configuration**.
Annuler	Ferme l'assistant **Créer un pool d'identités** sans enregistrer les modifications.

Créer un pool d'identités - Fibre Channel over Ethernet

Vous pouvez ajouter le nombre requis d'adresses MAC de protocole d'initialisation (FIP) FCoE (Fibre Channel over Ethernet) au pool d'identités. Les valeurs de nom de port universel (WWPN)/nom de nœud universel (WWNN) sont générées à partir de ces adresses MAC.

Inclure des identités FCoE	Cochez la case pour ajouter des adresses MAC FCoE au pool d'identités.
FIP/Adresse MAC	Saisissez l'adresse MAC de début du protocole d'initialisation FCoE (FIP) du pool d'identité dans l'un des formats suivants : • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF La longueur maximale d'une adresse MAC est de 50 caractères. Cette option s'affiche uniquement si la case **Inclure des identités FCoE** est cochée. Les valeurs WWPN/WWNN sont générées à partir de l'adresse MAC.
Nombre d'identités FCoE	Sélectionnez le nombre d'identités FCoE requises. Les identités peuvent être comprises entre 1 et 5 000.

Actions

Précédent	Affiche l'onglet **iSCSI**.
Suivant	Affiche l'onglet **Fibre Channel**.
Terminer	Enregistre les modifications et affiche la page **Pools d'identités**.
Annuler	Ferme l'assistant **Créer un pool d'identités** sans enregistrer les modifications.

Créer un pool d'identités - Ethernet

Dans l'onglet **Ethernet**, vous pouvez ajouter le nombre requis d'adresses MAC au pool d'identités.

Inclure les adresses MAC Ethernet virtuelles	Cochez la case pour ajouter des adresses MAC virtuelles au pool d'identités.
Adresse MAC virtuelle de début	Saisissez la première adresse MAC virtuelle dans l'un des formats suivants : • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` La longueur maximale d'une adresse MAC est de 50 caractères. Cette option s'affiche uniquement si la case **Inclure les adresses MAC Ethernet virtuelles** est cochée.
Nombre d'identités MAC virtuelles	Sélectionnez le nombre d'identités MAC virtuelles. Les identités peuvent être comprises entre 1 et 50. Cette option s'affiche uniquement si la case **Inclure les adresses MAC Ethernet virtuelles** est cochée.

Actions

Précédent	Affiche l'onglet **Informations sur le pool**.
Suivant	Affiche l'onglet **iSCSI**.
Terminer	Enregistre les modifications et affiche la page **Pools d'identités**.
Annuler	Ferme l'assistant **Créer un pool d'identités** sans enregistrer les modifications.

Affichage des définitions des pools d'identités

Pour afficher les définitions d'un pool d'identités :

1. Sur la page **Configuration**, cliquez sur **Pools d'identités**.
2. Sélectionnez un pool d'identités, puis cliquez sur **Récapitulatif**.
   Les différentes définitions du pool d'identités sont répertoriées.
3. Pour afficher l'utilisation de ces définitions d'identité, cliquez sur l'onglet **Utilisation** et sélectionnez l'option de filtre **Afficher par**.

Modification des pools d'identités

Vous pouvez modifier un pool d'identités pour ajouter des plages que vous n'avez pas spécifiées précédemment, ajouter un type d'identité ou supprimer des plages de type d'identité.

Pour modifier les définitions d'un pool d'identités :

1. Sur la page **Configuration**, cliquez sur **Pools d'identités**.
2. Sélectionnez le pool d'identités, puis cliquez sur **Modifier**.
   La boîte de dialogue **Modifier des pools d'identités** s'affiche.
3. Apportez les modifications aux définitions dans les sections appropriées, puis cliquez sur **Terminer**.

Le pool d'identités est modifié.

Suppression des pools d'identités

Vous ne pouvez pas supprimer un pool d'identités si les identités sont réservées ou affectées à un modèle de déploiement.

Pour supprimer un pool d'identités :

1. Sur la page **Configuration**, cliquez sur **Pools d'identités**.
2. Sélectionnez le pool d'identités, puis cliquez sur **Supprimer**.

3. Cliquez sur **Oui**.

Le pool d'identités est supprimé et les identités réservées associées à un ou plusieurs modèles de déploiement sont supprimées.

Définir des réseaux

Sur la page VLAN, vous pouvez saisir des informations sur les réseaux actuellement configurés dans votre environnement auquel les périphériques peuvent accéder.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Sélectionnez **Configuration** > **VLAN** > **Définir**.
2. Dans la boîte de dialogue **Définir réseau**, saisissez un nom et une description appropriée.
3. Saisissez l'ID VLAN, puis sélectionnez le type de réseau.

   Vous pouvez sélectionner un type de réseau seulement pour le châssis MX7000. Pour plus d'informations sur les types de réseau, voir Types de réseau , page 101.
4. Cliquez sur **Terminer**.

Le réseau actuellement configuré dans votre environnement est maintenant défini et les ressources peuvent accéder au réseau.

REMARQUE : Les restrictions basées sur le périmètre ne s'appliquent pas aux VLAN, puisqu'il s'agit de pools de ressources communs. Une fois qu'un VLAN est défini par l'administrateur, tous les gestionnaires de périphériques peuvent l'utiliser.

Types de réseau

REMARQUE : Vous pouvez sélectionner un type de réseau pour le châssis MX7000 uniquement.

Tableau 15. Types de réseau

Types de réseau	Description
Usage général (bronze)	Utilisé pour le trafic de données de priorité faible
Usage général (argent)	Utilisé pour le trafic de données de priorité standard ou par défaut
Usage général (or)	Utilisé pour le trafic de données de priorité élevée
Usage général (platine)	Utilisé pour le trafic de données de très haute priorité
Interconnexion de cluster	Utilisé pour les VLAN de pulsation de cluster
Gestion par hyperviseur	Utilisé pour les connexions de gestion des hyperviseurs telles que le VLAN de gestion ESXi
Stockage - iSCSI	Utilisé pour les VLAN iSCSI
Stockage - FCoE	Utilisé pour les VLAN FCoE
Stockage - Réplication des données	Utilisé pour les VLAN prenant en charge la réplication des données de stockage, par exemple pour VMware VSAN (Virtual Storage Area Network - Réseau de stockage virtuel)
Migration de machine virtuelle	Utilisé pour les VLAN prenant en charge vMotion et les technologies similaires
Journalisation de VMware FT	Utilisé pour les VLAN prenant en charge VMware Fault Tolerance

Modification ou suppression d'un réseau configuré

1. Accédez à la page VLAN en cliquant sur **Configuration** > **VLAN**.
2. Sélectionnez un réseau dans la liste, puis cliquez sur **Modifier** dans le volet de droite pour modifier le nom, la description, l'ID VLAN ou le type de réseau.

   REMARQUE : La configuration VLAN sur les châssis M1000e et FX2 n'est pas prise en charge dans une infra IPv6, car l'adressage IPv6 n'est pas pris en charge par M I/O Aggregator (IOA) et les modules d'E/S FN.

   REMARQUE : Le nom et les ID VLAN modifiés ne sont pas mis à jour sur le châssis MX7000 cible après l'exécution d'une tâche de déploiement sans état.

3. Pour supprimer le réseau, sélectionnez-le et cliquez sur **Supprimer**.
4. Cliquez sur **Oui**.

Exportation des définitions VLAN

Les définitions de réseau disponibles dans OpenManage Enterprise peuvent être téléchargées au format de fichier CSV ou JASON.

1. Pour les télécharger sous forme de fichier CSV :
   a. Cliquez sur **Configuration** > **VLAN** > **Exporter**, puis sélectionnez **Exporter tout dans un fichier CSV**.
2. Pour les télécharger sous forme de fichier JSON :
   a. Cliquez sur **Configuration** > **VLAN** > **Exporter**, puis sélectionnez **Exporter tout dans un fichier JSON**.

Importation des définitions de réseau

Les options suivantes sont disponibles pour importer les définitions de réseau :

1. **Importer des définitions VLAN à partir d'un fichier**

   Pour importer des définitions VLAN à partir d'un fichier :

   a. Cliquez sur **Configuration** > **VLAN**.
   b. Cliquez sur **Importer**, puis sélectionnez **Importer à partir d'un fichier**.
   c. Accédez à l'emplacement du fichier et sélectionnez un fichier .json ou .csv existant contenant les définitions VLAN, puis cliquez sur **Ouvrir**.

   REMARQUE :

   - Des entrées ou un type de contenu non valides dans les fichiers sont marqués et ne sont pas importés.
   - Les définitions de VLAN dans les fichiers .csv et .json doivent être saisies aux formats suivants :

   Tableau 16. Format de définition de VLAN pour les fichiers CSV

Nom	Description	VLANMin	VLANMax	Type
VLAN1	VLAN avec un ID unique	1	1	1
VLAN2 (plage)	VLAN avec une plage d'ID	2	10	2

   et

   Tableau 17. Format de définition de VLAN pour les fichiers JSON

```
[{"Name":"VLAN1","Description":"VLAN avec un ID
unique","VlanMinimum":1,"VlanMaximum":1,"Type":1},
```

Tableau 17. Format de définition de VLAN pour les fichiers JSON

```
{"Name":"VLAN2 (plage)","Description":"VLAN avec une plage
d'ID","VlanMinimum":2,"VlanMaximum":10,"Type":2}]
```

d. Cliquez sur **Terminer**. Une tâche nommée **ImportVLANDefinitionsTask** est créée pour importer les réseaux à partir du fichier sélectionné.

2. **Importer des définitions VLAN à partir d'un châssis**

   Pour importer des définitions VLAN à partir d'un châssis MX7000 existant :

   REMARQUE : L'application OpenManage Enterprise-Modular version 1.2 doit déjà être installée dans le châssis MX7000.

   a. Cliquez sur **Configuration** > **VLAN**.
   b. Cliquez sur **Importer**, puis sélectionnez **Importer des définitions VLAN à partir d'un châssis**.
   c. Dans l'écran **Tâche cible**, sélectionnez le châssis à partir duquel les définitions VLAN doivent être importées, puis cliquez sur **OK**. Une tâche nommée **ImportVLANDefinitionsTask** est créée pour importer les réseaux à partir du châssis sélectionné.

Une fois la tâche terminée, actualisez la page **Configuration** > **VLAN** pour afficher les définitions VLAN correctement importées.

Pour afficher les détails d'exécution de la tâche et l'état de chaque réseau importé à partir du châssis, accédez à la page **Tâches** en cliquant sur **Surveiller** > **Tâches**, sélectionnez la tâche, puis cliquez sur **Afficher les détails**.

12

Gestion des profils

Un « profil » est une instance spécifique d'un modèle de déploiement existant qui est personnalisée avec des attributs propres à un appareil individuel. Des profils peuvent être créés implicitement au cours du déploiement d'un modèle/déploiement automatique ou à partir des modèles existants par l'utilisateur. Un profil se compose de valeurs d'attribut propres à la cible avec des choix BootToISO, ainsi que des informations sur l'adresse IP de gestion de l'iDRAC du périphérique cible. Il peut également contenir une bande passante réseau et des allocations VLAN pour les ports NIC de serveur, le cas échéant. Les profils sont liés au modèle source à partir duquel ils ont été créés.

Sur la page **Configuration** > **Profils**, tous les profils qui se trouvent dans le périmètre de l'utilisateur connecté s'affichent. Par exemple, un administrateur peut voir et gérer tous les profils, mais un gestionnaire de périphériques dont le périmètre est limité peut voir et utiliser uniquement les profils qu'il crée et qu'il détient.

Les informations suivantes des profils répertoriés s'affichent :

Tableau 18. Gestion des profils : définition des champs

Nom du champ	Description
Modifié	Un symbole « modifié » ⚠ est affiché pour notifier toute modification apportée aux attributs de profil ou de modèle associés après l'attribution initiale. Si le profil modifié est redéployé sur le périphérique, le symbole disparaît.
Nom du profil	Nom du profil.
Nom du modèle	Nom du modèle source lié.
Cible	Numéro de série ou adresse IP du périphérique auquel le profil est attribué. Si le profil n'est attribué à aucun périphérique, la cible est vide.
Type de cible	Type de périphérique (serveur ou châssis) auquel le profil est attribué.
Châssis	Nom du châssis si le serveur cible est détecté en tant que partie d'un châssis.
État du profil	L'état du profil s'affiche comme suit : « Attribué au périphérique » si le profil est attribué, « Non attribué » s'il n'est pas attribué et « Déployé » s'il est déployé.
État de la dernière action	Affiche l'état de la dernière action d'un profil : Abandonné, Annulé, Terminé, Échec, Nouveau, Non exécuté, En pause, En file d'attente, Exécution, Planifié, Démarrage, Arrêté, Terminé avec des erreurs.

L'option **Filtres avancés** permet de personnaliser la liste des profils.

À droite : les paramètres Description, Heure du dernier déploiement, Heure de la dernière modification, Date de création et Créé par sont affichés pour le profil sélectionné. Cliquez sur Afficher les identités pour afficher la configuration de la carte NIC et les identités virtuelles qui sont marquées pour le profil.

En fonction des différents états du profil, les actions suivantes peuvent être effectuées sur la page **Configuration** > **Profils**, comme indiqué ci-dessous :

REMARQUE : Les opérations Créer et Supprimer ne sont pas répertoriées dans le tableau.

Tableau 19. États du profil et opérations possibles

État du profil	Modifier	Attribuer une cible	Annuler l'attribution d'une cible	Redéployer	Migrer
Profil non attribué	Oui	Oui	Non	Non	Non

Tableau 19. États du profil et opérations possibles (suite)

État du profil	Modifier	Attribuer une cible	Annuler l'attribution d'une cible	Redéployer	Migrer
Attribué au périphérique	Oui	Non	Oui	Non	Non
Déployé	Oui	Non	Oui	Oui	Oui

- Créer des profils et préréserver des identités virtuelles. Voir, Création de profils , page 105
- Affichage des détails d'un profil. Voir, Affichage des détails d'un profil , page 106
- Modification des attributs et des paramètres d'un profil. Voir, Modifier un profil , page 106
- Attribution d'un profil à un périphérique ou à un numéro de série (via le déploiement automatique). Voir, Attribution d'un profil , page 107
- Annulation de l'attribution d'un profil à un périphérique ou numéro de série. Voir, Annulation de l'attribution de profils , page 108
- Redéploiement des modifications apportées au profil sur le périphérique cible associé. Voir, Redéploiement des profils , page 108
- Migration du profil d'une cible (périphérique ou numéro de série) vers un autre.
- Suppression des profils. Voir, Suppression des profils , page 109
- Exportation et téléchargement des données d'un ou plusieurs profils au format HTML, CSV ou PDF. Voir, Exportation des données d'un ou plusieurs profils au format HTML, CSV ou PDF , page 109

Sujets :

Création de profils

Des profils peuvent être créés à l'aide des modèles de déploiement existants pour le déploiement sur les appareils cibles existants ou peuvent être réservés pour le déploiement automatique sur les appareils restant à détecter.

REMARQUE :

- Seuls les utilisateurs disposant des privilèges de gestionnaire de périphériques ou d'administrateur OpenManage Enterprise sont autorisés à effectuer les tâches de gestion des profils. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Après une mise à niveau depuis la version 3.5 ou une version antérieure, les profils créés par les gestionnaires de périphériques AD/LDAP et OIDC (PingFederate ou KeyCloak) à partir de n'importe quelle version antérieure d'OpenManage Enterprise sont uniquement affectés à l'administrateur. Par conséquent, les gestionnaires de périphériques doivent recréer les profils postérieurs à la mise à niveau.

Pour créer un profil à partir d'un modèle de déploiement existant :

1. Accédez à la page Profils en cliquant sur **Configuration** > **Profils**.
2. Cliquez sur **Créer** pour activer l'Assistant Créer des profils.
3. Dans la section Modèle, sélectionnez le **type de modèle** Serveur ou Châssis, puis sélectionnez un modèle de déploiement dans la liste déroulante **Sélectionner un modèle**. Cliquez sur **Suivant**.
4. Sur la page **Détails**, modifiez la valeur indiquée dans **Préfixe de nom** et saisissez une description dans la zone **Description**, si nécessaire. Dans la zone **Nombre de profils**, saisissez le nombre de profils. Cliquez sur **Suivant**.
5. Si vous le souhaitez, sur la page **Amorcer à partir de l'image ISO du réseau**, cochez la case **Amorcer à partir de l'image ISO du réseau** et spécifiez le chemin complet de l'ISO, l'emplacement du partage de fichiers et choisissez une option de **Durée de liaison de l'image ISO** pour définir le nombre d'heures pendant lesquelles le fichier ISO du réseau reste mappé sur le ou les périphériques cibles.
6. Cliquez sur **Terminer**.

Les profils sont créés en fonction du nom du modèle de déploiement et du nombre indiqué. Ces profils sont répertoriés sur la page Profils.

Affichage des détails d'un profil

Pour afficher uniquement les détails d'un profil existant sans les modifier :

1. Sélectionnez un profil dans la liste des profils de la page **Configuration** > **Profils**.
2. Cliquez sur **Afficher** pour activer l'Assistant Afficher le profil.
3. Sur la page **Détails** de l'Assistant, les paramètres Modèle source, Nom, Description et Informations sur la cible sont affichés.
4. Cliquez sur **Suivant**. Sur la page **Amorcer à partir de l'image ISO du réseau**, le chemin du fichier d'image ISO, l'emplacement de partage de ce fichier et la valeur de Durée de liaison de l'image ISO sont affichés si le profil a été initialement défini à l'aide de cette préférence.

Profils : afficher le réseau

Pour afficher la bande passante réseau et les allocations de VLAN pour les ports NIC associés à un profil, procédez comme suit :

1. Sélectionnez un profil sur la page **Configuration** > **profils** de configuration.
2. Cliquez sur **Afficher** pour activer l'Assistant Afficher le profil.
3. La section **bande passante** affiche les paramètres de bande passante suivants des cartes réseau (NIC) partitionnées : identifiant NIC, port, partition, bande passante min. (%) et bande passante maximale (%). Cliquez sur **Suivant**.
4. La section **VLAN** affiche les informations de VLAN suivantes pour les profils : NIC regroupement, NIC identifiant, port, groupe, réseau non balisé et réseau balisé.
5. Cliquez sur **Terminer** pour fermer l'Assistant.

Modifier un profil

Vous pouvez modifier un profil existant sur la page **Configuration** > **Profils**. Les modifications apportées au profil n'ont pas d'incidence automatique sur le système cible associé. Pour que les modifications prennent effet, le profil modifié doit être redéployé sur le périphérique cible.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

Pour renommer ou modifier un réseau ou encore changer les attributs d'un profil existant, sélectionnez le profil sur la page Profils, puis cliquez sur **Modifier**. Les options de modification suivantes peuvent être sélectionnées :

1. Sélectionnez **Renommer**, puis, dans l'Assistant Renommer le profil, modifiez le nom du profil dans la zone **Nom**.
2. Sélectionnez **Modifier le profil** pour activer l'Assistant Modifier le profil, puis modifiez les éléments suivants :
   a. Sur la page **Détails**, vous pouvez modifier les valeurs indiquées dans les zones **Nom** et **Description**. Cliquez sur **Suivant**.
   b. À la page Amorcer à partir de l'image ISO du réseau, cochez la case **Amorcer à partir de l'image ISO du réseau** pour spécifier le chemin complet de l'ISO ainsi que l'emplacement du partage, puis procédez comme suit :
      - Sélectionnez le **type de partage** CIFS ou NFS.
      - Dans la zone **Chemin d'accès de l'ISO**, saisissez le chemin complet de l'ISO. Utilisez les info-bulles pour entrer la syntaxe correcte.
      - Renseignez les zones **Adresse IP de partage**, **Nom d'utilisateur** et **Mot de passe**.
      - Sélectionnez les options du menu déroulant **Durée de liaison de l'image ISO** pour définir le nombre d'heures pendant lesquelles le fichier ISO du réseau reste mappé sur le périphérique cible. Par défaut, cette valeur est définie sur quatre heures.
      - Cliquez sur **Suivant**.
   c. Sur la page **IP de gestion de l'iDRAC**, sélectionnez l'une des options suivantes :
      - Ne pas modifier les paramètres IP.
      - Définir en tant que protocole DHCP
      - Définir une adresse IP statique. Renseignez les zones IP de gestion, Masque de sous-réseau et Passerelle.
   d. Sur la page **Attributs cibles**, vous pouvez sélectionner et modifier les attributs BIOS, Système, NIC, iDRAC et Identité virtuelle du profil.
   e. Cliquez sur **Terminer** pour enregistrer les modifications.

Attribution d'un profil

Sur la page **Configuration** > **Profils**, un profil non attribué peut être déployé sur un serveur existant ou réservé pour le déploiement automatique sur un serveur restant à détecter.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les attributs existants, le cas échéant, du serveur cible sont écrasés lorsqu'un profil est déployé sur celui-ci.
- Seuls les périphériques qui ne sont associés à aucun profil sont disponibles pour le déploiement ou le déploiement automatique.

1. Pour **déployer un profil** :
   a. Sélectionnez un profil non attribué sur la page **Configuration** > **Profils**, puis cliquez sur **Attribuer** > **Déployer** pour activer l'Assistant Déployer un profil.
   b. La page **Détails** affiche le modèle source, le nom ainsi que la description du profil. Cliquez sur **Suivant**.
   c. Sur la page **Cible** :
      - Cliquez sur **Sélectionner**, puis, dans la liste des périphériques, sélectionnez un périphérique cible.
        REMARQUE : Les périphériques auxquels un profil a déjà été attribué seront grisés et ne pourront pas être sélectionnés dans la liste de cibles.
      - Si un redémarrage est nécessaire après le déploiement, cochez la case **Ne pas forcer le redémarrage du système d'exploitation hôte en cas d'échec du redémarrage normal**.
      - Cliquez sur **Suivant**.
   d. (En option) Sur la page **Amorcer à partir de l'image ISO du réseau**, cochez la case **Amorcer à partir de l'image ISO du réseau** et indiquez le chemin de l'ISO approprié, les détails de l'emplacement du partage ainsi que la valeur de Durée de liaison de l'image ISO. Cliquez sur **Suivant**.
   e. Sur la page **IP de gestion de l'iDRAC**, sélectionnez l'une des options suivantes et indiquez d'autres informations pertinentes.
      - Ne pas modifier les paramètres IP
      - Définir en tant que protocole DHCP
      - Définir une adresse IP statique
   f. Sur la page **Attributs cibles**, les attributs sont affichés dans les sections BIOS, Système, NIC et iDRAC. Vous pouvez sélectionner, désélectionner ou modifier les attributs avant le déploiement.
   g. Sur la page **Identités virtuelles**, cliquez sur **Réserver des identités**. Les identités virtuelles attribuées pour les cartes d'interface réseau de l'appareil cible sélectionné s'affichent. Pour afficher toutes les identités attribuées du pool d'identités de l'appareil cible sélectionné, cliquez sur **Afficher tous les détails de la carte d'interface réseau**.
   h. Sur la page **Planifier**, vous pouvez choisir **Exécuter maintenant** pour déployer le profil immédiatement ou **Activer la planification**, puis sélectionner une date et une heure appropriées pour le déploiement du profil.
   i. Cliquez sur **Terminer**.

   REMARQUE : Si des identités sont déjà attribuées en dehors de l'appliance, ces identités ne seront utilisées dans un nouveau déploiement que si elles sont désactivées. Pour en savoir plus, voir Pools d'identités , page 96

2. Pour **déployer automatiquement un profil** :

   REMARQUE : Pour les périphériques modulaires, la vérification stricte des définitions de VLAN est activée par défaut.

   a. Sélectionnez un profil non attribué sur la page **Configuration** > **Profils**, puis cliquez sur **Attribuer** > **Déployer automatiquement** pour activer l'Assistant Déployer automatiquement.
   b. La page Détails affiche le modèle source, le nom et la description (le cas échéant) du profil. Cliquez sur **Suivant**.
   c. Sur la page **Cible**, spécifiez le numéro de série ou l'ID du nœud du périphérique restant à détecter dans la zone **ID**. Cliquez sur **Suivant**.
   d. (En option) Sur la page Amorcer à partir de l'image ISO du réseau, cochez la case **Amorcer à partir de l'image ISO du réseau** pour spécifier le chemin complet de l'ISO ainsi que l'emplacement du partage :
      - Sélectionnez le **type de partage** CIFS ou NFS.
      - Dans la zone **Chemin d'accès de l'ISO**, saisissez le chemin complet de l'ISO. Utilisez les info-bulles pour entrer la syntaxe correcte.
      - Renseignez les zones **Adresse IP de partage**, **Nom d'utilisateur** et **Mot de passe**.

- Sélectionnez les options du menu déroulant **Durée de liaison de l'image ISO** pour définir le nombre d'heures pendant lesquelles le fichier ISO du réseau reste mappé sur le ou les périphériques cibles. Par défaut, cette valeur est définie sur quatre heures.

e. Cliquez sur **Terminer**.

Annulation de l'attribution de profils

À l'aide des options **Configuration** > **Profils** > **Annuler l'attribution**, vous pouvez dissocier les profils déployés automatiquement ou non de leurs cibles respectives. .

Pour annuler l'attribution de profils :

1. Sélectionnez les profils dans la liste Profils de la page **Configuration** > **Profils**.
2. Cliquez sur **Annuler l'attribution**.
3. Cliquez sur **Terminer** dans la boîte de dialogue de confirmation.

L'attribution des profils sélectionnés est annulée, et les identités de leurs cibles respectives sont supprimées.

REMARQUE : Dans le cas de périphériques cibles déployés, l'annulation de l'attribution des profils rétablit leurs identités attribuées en usine.

Redéploiement des profils

Pour que les modifications des attributs d'un profil déjà déployé prennent effet sur le périphérique cible associé, le profil doit être redéployé. Dans le cas de périphériques modulaires, les définitions de VLAN peuvent être configurées lors du redéploiement ; en revanche, la vérification stricte pour la mise en correspondance des attributs VLAN est alors désactivée.

REMARQUE : Les modifications d'attribut VLAN échouent sur les traîneaux MX7000 cibles lors du redéploiement du profil si les attributs VLAN n'ont pas été initialement déployés sur les traîneaux MX7000 lors du déploiement du modèle à l'aide de l'option Propager immédiatement les paramètres VLAN.

Pour redéployer le ou les profils :

1. Sur la page **Configuration** > **Profils**, sélectionnez le ou les profils qui sont « Déployés » et/ou « Modifiés » (⚠), puis cliquez sur **Redéployer**.
2. Sur la page Options de déploiement de l'attribut de l'Assistant Redéploiement, choisissez l'une des options de déploiement de l'attribut suivantes, puis cliquez sur **Suivant** :
   - **Attributs modifiés uniquement** : pour redéployer uniquement les attributs modifiés sur le périphérique cible.
   - **Tous les attributs** : pour redéployer tous les attributs, ainsi que tous les attributs modifiés, sur le périphérique cible.
3. Sur la page Planifier, sélectionnez l'une des options suivantes :
   - **Exécuter maintenant** permet d'appliquer les modifications immédiatement.
   - **Activer la planification**, puis sélectionnez la date et l'heure du redéploiement à planifier.
4. Cliquez sur **Terminer** pour continuer.

Lorsqu'un profil est redéployé, une tâche de **Redéploiement des profils** est exécutée. L'état des tâches est disponible sur la page **Surveiller** > **Tâches**.

Migration d'un profil

Vous pouvez migrer un profil déployé ou déployé automatiquement à partir d'un périphérique cible ou d'un numéro de série existant vers un autre périphérique ou numéro de série cible identique.

Lorsqu'une migration réussit, l'attribution de la cible du profil reflète la nouvelle cible. Si la migration s'effectue d'un périphérique cible vers un numéro de série restant à détecter, l'état du profil est remplacé par « Attribué ».

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

- La migration du profil déplace les paramètres définis par le profil (y compris les identités virtuelles déployées) de la source vers la cible.
- Vous pouvez forcer la migration d'un profil même si le périphérique source ne peut pas être contacté. Dans ce cas, l'utilisateur doit s'assurer qu'il n'y a aucun conflit d'identités virtuelles.
- Les attributs réellement spécifiques à la cible ne sont pas récupérés à partir du serveur « source » dans le cadre de la migration. De ce fait, les mêmes détails d'inventaire peuvent être présents sur deux serveurs après la migration.

Pour migrer un profil :

1. Sur la **page Configuration** > **Profils**, sélectionnez un profil et cliquez sur **Migrer** pour activer l'Assistant Migrer le profil.
2. Sur la page Sélection :
   a. Depuis le menu déroulant **Sélectionner un profil source**, sélectionnez le profil à migrer.
   b. Cliquez sur **Sélectionner une cible** et dans la boîte de dialogue Tâche cible, sélectionnez un périphérique cible, puis cliquez sur **OK**.
   c. Si nécessaire, cochez la case « Forcer la migration même si le périphérique source ne peut pas être contacté ».

      REMARQUE : Vous devez vous assurer qu'il n'y a aucun conflit d'identités virtuelles.

   d. Cliquez sur **Suivant**.
3. Sur la page Planifier, sélectionnez l'une des options suivantes :
   a. Sélectionnez **Mettre à jour maintenant** pour migrer les paramètres de profil immédiatement vers la cible.
   b. Sélectionnez la **Date** et l'**Heure** de la migration à planifier.
4. Cliquez sur **Terminer**.

Une tâche est créée pour migrer les paramètres du profil vers le nouveau périphérique cible. Vous pouvez afficher l'état de la tâche sur la page **Surveiller** > **Tâches**.

Suppression des profils

Les profils « non attribués » existants peuvent être supprimés de la page **Configuration** > **Profils** :

REMARQUE :

- Un profil attribué ou déployé ne peut être supprimé du Portail de profils que s'il n'est pas attribué.
- La suppression d'un profil non attribué contenant des identités réservées a pour effet de renvoyer ces identités à leur pool d'identités d'origine. Il est recommandé de patienter 10 minutes pour utiliser ces identités récupérées dans le cadre de réservations et de déploiements ultérieurs.

Pour supprimer les profils non attribués :

1. Sélectionnez les profils non attribués sur la page Profils.
2. Cliquez sur **Supprimer** et confirmez la suppression en cliquant sur **Oui** lorsque vous y êtes invité.

Exportation des données d'un ou plusieurs profils au format HTML, CSV ou PDF

Pour exporter les données d'un ou plusieurs profils au format HTML, CSV ou PDF.

1. Sur la page **Configuration** > **Profils**, sélectionnez le ou les profils.
2. Cliquez sur **Exporter** et, dans la boîte de dialogue Exporter la sélection, choisissez HTML, CSV ou PDF.
3. Cliquez sur **Terminer**. Les données du ou des profils sont téléchargées au format sélectionné.

13

Gestion de la conformité de la configuration du périphérique

En sélectionnant **OpenManage Enterprise** > **Configuration** > **Conformité de la configuration</>4, vous pouvez créer des lignes de base de conformité de la configuration à l'aide des modèles de conformité intégrés ou créés par l'utilisateur.** Vous pouvez créer un modèle de conformité à partir d'un modèle de déploiement existant, d'un appareil de référence ou d'une importation à partir d'un fichier. Pour utiliser cette fonctionnalité, vous devez disposer de la licence de niveau entreprise OpenManage Enterprise et iDRAC pour les serveurs. Aucune licence n'est nécessaire pour Chassis Management Controller. Seuls les utilisateurs dotés de certains privilèges sont habilités à utiliser cette fonctionnalité. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Une fois qu'une ligne de base de la configuration est créée à l'aide d'un modèle de conformité, le récapitulatif du niveau de conformité de chaque ligne de base est répertorié dans un tableau. Chaque appareil associé à la ligne de base dispose de son propre état. Toutefois, l'état le plus grave est considéré comme l'état de la ligne de base. Pour en savoir plus sur l'état d'intégrité globale, voir le livre blanc *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge Dell EMC PowerEdge de 14e génération et génération ultérieure) disponible sur le site de support.

REMARQUE : Une ligne de base associée à plusieurs périphériques peut parfois apparaître de manière permanente comme étant non conforme car quelques valeurs d'attribut ne sont pas nécessairement identiques sur toutes les cibles. Par exemple, les attributs de contrôle de démarrage tels que l'IQN de la cible iSCSI, l'ID de LUN, le WWPN de la cible FCoE, etc. ne sont pas identiques sur toutes les cibles et peuvent conduire à une non-conformité permanente de la ligne de base.

Le rapport Récapitulatif de la conformité globale affiche les champs suivants :

- **CONFORMITÉ** : indique le niveau de conformité global des périphériques reliés à la ligne de base de conformité de la configuration. L'état d'un périphérique ayant un niveau de conformité inférieur (critique, par exemple) est indiqué comme l'état de l'ensemble de la ligne de base.
- **NOM** : nom de la ligne de base de conformité de la configuration.
- **MODÈLE** : nom du modèle de conformité utilisé par la ligne de base.
- **HEURE DE LA DERNIÈRE EXÉCUTION** : date et heure de dernière exécution de la ligne de base de conformité.

Pour afficher le rapport de conformité de la configuration d'une ligne de base, cochez la case correspondante, puis cliquez sur **Afficher le rapport** dans le volet de droite.

Utilisez la fonction Générateur d'interrogation pour générer la conformité au niveau du périphérique par rapport à la ligne de base sélectionnée. Voir Sélection d'un critère de requête , page 58.

OpenManage Enterprise fournit un rapport intégré pour afficher la liste des périphériques surveillés et leur conformité à la ligne de base de conformité. Sélectionnez **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Périphériques par ligne de base de conformité de modèle**, puis cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

Tâches associées

Création d'une ligne de base de conformité de la configuration , page 113
Modification d'une ligne de base de conformité de la configuration , page 114
Suppression d'une ligne de base de conformité de la configuration , page 116
Gérer les modèles de conformité , page 111
Sélection d'un critère de requête , page 58

Sujets :

- Suppression d'une ligne de base de conformité de la configuration

Gérer les modèles de conformité

Utilisez le modèle de conformité pour créer des lignes de base de conformité, puis vérifiez régulièrement l'état de conformité de la configuration des périphériques associés à la ligne de base. Voir Gestion de la conformité de la configuration du périphérique , page 110.

Vous pouvez créer des modèles de conformité à l'aide d'un modèle de déploiement, d'un appareil de référence ou d'une importation à partir d'un fichier. Voir Gérer les modèles de conformité , page 111.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

En sélectionnant **Configuration** > **Conformité de la configuration** > **Gestion des modèles**, vous pouvez afficher la liste des modèles de conformité en fonction de l'accès basé sur le périmètre dont vous disposez dans OpenManage Enterprise. Par exemple, un administrateur peut afficher et gérer tous les modèles de conformité, mais les gestionnaires de périphériques peuvent uniquement afficher et gérer les modèles qu'ils créent et détiennent. Sur cette page :

- Vous pouvez créer un modèle de conformité en procédant comme suit :
  - Utilisation d'un modèle de déploiement. Voir Créer un modèle de conformité à partir du modèle de déploiement , page 111.
  - Utilisation d'un périphérique de référence. Voir Créer un modèle de conformité à partir d'un appareil de référence , page 112.
  - Importation depuis un fichier de modèle. Voir Créer un modèle de conformité par importation depuis un fichier , page 112.
- Modifier un modèle de conformité. Voir Modifier un modèle de conformité , page 113.
- Cloner un modèle de conformité. Voir Cloner un modèle de conformité , page 112.
- Exporter un rapport sur un modèle de conformité. Sur la page **Modèles de conformité**, cochez la case correspondante, puis cliquez sur **Exporter**. Voir Exportation de toutes les données ou des données sélectionnées , page 68.
- Supprimer un modèle de conformité. Sur la page **Modèles de conformité**, cochez la case correspondante, puis cliquez sur **Supprimer**.

La conformité de la configuration peut évoluer pour prendre en charge jusqu'à 6 000 périphériques. Pour gérer efficacement l'activité de conformité de la configuration à grande échelle, procédez comme suit :

- Désactivez la tâche Inventaire de la configuration par défaut qui est déclenchée automatiquement et lancez-la manuellement si nécessaire.
- Créez des lignes de base de conformité en réduisant le nombre de périphériques. Par exemple, vous devez classer 6 000 périphériques dans quatre lignes de base distinctes comprenant chacune 1 500 périphériques.
- Vous ne devez pas vérifier la conformité de toutes les lignes de base en même temps.

REMARQUE : Lorsque vous modifiez un modèle de conformité, la conformité de la configuration est déclenchée automatiquement sur toutes les lignes de base auxquelles elle est associée. Si le modèle est appelé à être souvent modifié, l'environnement d'évolution décrit ci-dessus n'est pas pris en charge et il est alors recommandé d'associer un maximum de 100 périphériques par ligne de base pour bénéficier de performances optimales.

Information associée

Gestion de la conformité de la configuration du périphérique , page 110
Modification d'une ligne de base de conformité de la configuration , page 114
Suppression d'une ligne de base de conformité de la configuration , page 116
Créer un modèle de conformité à partir du modèle de déploiement , page 111
Modifier un modèle de conformité , page 113

Créer un modèle de conformité à partir du modèle de déploiement

1. Cliquez sur **Configuration** > **Conformité de la configuration** > **Gestion des modèles** > **Créer** > **Depuis un modèle de déploiement**.

2. Dans la boîte de dialogue **Cloner un modèle de déploiement**, dans le menu déroulant **Modèle**, sélectionnez un modèle de déploiement qui doit être utilisé comme référence pour le nouveau modèle.
3. Saisissez un nom et une description pour le modèle de conformité.
4. Cliquez sur **Terminer**.
   Un modèle de conformité est créé et répertorié dans la liste des modèles de conformité.

Tâches associées

Gérer les modèles de conformité , page 111
Cloner un modèle de conformité , page 112

Créer un modèle de conformité à partir d'un appareil de référence

Pour utiliser les propriétés de configuration d'un périphérique en tant que modèle de création d'une ligne de base de configuration, le périphérique doit déjà être intégré. Voir Intégration de périphériques , page 45.

1. Cliquez sur **Configuration** > **Conformité de la configuration** > **Gestion des modèles** > **Créer** > **À partir d'un appareil de référence**.
2. Dans la boîte de dialogue **Créer un modèle de conformité**, saisissez le nom et la description du modèle de conformité.
3. Sélectionnez les options de création du modèle de conformité en clonant les propriétés d'un serveur ou d'un châssis.
4. Cliquez sur **Suivant**.
5. Dans la section **Périphérique de référence**, sélectionnez l'appareil qui doit être utilisé en tant que référence pour la création du modèle de conformité. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.
   a. Si vous sélectionnez un serveur en tant que référence, sélectionnez les propriétés de configuration de serveur qui doivent être clonées.
6. Cliquez sur **Terminer**.
   Une tâche de création de modèle est créée et exécutée. Le nouveau modèle de conformité est répertorié sur la page **Modèles de conformité**.

Créer un modèle de conformité par importation depuis un fichier

1. Cliquez sur **Configuration** > **Conformité de la configuration** > **Gestion des modèles** > **Créer** > **Importer depuis un fichier**.
2. Dans la boîte de dialogue **Importer un modèle de conformité**, saisissez le nom du modèle de conformité.
3. Sélectionnez le serveur ou le type de modèle de châssis, puis cliquez sur **Sélectionner un fichier** pour accéder au fichier et sélectionnez-le.
4. Cliquez sur **Terminer**.
   Le modèle de conformité est créé et répertorié.

Cloner un modèle de conformité

1. Cliquez sur **Configuration** > **Conformité de la configuration** > **Gestion des modèles**.
2. Sélectionnez le modèle de conformité qui doit être cloné, puis cliquez sur **Cloner**.
3. Dans la boîte de dialogue **Cloner le modèle**, saisissez le nom du nouveau modèle de conformité.
4. Cliquez sur **Terminer**.
   Le nouveau modèle de conformité est créé et répertorié sous **Modèles de conformité**.

Information associée

Créer un modèle de conformité à partir du modèle de déploiement , page 111
Modifier un modèle de conformité , page 113

Modifier un modèle de conformité

Les modèles de conformité peuvent être modifiés sur la page **Conformité de la configuration** > **Modèles de conformité**. Lors de la modification, la sélection ou la désélection des attributs d'un modèle, les attributs stockés dans le modèle ne sont pas modifiés et tous les attributs font toujours partie du modèle s'il est exporté. Cela a une incidence sur ce qui est déployé.

REMARQUE :

- La modification d'un modèle de conformité qui est déjà associé à d'autres lignes de base déclenche automatiquement une conformité de la configuration pour tous les appareils de l'ensemble des lignes de base qui utilisent le modèle.
- La modification d'un modèle de conformité lié à plusieurs lignes de base contenant un grand nombre d'appareils peut entraîner un délai d'expiration de la session, car la vérification de la conformité de la configuration de tous les appareils associés peut prendre plusieurs minutes. Un délai d'expiration de la session ne signifie pas que les modifications apportées au modèle de conformité ont rencontré un problème.
- Lors de la modification d'un modèle de conformité sur des systèmes à grande échelle comprenant 1 000 appareils ou d'un inventaire de configuration contenant jusqu'à 6 000 appareils gérés, assurez-vous qu'aucune autre opération d'inventaire ou de conformité de configuration n'est exécutée en parallèle. Vous pouvez également **désactiver** la tâche d'inventaire de la configuration générée par défaut par le système sur la page **Surveiller** > **Tâches** (en définissant la source sur Généré par le système).
- Pour des performances optimales, il est recommandé d'associer un maximum de 1 500 périphériques par ligne de base.
- Si le modèle est appelé à être souvent modifié, il est recommandé d'associer un maximum de 100 périphériques par ligne de base.

1. Sur la page **Modèles de conformité**, cochez la case correspondante, puis cliquez sur **Modifier**.
2. Sur la page **Détails du modèle**, les propriétés de configuration du modèle de conformité sont répertoriées.
3. Développez la propriété à modifier, puis saisissez ou sélectionnez les données dans les champs.
   a. Pour activer la propriété, cochez la case, si elle n'est pas déjà activée.
4. Cliquez sur **Enregistrer** ou **Abandonner** pour appliquer ou annuler les modifications.
   Le modèle de conformité est modifié et les informations mises à jour sont enregistrées.

Tâches associées

Gérer les modèles de conformité , page 111
Cloner un modèle de conformité , page 112

Création d'une ligne de base de conformité de la configuration

Une ligne de base de conformité de la configuration est une liste de périphériques associés à un modèle de conformité. Un périphérique dans OpenManage Enterprise peut être affecté à 10 lignes de base. Vous pouvez vérifier la conformité d'un maximum de 250 périphériques à la fois. .

Pour afficher la liste des lignes de base, cliquez sur **OpenManage Enterprise** > **Configuration** > **Conformité de la configuration**.

La liste des lignes de base de conformité disponibles dépend de vos privilèges d'accès basés sur les rôles et le périmètre dans OpenManage Enterprise. Par exemple, un administrateur peut afficher et gérer toutes les lignes de base de conformité. Toutefois, un gestionnaire de périphériques peut uniquement afficher et gérer les lignes de base de conformité créées et détenues par ce gestionnaire de périphériques. En outre, les périphériques cibles disponibles pour les gestionnaires de périphériques sont restreints par les périphériques/groupes de périphériques qui sont dans leur périmètre respectif.

Vous pouvez créer une ligne de base de conformité de la configuration en :

- Utilisant un modèle de déploiement existant. Voir Gestion de la conformité de la configuration du périphérique , page 110.
- Utilisant un modèle capturé à partir d'un dispositif de support. Voir Créer un modèle de conformité à partir d'un appareil de référence , page 112.
- Utilisant un modèle importé à partir d'un fichier. Voir Créer un modèle de conformité par importation depuis un fichier , page 112.

Lorsque vous sélectionnez un modèle pour créer une ligne de base, les attributs associés aux modèles sont également sélectionnés. Cependant, vous pouvez modifier les propriétés de la ligne de base. Voir Modification d'une ligne de base de conformité de la configuration , page 114.

PRÉCAUTION : Si un modèle de conformité utilisé pour une ligne de base est déjà associé à une autre ligne de base, la modification des propriétés du modèle change les niveaux de conformité de ligne de base des appareils déjà associés. Lisez attentivement les messages d'événement et d'erreur affichés et agissez en conséquence. Pour plus d'informations les messages d'erreur et d'événement, voir le *Guide de référence des messages d'erreur et d'événement* disponible sur le site de support.

REMARQUE : Avant de créer une ligne de base de conformité de la configuration, assurez-vous d'avoir créé le modèle de conformité correspondant.

1. Sélectionnez **Configuration** > **Conformité de la configuration** > **Créer une ligne de base**.
2. Dans la boîte de dialogue **Créer une ligne de base de conformité** :
   - Dans la section **Informations sur la configuration de base** :
   a. Dans le menu déroulant **Modèle**, sélectionnez un modèle de conformité. Pour plus d'informations sur les modèles, voir Gestion de la conformité de la configuration du périphérique , page 110.
   b. Saisissez le nom et la description d'une ligne de base de conformité.
   c. Cliquez sur **Suivant**.
   - Dans la section **Cible** :
   a. Sélectionnez des périphériques ou des groupes de périphériques. Seuls les périphériques compatibles sont affichés. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.

   REMARQUE : Seuls les périphériques compatibles sont répertoriés. Si vous sélectionnez un groupe, les appareils qui ne sont pas compatibles avec le modèle de conformité, ou les appareils qui ne prennent pas en charge la fonctionnalité de ligne de base de conformité de la configuration, sont exclusivement identifiés pour vous aider à procéder à une sélection efficace.
3. Cliquez sur **Terminer**.
   Une ligne de base de conformité est créée et indiquée. Une comparaison de conformité est lancée lorsque la ligne de base est créée ou mise à jour. Le niveau de conformité global de la ligne de base est indiqué dans la colonne **Conformité**. Pour plus d'informations sur les champs de la liste, voir Gestion de la conformité de la configuration du périphérique , page 110.

   REMARQUE : Chaque fois que vous créez une ligne de base de configuration, l'appliance crée et exécute automatiquement une tâche d'inventaire de configuration pour effectuer l'inventaire des appareils associés à la ligne de base pour laquelle les données d'inventaire ne sont pas disponibles. Cette tâche d'inventaire de configuration porte le même nom que la ligne de base pour laquelle l'inventaire est effectué. En outre, sur la page Conformité de la configuration, une barre de progression indiquant la progression de la tâche d'inventaire s'affiche en regard de la ligne de base correspondante.

Information associée

Gestion de la conformité de la configuration du périphérique , page 110
Suppression d'une ligne de base de conformité de la configuration , page 116

Modification d'une ligne de base de conformité de la configuration

Vous pouvez modifier les périphériques, le nom et d'autres propriétés associées à une ligne de base de configuration. Pour obtenir la description des champs affichés dans la liste, voir Gestion de la conformité de la configuration du périphérique , page 110.

PRÉCAUTION : Si un modèle de conformité utilisé pour une ligne de base est déjà associé à une autre ligne de base, la modification des propriétés du modèle change les niveaux de conformité de ligne de base des appareils déjà associés. Voir Modifier un modèle de conformité , page 113. Lisez attentivement les messages d'événement et d'erreur affichés et agissez en conséquence. Pour plus d'informations les messages d'erreur et d'événement, voir le *Guide de référence des messages d'erreur et d'événement* disponible sur le site de support.

1. Sélectionnez **Configuration** > **Conformité de la configuration**.
2. Dans la liste des lignes de base de conformité de la configuration, cochez la case correspondante, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier la ligne de base de conformité**, mettez les informations à jour. Voir Création d'une ligne de base de conformité de la configuration , page 113.

   REMARQUE : Chaque fois que vous modifiez une ligne de base de configuration, une tâche d'inventaire de configuration est automatiquement déclenchée pour effectuer l'inventaire des appareils associés à la ligne de base pour laquelle les données d'inventaire ne sont pas disponibles. Cette tâche d'inventaire de configuration porte le même nom que la ligne de base pour

laquelle l'inventaire est effectué. En outre, sur la page Conformité de la configuration, une barre de progression indiquant la progression de la tâche d'inventaire s'affiche en regard de la ligne de base correspondante.

Tâches associées

Gérer les modèles de conformité , page 111
Sélection d'un critère de requête , page 58

Information associée

Gestion de la conformité de la configuration du périphérique , page 110
Suppression d'une ligne de base de conformité de la configuration , page 116

Suppression des lignes de base de conformité de la configuration

Vous pouvez supprimer les lignes de base de conformité de la configuration sur la page **Configuration** > **Conformité de la configuration** et délier les appareils des lignes de base associées.

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

Pour supprimer les lignes de base de conformité de la configuration :

1. Sélectionnez la ou les lignes de base dans la liste des lignes de base sur la page Conformité de la configuration.
2. Cliquez sur **Supprimer**, puis sur **Oui** à l'invite de commande.

Les lignes de base de configuration supprimées sont retirées de la page Conformité de la configuration.

Actualisation de la conformité des lignes de base de conformité de la configuration

La vérification de l'état de conformité d'une ligne de base de conformité est déclenchée automatiquement si des modifications sont apportées aux attributs du modèle de référence de la ligne de base ou à l'inventaire de configuration de l'un des appareils associés à la ligne de base.

L'état de conformité d'une ligne de base de conformité de la configuration est un niveau de conformité cumulatif des appareils associés à cette ligne de base de conformité de la configuration. L'état d'un périphérique ayant un niveau de conformité inférieur (critique, par exemple) est indiqué comme l'état de l'ensemble de la ligne de base.

Le récapitulatif de la conformité globale de toutes les lignes de base de configuration est représenté par un graphique circulaire situé au-dessus de la grille de la ligne de base. La date et l'heure de la dernière exécution de la conformité s'affichent sous le graphique.

La vérification de l'état de la conformité des lignes de base volumineuses peut prendre plusieurs minutes. Toutefois, vous pouvez cliquer sur **Actualiser la conformité** pour obtenir à la demande un récapitulatif de la conformité globale des appareils pendant que les tâches de conformité des lignes de base volumineuses sont en cours d'exécution.

REMARQUE : Lorsque la conformité de la configuration est en cours d'exécution, le lancement de nouvelles tâches ayant une incidence sur les lignes de base, telles que la modification d'un modèle de conformité ou d'une ligne de base, n'est pas autorisé.

Pour lancer l'actualisation du récapitulatif de conformité globale de toutes les lignes de base, procédez comme suit :

1. Cliquez sur **Configuration** > **Conformité de la configuration** pour afficher la page Conformité de la configuration.
2. Cliquez sur **Actualiser la conformité**.

La tâche d'actualisation de la conformité (chargement du récapitulatif de conformité) est lancée. Le récapitulatif de conformité globale à ce moment-là s'affiche et l'heure de la dernière exécution de la conformité est mise à jour.

Correction des périphériques non conformes

Sur la page Rapport de conformité d'une ligne de base, vous pouvez corriger les appareils qui ne correspondent pas à la ligne de base associée en modifiant les valeurs d'attribut pour qu'elles correspondent aux attributs de ligne de base associés.

La page Rapport de conformité affiche les champs suivants pour les appareils cibles associés à la ligne de base du modèle de conformité :

- **CONFORMITÉ** : l'état de l'appareil ayant un niveau de conformité inférieur (critique, par exemple) est indiqué comme l'état de l'appareil.
- **NOM DU PÉRIPHÉRIQUE** : nom de l'appareil cible associé à la ligne de base.
- **ADRESSE IP** : adresse IP de l'appareil cible.
- **TYPE** : type de l'appareil cible associé.
- **MODÈLE** : nom du modèle de l'appareil cible.
- **NUMÉRO DE SÉRIE** : numéro de série de l'appareil cible.
- **HEURE DE LA DERNIÈRE EXÉCUTION** : date et heure de dernière exécution de la ligne de base de conformité.

Vous pouvez utiliser les filtres avancés pour identifier rapidement les appareils non conformes. En outre, la prise en charge des fonctionnalités de tri et Sélectionner tout peut être utilisée sur les résultats de conformité de la configuration. Pour annuler les filtres, cliquez sur **Effacer les filtres**.

Pour afficher les attributs dérivés d'un appareil cible non conforme, sélectionnez l'appareil, puis cliquez sur **Afficher le rapport**. Le **Rapport de conformité** de l'appareil cible respectif répertorie les noms d'attributs avec les valeurs attendues et actuelles de ces derniers.

Pour corriger un ou plusieurs périphériques non conformes :

1. Sélectionnez **Configuration** > **Conformité de la configuration**.
2. Dans la liste des lignes de base de conformité de la configuration, sélectionnez la case correspondante, puis cliquez sur **Afficher le rapport**.
3. Dans la liste des périphériques non conformes, sélectionnez un ou plusieurs périphériques, puis cliquez sur **Rendre conforme**.
4. Planifiez les changements de configuration pour les exécuter immédiatement ou plus tard, puis cliquez sur **Terminer**.

   Pour appliquer les changements de configuration après le prochain redémarrage du serveur, vous pouvez sélectionner l'option **Modification de la configuration du ou des périphériques lors du prochain redémarrage**.

Une nouvelle tâche d'inventaire de configuration est exécutée et l'état de conformité de la ligne de base est mis à jour sur la page **Conformité**.

Exporter le rapport de ligne de base de conformité

Une liste complète ou partielle des appareils associés à une ligne de base de modèle de conformité peut être exportée vers un fichier CSV.

Sur la page Rapport de conformité d'une ligne de base de configuration

1. Cliquez sur **Exporter tout** pour exporter les détails relatifs à tous les appareils dans la ligne de base de conformité. Ou
2. Cliquez sur **Exporter la sélection** après avoir sélectionné les appareils individuels dans le rapport.

Suppression d'une ligne de base de conformité de la configuration

Vous pouvez supprimer le niveau de conformité de la configuration des périphériques associés à une ligne de base de configuration. Pour obtenir la description des champs affichés dans la liste, voir Gestion de la conformité de la configuration du périphérique , page 110.

PRÉCAUTION : Lorsque vous supprimez une ligne de base de conformité ou un ou plusieurs périphérique(s) d'une ligne de base de conformité :

- **Les données de conformité de la ligne de base et/ou le ou les périphériques sont supprimés des données OpenManage Enterprise.**
- **Si un périphérique est supprimé, son inventaire de configuration n'est plus récupéré et les informations déjà récupérées sont également supprimées, sauf si l'inventaire est associé à une tâche d'inventaire.**

Un modèle de conformité utilisé comme ligne de base de conformité ne peut pas être supprimé s'il est associé à un appareil. Des messages appropriés s'affichent dans de tels cas. Lisez attentivement les messages d'événement et d'erreur affichés et agissez en conséquence.

Pour plus d'informations les messages d'erreur et d'événement, voir le *Guide de référence des messages d'erreur et d'événement* disponible sur le site de support.

1. Cliquez sur **Configuration** > **Conformité de la configuration**.
2. Dans la liste de lignes de base de conformité de la configuration, cochez la case correspondante, puis cliquez sur **Supprimer**.
3. À l'invite de sélection ou non de la suppression, cliquez sur **OUI**.
   La ligne de base de conformité est supprimée et le tableau **Récapitulatif de conformité global** des lignes de base est mis à jour.

Tâches associées

Création d'une ligne de base de conformité de la configuration , page 113
Sélection d'un critère de requête , page 58
Gérer les modèles de conformité , page 111
Modification d'une ligne de base de conformité de la configuration , page 114

Information associée

Gestion de la conformité de la configuration du périphérique , page 110

14

Surveillance et gestion des alertes d'appareil

En sélectionnant **OpenManage Enterprise** > **Alertes**, vous pouvez afficher et gérer les alertes générées par les appareils dans l'environnement du système de gestion. La page Alertes présente les onglets suivants :

- **Journal des alertes** : vous pouvez afficher et gérer toutes les alertes générées sur les appareils cibles.
- **Politiques d'alerte** : vous pouvez créer des politiques d'alerte pour envoyer les alertes générées sur les appareils cibles à différentes destinations (adresse e-mail, numéro de téléphone, serveur Syslog, etc.).
- **Définitions d'alerte** : vous pouvez afficher les alertes générées en cas d'erreur ou à titre informatif.

REMARQUE :

- Pour gérer et surveiller des alertes de périphériques sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les stratégies et les journaux d'alertes sont régis par l'accès basé sur le périmètre dont vous disposez dans OpenManage Enterprise. Par exemple, un administrateur peut afficher et gérer toutes les stratégies d'alerte, mais les gestionnaires de périphériques peuvent uniquement afficher et gérer les stratégies d'alerte par défaut et les stratégies qu'ils créent et détiennent. En outre, les gestionnaires de périphériques peuvent uniquement afficher les alertes pour les périphériques qui se trouvent dans leur périmètre.
- Actuellement, OpenManage Enterprise reçoit uniquement les alertes SNMPv1 et SNMPv2 des serveurs PowerEdge suivants : MX840c et MX5016s.
- L'application OpenManage Enterprise fournit un rapport intégré qui affiche la liste des périphériques qu'elle surveille ainsi que les alertes générées pour chaque périphérique. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Nombre d'alertes par rapport de périphérique**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140

Concepts associés

Affichage des journaux d'alertes , page 118

Sujets :

Affichage des journaux d'alertes

La page **Journal des alertes** affiche la liste des journaux d'alertes pour les événements survenus sur les appareils. Dans OpenManage Enterprise, cliquez sur **Alertes** > **Journal des alertes**. La page **Journal des alertes** s'affiche.

Par défaut, seules les alertes qui n'ont pas été acquittées s'affichent. Vous pouvez personnaliser la liste des alertes à l'aide des **Filtres avancés**, situés en haut à gauche de la liste des alertes, ou en modifiant les **Paramètres d'affichage des alertes** sur la page **Paramètres d'application**. Voir Personnalisation de l'affichage des alertes , page 166. Vous pouvez afficher les détails d'alerte suivants :

- **Accusé de réception** : si l'alerte a été acquittée, une coche apparaît sous **ACCUSÉ DE RÉCEPTION**. Cliquez entre les crochets sous **ACCUSÉ DE RÉCEPTION** pour acquitter une alerte ou annuler son acquittement.
- **Heure** : heure à laquelle l'alerte a été générée.
- **Nom de la source** : nom de l'hôte du système d'exploitation de l'appareil qui a généré l'alerte. Cliquez sur le nom de la source pour afficher et configurer les propriétés de l'appareil.

  REMARQUE : Les alertes ne peuvent pas être filtrées en fonction de l'adresse IP (nom de la source) si l'alerte est générée à partir d'un périphérique non détecté ou dans le cas d'une alerte interne.
- **Catégorie** : la catégorie indique le type d'alerte. Par exemple, intégrité du système ou audit.
- **ID du message** : ID de l'alerte générée.
- **Message** : alerte générée.

- La zone sur la droite fournit des informations supplémentaires, telles qu'une description détaillée et l'action recommandée pour l'alerte sélectionnée.

REMARQUE : OpenManage Enterprise version 3.2 et supérieures permet d'effectuer le suivi du point de données **Auteur de la dernière mise à jour**, alors que ce n'était pas le cas dans les versions précédentes. Par conséquent, sachez que si le Journal d'alertes est filtré en fonction du champ avancé **Utilisateur**, les alertes acceptées sur les versions précédentes ne s'affichent pas.

Sélectionnez une alerte pour afficher des informations supplémentaires, telles qu'une description détaillée et l'action recommandée sur le côté droit de la page Journal des alertes. Vous pouvez effectuer les opérations suivantes sur la page Journal des alertes :

- Accuser réception des alertes
- Non acceptation des alertes
- Ignorer des alertes
- Exporter des alertes
- Suppression des alertes
- Alertes archivées

Information associée

Surveillance et gestion des alertes d'appareil , page 118

Gestion des journaux d'alertes

Une fois les journaux d'alertes générés et affichés sur la page **Journal des alertes**, vous pouvez en accuser réception, refuser l'acceptation, ignorer, exporter, supprimer et archiver les alertes.

Accuser réception des alertes

Une fois que vous avez affiché une alerte et saisi son contenu, vous pouvez confirmer que vous l'avez lue au moyen d'un message d'alerte. Acquitter une alerte évite de stocker le même événement dans le système. Par exemple, si un périphérique est bruyant et génère plusieurs fois le même événement, vous pouvez ignorer les autres enregistrements de l'alerte en acquittant les événements qui sont reçus du périphérique. En outre, aucun événement du même type ne sera plus enregistré.

Pour accuser réception d'une alerte, sur la page **Journal des alertes**, cochez la case correspondant à l'alerte, puis cliquez sur **Accuser réception**.

Une coche s'affiche dans la colonne **ACCEPTER**. Dès qu'une alerte est acceptée, le champ **Auteur de la dernière mise à jour**, situé dans la section détails des alertes, est renseigné automatiquement.

Non acceptation des alertes

Vous pouvez annuler l'acquittement des journaux d'alertes qui ont été acquittés (ou acceptés). Annuler l'acquittement d'une alerte implique que tous les événements de tout périphérique sont enregistrés, même lorsque le même événement se reproduit fréquemment. Par défaut, toutes les alertes sont sélectionnées.

Pour refuser des alertes, cochez la case correspondant aux alertes, puis cliquez sur le bouton **Ne pas accepter**. Sinon, vous pouvez cliquer sur la coche correspondant à chaque alerte à désaccepter.

REMARQUE : Le champ **Auteur de la dernière mise à jour** dans la section détails de l'alerte conservera le nom d'utilisateur de la dernière personne ayant accepté l'alerte.

Ignorer des alertes

Ignorer une alerte crée une stratégie d'alerte, qui est activée. Cette alerte est ensuite systématiquement ignorée. Cochez la case correspondant à l'alerte, puis cliquez sur **Ignorer**. Un message s'affiche, indiquant qu'une tâche est en cours de création pour ignorer l'alerte sélectionnée. Le nombre total d'alertes affiché dans la ligne d'en-tête d'OpenManage Enterprise est réduit d'une unité.

Exporter des alertes

Vous pouvez exporter des journaux d'alertes au format .csv vers un partage réseau ou disque local sur votre système.

Pour exporter des journaux d'alertes, sur la page **Journal des alertes**, sélectionnez les journaux d'alertes que vous souhaitez exporter et cliquez sur **Exporter** > **Exporter la sélection**. Vous pouvez exporter tous les journaux d'alertes en cliquant sur **Exporter** > **Tout exporter**. Les journaux d'alertes sont exportés au format .csv.

Suppression des alertes

Vous pouvez supprimer une alerte pour retirer définitivement cette occurrence de l'alerte depuis la console.

Cochez la case correspondant à l'alerte, puis cliquez sur **Supprimer**. Un message s'affiche pour confirmer le processus de suppression. Cliquez sur **OUI** pour supprimer l'alerte. Le nombre total d'alertes affiché dans la ligne d'en-tête d'OpenManage Enterprise est réduit d'une unité.

Affichage d'alertes archivées

Un maximum de 50 000 alertes peut être généré et affiché dans OpenManage Enterprise. Quand 95 % de la limite 50 000 est atteinte (soit 47 500), OpenManage Enterprise génère un message interne indiquant que lorsque le décompte atteint 50 000, OpenManage Enterprise purgera automatiquement 10 % des alertes archivées (soit 5 000). Le tableau répertorie différents scénarios impliquant la purge des alertes.

Tableau 20. Purge des alertes

Workflow	Description	Résultat
Tâche de purge	S'exécute toutes les 30 minutes sur la console.	Si les alertes ont atteint leur capacité maximale (qui est de 50 000), vérifiez et générez des archives de purge.
Avertissement sur la purge des alertes	Génère un avertissement interne sur la purge des alertes.	Si les alertes ont dépassé plus de 95 % (c'est-à-dire, 47 500), génère un avertissement de purge interne pour purger 10 % des alertes.
Purge des alertes	Alertes purgées dans le journal d'alertes.	Si le nombre d'alertes est supérieur à 100 %, 10 % des anciennes alertes sont purgées pour revenir à 90 % (soit 45 000).
Télécharger les alertes de purge	Téléchargez des alertes purgées.	Les archives des cinq alertes purgées en dernier peuvent être téléchargées à partir des Alertes archivées.

Téléchargement d'alertes archivées

Les alertes archivées correspondent au 10 % des alertes les plus anciennes (soit 5 000) qui sont purgées lorsque le nombre d'alertes dépasse 50 000. Ces 5 000 alertes les plus anciennes sont supprimées du tableau et stockées dans un fichier .csv, puis archivées. Pour télécharger le fichier d'une alerte archivée, procédez comme suit :

1. Cliquez sur **Alertes archivées**.

   Dans la boîte de dialogue **Alertes archivées**, les cinq alertes archivées à avoir été purgées en dernier s'affichent. Le nom, la taille de fichier et la date d'archivage sont indiqués.

2. Cochez la case correspondant au fichier d'alerte et cliquez sur **Terminer**. Le fichier .CSV est téléchargé vers l'emplacement que vous avez sélectionné.

REMARQUE : Pour télécharger les alertes archivées, vous devez bénéficier des privilèges nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Stratégies d'alerte

Cette rubrique présente les politiques d'alerte et leur utilité. Pour obtenir des instructions sur la création, la modification, l'activation, la désactivation et la suppression des politiques d'alerte, reportez-vous à *Configuration et gestion des politiques d'alerte*.

Les politiques d'alerte vous permettent de configurer et d'envoyer des alertes concernant des appareils ou composants spécifiques à une destination donnée, par exemple une adresse e-mail, un numéro de mobile, un serveur Syslog, etc. Les alertes vous aident à surveiller et gérer efficacement les appareils.

Vous pouvez utiliser les politiques d'alerte pour effectuer les opérations suivantes :

- Déclencher automatiquement des actions en fonction de l'entrée d'une alerte.
- Envoyer une alerte à une adresse e-mail.
- Envoyer une alerte à un téléphone au moyen d'un SMS ou d'une notification.
- Envoyer une alerte via un trap SNMP.
- Envoyer une alerte à un serveur Syslog.
- Exécuter des actions de contrôle de l'alimentation d'un appareil, telles que la mise sous ou hors tension d'un appareil lorsqu'une alerte d'une catégorie prédéfinie est générée.
- Exécuter un script à distance.

Pour afficher, créer, modifier, activer, désactiver et supprimer des politiques d'alerte, cliquez sur **Alertes** > **Politiques d'alerte**.

Tâches associées

Configuration et gestion des politiques d'alerte , page 121

Configuration et gestion des politiques d'alerte

Cette rubrique fournit des instructions sur la création, la modification, l'activation, la désactivation et la suppression de politiques d'alerte.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Information associée

Stratégies d'alerte , page 120
Transmission de journaux d'audit vers des serveurs Syslog distants , page 123

Créer une politique d'alerte

Vous pouvez créer des politiques d'alerte et les activer pour envoyer des alertes à une adresse e-mail, un numéro de téléphone ou des traps SNMP et exécuter des actions de contrôle d'appareil, telles qu'une mise sous tension ou hors tension, un cycle d'alimentation ou un arrêt normal lorsqu'une alerte d'une catégorie prédéfinie est générée.

REMARQUE : Après une mise à niveau depuis la version 3.5 ou une version antérieure, toutes les stratégies d'alerte créées par les gestionnaires de périphériques à partir d'une version antérieure d'OpenManage Enterprise sont uniquement affectées à l'administrateur. Par conséquent, les gestionnaires de périphériques doivent recréer les stratégies d'alerte post-mise à niveau pour continuer à recevoir des alertes.

Sur la page **Alertes** > **Politiques d'alerte**, cliquez sur **Créer**, puis procédez comme suit :

1. Saisissez un nom et une description pour la politique d'alerte, puis cliquez sur **Suivant**. La case **Activer la politique** est cochée par défaut.
2. Choisissez la catégorie d'alerte en sélectionnant une ou plusieurs catégories de la base d'informations de gestion (MIB) tierces importées et intégrées.

   Vous pouvez développer chaque catégorie pour afficher et sélectionner les sous-catégories. Pour en savoir plus sur les catégories et sous-catégories, reportez-vous à Définitions des alertes , page 126.
3. Sélectionnez les appareils ou groupes pour lesquels une alerte est requise, puis cliquez sur **Suivant**. Une alerte peut être appliquée à :
   - un ou plusieurs appareils ;
   - un ou plusieurs groupes d'appareils ;
   - un appareil non détecté spécifié par son adresse IP ou son nom d'hôte ;
   - tout appareil non détecté.

     REMARQUE : Les tâches Exécution de script à distance et Action d'alimentation ne peuvent pas être effectuées sur des appareils non détectés.

REMARQUE : Les alertes des protocoles SNMPv1, SNMPv2 et SNMPv3 envoyées par ces périphériques non détectés (étrangers) sont reconnues par OpenManage Enterprise.

4. (Facultatif) Spécifiez la durée pendant laquelle la politique d'alerte est applicable en sélectionnant les valeurs requises de **Plage de dates**, **Intervalle de temps** et **Jours**, puis cliquez sur **Suivant**.
5. Sélectionnez le niveau de gravité de l'alerte, puis cliquez sur **Suivant**.

   Pour sélectionner toutes les catégories de gravité, cochez la case **Toutes**.
6. Sélectionnez une ou plusieurs actions d'alerte, puis cliquez sur **Suivant**. Les options disponibles sont les suivantes :
   - E-mail : sélectionnez E-mail pour envoyer un e-mail à un destinataire spécifique en saisissant des informations dans chaque champ et en utilisant des jetons pour l'objet et le message, le cas échéant. Voir Substitution de jeton dans les scripts distants et la stratégie d'alerte , page 182

     REMARQUE : Des e-mails pour plusieurs alertes de même catégorie, ID de message et contenu sont envoyés une seule fois toutes les 2 minutes pour éviter les messages d'alerte répétitifs ou redondants dans la boîte de réception.
   - Transfert des Trap SNMP (Activer) : cliquez sur Activer pour afficher la fenêtre Configuration SNMP dans laquelle configurer les paramètres SNMP pour l'alerte. Voir Configuration des alertes SMTP, SNMP et Syslog , page 123.
   - Syslog (Activer) : cliquez sur Activer pour afficher la fenêtre Configuration de Syslog dans laquelle configurer les paramètres du journal système pour l'alerte. Voir Configuration des alertes SMTP, SNMP et Syslog , page 123.
   - Cochez la case Ignorer pour ignorer le message d'alerte et ne pas activer la stratégie d'alerte.
   - Envoyer un SMS à un numéro de téléphone spécifique.
   - Contrôle de l'alimentation : cochez la case Contrôle de l'alimentation pour afficher les actions qui permettent de mettre un appareil sous tension ou hors tension, d'effectuer un cycle d'alimentation ou de l'arrêter normalement. Pour arrêter un système d'exploitation avant d'exécuter des actions de contrôle de l'alimentation, cochez la case **Arrêter le système d'exploitation en premier**.
   - Exécution de script à distance (Activer) : cliquez sur Activer pour afficher la fenêtre Paramètre des commandes à distance dans laquelle vous pouvez ajouter et exécuter des commandes à distance sur des nœuds distants. Pour en savoir plus sur l'ajout de commandes à distance, consultez Exécution des commandes et scripts distants , page 124.

     Dans le menu déroulant, sélectionnez le script que vous souhaitez exécuter lorsque cette politique d'alerte est exécutée. Vous pouvez configurer l'exécution de la commande à distance également comme décrit dans Gestion des paramètres de l'appliance OpenManage Enterprise , page 147.
   - Envoyer une notification au téléphone mobile enregistré auprès d'OpenManage Enterprise. Voir Paramètres d'OpenManage Mobile , page 175.
7. Passez en revue les détails de la politique d'alerte créée dans l'onglet Résumé, puis cliquez sur **Terminer**.
   La stratégie d'alerte a été créée avec succès et répertoriée dans la section **Stratégies d'alerte**.

Modifier les politiques d'alerte

Une fois que les politiques d'alerte ont été créées sur la page **Politiques d'alerte**, vous pouvez les modifier, les activer, les désactiver et les supprimer. En outre, OME fournit des politiques d'alerte intégrées qui déclenchent des actions associées lors de la réception de l'alerte. Vous ne pouvez pas modifier ou supprimer les politiques d'alerte intégrées. Toutefois, vous pouvez les activer ou les désactiver.

Pour afficher les politiques d'alerte existantes, cliquez sur **Alertes** > **Politiques d'alerte**.

Pour sélectionner toutes les politiques d'alerte, cochez la case à gauche de l'option **Activé**. Cochez une ou plusieurs cases en regard d'une politique d'alerte pour effectuer les actions suivantes :

- **Modifier une politique d'alerte** : sélectionnez une politique d'alerte, puis cliquez sur **Modifier** pour modifier les informations requises dans la boîte de dialogue Configuration et gestion des politiques d'alerte , page 121.

  REMARQUE : Une seule politique d'alerte peut être modifiée à la fois.

  REMARQUE : Par défaut, la case Intervalle de temps est décochée pour les stratégies d'alerte dans les versions d'OpenManage Enterprise antérieures à la version 3.3.1. Après la mise à niveau, cochez la case Intervalle de temps et mettez à jour les champs pour réactiver les stratégies.
- **Activer des politiques d'alerte** : sélectionnez une politique d'alerte et cliquez sur **Activer**. Une coche apparaît dans la colonne **Activé** lorsqu'une politique d'alerte est activée. Le bouton **Activer** d'une stratégie d'alerte déjà activée est grisé.
- **Désactiver des politiques d'alerte** : sélectionnez une politique d'alerte et cliquez sur **Désactiver**. La politique d'alerte est désactivée et la coche dans la colonne **ACTIVÉ** est supprimée.

  Vous pouvez aussi désactiver une politique d'alerte lorsque vous la créez en décochant la case à cocher **Activer la politique** dans la section Nom et description.
- **Supprimer des politiques d'alerte** : sélectionnez une politique d'alerte et cliquez sur **Supprimer**.

Vous pouvez supprimer plusieurs règles d'alerte à la fois en cochant les cases correspondantes. Pour cocher ou décocher toutes les cases, cochez la case dans la ligne d'en-tête en regard de la colonne **ACTIVÉ**.

Transmission de journaux d'audit vers des serveurs Syslog distants

Pour surveiller tous les journaux d'audit d'OpenManage Enterprise depuis des serveurs Syslog, créez une stratégie d'alerte. Tous les journaux d'audit, notamment les tentatives de connexion d'utilisateurs, la création de stratégies d'alerte et l'exécution de différentes tâches peuvent être transmis aux serveurs Syslog.

Pour créer une stratégie d'alerte afin de transmettre les journaux d'audit à des serveurs Syslog :

1. Sélectionnez **Alertes** > **Stratégies d'alerte** > **Créer**.
2. Dans la boîte de dialogue **Créer une stratégie d'alerte**, dans la section **Nom et description**, saisissez le nom et la description de la stratégie d'alerte.
   a. La case **Activer la stratégie** est cochée par défaut pour indiquer que la stratégie d'alerte sera activée une fois créée. Pour désactiver la stratégie d'alerte, décochez la case. Pour en savoir plus sur l'activation des stratégies d'alerte à une date ultérieure, voir la section Configuration et gestion des politiques d'alerte , page 121.
   b. Cliquez sur **Suivant**.
3. Dans la section **Catégorie**, développez l'arborescence **Application** et sélectionnez les catégories et sous-catégories des journaux de l'appliance. Cliquez sur **Suivant**.
4. Dans la section **Cible**, l'option **Sélectionner des périphériques** est sélectionnée par défaut. Cliquez sur **Sélectionner des périphériques** et sélectionnez des périphériques dans le volet de gauche. Cliquez sur **Suivant**.

   REMARQUE : Il n'est pas possible de sélectionner des périphériques ou des groupes cibles lors de la transmission des journaux d'audit au serveur Syslog.

5. (Facultatif) Par défaut, les stratégies d'alerte sont toujours actives. Pour limiter l'activité, dans la section **Date et heure**, sélectionnez les dates de début et de fin, puis sélectionnez le délai d'exécution.
   a. Cochez les cases correspondant aux jours auxquels les stratégies d'alerte doivent être exécutées.
   b. Cliquez sur **Suivant**.
6. Dans la section **Gravité**, sélectionnez le niveau de gravité des alertes pour lesquelles cette stratégie doit être activée.
   a. Pour sélectionner toutes les catégories de gravité, cochez la case **Toutes**.
   b. Cliquez sur **Suivant**.
7. Dans la section **Actions**, sélectionnez **Syslog**.

   Si les serveurs Syslog ne sont pas configurés dans OpenManage Enterprise, cliquez sur **Activer** et saisissez l'adresse IP de destination ou le nom d'hôte des serveurs Syslog. Pour en savoir plus sur la configuration des serveurs Syslog, voir la section Configuration des alertes SMTP, SNMP et Syslog , page 123.
8. Cliquez sur **Suivant**.
9. Dans la section **Résumé**, les détails de la stratégie d'alerte que vous avez définis s'affichent. Lisez attentivement les informations.
10. Cliquez sur **Terminer**.

La stratégie d'alerte a été créée avec succès et répertoriée dans la section **Stratégies d'alerte**.

Tâches associées

Configuration et gestion des politiques d'alerte , page 121
Surveillance des journaux d'audit , page 127

Configuration des alertes SMTP, SNMP et Syslog

En cliquant sur **OpenManage Enterprise** > **Paramètres de l'application** > **Alertes**, vous pouvez configurer l'adresse e-mail (SMTP) qui reçoit les alertes système, les destinations de transfert des alertes SNMP et les propriétés de transfert Syslog. Pour gérer ces paramètres, vous devez disposer d'informations d'identification OpenManage Enterprise de niveau administrateur.

Pour configurer et authentifier le serveur SMTP qui gère la communication par e-mail entre les utilisateurs et OpenManage Enterprise :

REMARQUE : OpenManage Enterprise ne peut pas envoyer d'e-mail à un serveur SMTP interne disposant d'un certificat émis par une autorité de certification racine interne.

1. Développez **Configuration des e-mails**.

2. Saisissez l'adresse réseau du serveur SMTP qui envoie les e-mails.
3. Pour authentifier le serveur SMTP, cochez la case **Activer l'authentification** et saisissez le nom d'utilisateur et le mot de passe.
4. Par défaut, le numéro de port SMTP à atteindre est 25. Si nécessaire, modifiez-le.
5. Cochez la case **Utiliser SSL** pour sécuriser votre transaction SMTP.
6. Pour vérifier si le serveur SMTP fonctionne correctement, cliquez sur la case à cocher **Envoyer un e-mail test** et saisissez un **Destinataire d'e-mail**.
7. Cliquez sur **Appliquer**.
8. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Pour configurer le transfert des alertes SNMP :

1. Développez **Configuration du transfert des alertes SNMP**.
2. Cochez la case **ACTIVÉ** pour activer les interruptions SNMP respectives afin d'envoyer des alertes en cas d'événements prédéfinis.
3. Dans la zone **ADRESSE DE DESTINATION**, saisissez l'adresse IP du périphérique de destination qui doit recevoir l'alerte.

   REMARQUE : La saisie de l'adresse IP de la console n'est pas autorisée pour éviter la duplication des alertes.
4. Dans le menu **VERSION SNMP**, sélectionnez le type de version SNMP : SNMPv1, SNMPv2 ou SNMPv3 et renseignez les champs suivants :
   a. Dans la zone CHAÎNE DE COMMUNAUTÉ, saisissez la chaîne de la communauté SNMP du périphérique qui doit recevoir l'alerte.
   b. Si nécessaire, modifiez le NUMÉRO DE PORT. Le numéro de port par défaut pour les interruptions SNMP est le 162. Voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
   c. Si SNMPv3 est sélectionné, fournissez les informations supplémentaires suivantes :
      i. NOM D'UTILISATEUR : fournissez un nom d'utilisateur.
      ii. TYPE D'AUTHENTIFICATION : dans la liste déroulante, sélectionnez SHA, MD_5 ou Aucun.
      iii. PHRASE SECRÈTE D'AUTHENTIFICATION : fournissez une phrase secrète d'authentification comportant au moins huit caractères.
      iv. TYPE DE CONFIDENTIALITÉ : dans la liste déroulante, sélectionnez DES, AES_128 ou Aucun.
      v. PHRASE SECRÈTE DE CONFIDENTIALITÉ : fournissez une phrase secrète de confidentialité contenant au moins huit caractères.
5. Pour tester un message SNMP, cliquez sur le bouton **Envoyer** de l'interruption correspondante.
6. Cliquez sur **Appliquer**. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Pour mettre à jour la configuration de transfert Syslog, procédez comme suit :

1. Développez **Configuration des transferts Syslog**.
2. Cochez la case pour activer la fonctionnalité Syslog sur le serveur respectif dans la colonne **SERVEUR**.
3. Dans la zone **NOM DE L'HÔTE/ADRESSE DE DESTINATION**, saisissez l'adresse IP du périphérique qui doit recevoir les messages Syslog.
4. Le numéro de port par défaut lorsque UDP est utilisé est le 514. Si nécessaire, modifiez-le, en saisissant ou en effectuant une sélection dans la zone. Voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
5. Cliquez sur **Appliquer**.
6. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Exécution des commandes et scripts distants

Lorsque vous obtenez une interruption SNMP, vous pouvez exécuter un script sur OpenManage Enterprise. Cette opération configure une règle qui ouvre un ticket sur votre système de génération de tickets tiers à des fins de gestion des alertes. Vous pouvez créer et stocker un maximum de **quatre** commandes à distance.

REMARQUE : Les caractères spéciaux suivants ne sont pas pris en charge dans les paramètres RACADM et IPMI CLI : **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * et **'**.

1. Cliquez sur **Paramètres d'application** > **Exécution de script**.
2. Dans la section **Paramètres de commandes distantes**, procédez comme suit :
   a. Pour ajouter une commande à distance, cliquez sur **Créer**.
   b. Dans le champ **Nom de la commande**, saisissez le nom de la commande.
   c. Sélectionnez l'un des types de commande suivants :
      i. Script
      ii. RACADM
      iii. Outil IPMI
   d. Si vous sélectionnez **Script**, procédez comme suit :
      i. Dans la boîte de dialogue **Adresse IP**, saisissez l'adresse IP.

ii. Sélectionnez la méthode d'authentification : **Mot de passe** ou **Clé SSH**.
iii. Saisissez le **nom d'utilisateur** et le **mot de passe** ou la **clé SSH**.
iv. Dans le champ **Commande**, saisissez les commandes.
- Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.
- La substitution de jeton dans les scripts est possible. Voir Substitution de jeton dans les scripts distants et la stratégie d'alerte , page 182

v. Cliquez sur **Terminer**.

e. Si vous sélectionnez **RACADM**, procédez comme suit :
i. Dans le champ **Nom de la commande**, saisissez le nom de la commande.
ii. Dans le champ **Commande**, saisissez les commandes. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.
iii. Cliquez sur **Terminer**.

f. Si vous sélectionnez **Outil IPMI**, procédez comme suit :
i. Dans le champ **Nom de la commande**, saisissez le nom de la commande.
ii. Dans le champ **Commande**, saisissez les commandes. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.
iii. Cliquez sur **Terminer**.

3. Pour modifier un paramètre d'une commande à distance, sélectionnez cette dernière, puis cliquez sur **Modifier**.
4. Pour supprimer un paramètre d'une commande à distance, sélectionnez cette dernière, puis cliquez sur **Supprimer**.

Actualisation automatique du châssis MX7000 lors de l'insertion et du retrait des traîneaux

OpenManage Enterprise peut presque instantanément refléter l'ajout ou la suppression de traîneaux après la détection ou l'intégration d'un châssis MX7000 autonome ou maître.

Lorsqu'un châssis MX7000 autonome ou maître est détecté ou intégré à l'aide d'OpenManage Enterprise (version 3.4 et ultérieure), une stratégie d'alerte est créée simultanément sur le châssis MX7000. Pour plus d'informations sur la détection et l'intégration de périphériques dans OpenManage Enterprise, reportez-vous aux sections Création d'une tâche de détection de périphérique , page 44 et Intégration de périphériques , page 45.

La stratégie d'alerte créée automatiquement dans l'appliance OpenManage Enterprise-Modular pour MX7000 déclenche une tâche d'actualisation de l'inventaire de châssis, nommée **Actualiser l'inventaire de châssis** dans OpenManage Enterprise chaque fois qu'un traîneau est inséré, retiré ou remis en place dans le châssis MX7000.

Après l'achèvement de la tâche d'actualisation de l'inventaire de châssis, les modifications associées aux traîneaux, apportées au châssis MX7000, s'affichent à la page Tous les périphériques.

Les conditions préalables suivantes doivent être remplies lors de l'intégration du châssis MX7000 pour créer la stratégie d'alerte automatique :

- L'application OpenManage Enterprise-Modular version 1.2 doit déjà être installée dans le châssis MX7000.
- Le châssis MX7000 doit être intégré avec les options **Activer la réception d'interruptions pour les serveurs iDRAC et les châssis MX7000 détectés** et **Définir la chaîne de communauté pour la destination d'interruption à partir des paramètres d'application**.
- L'adresse IP de l'appliance OpenManage Enterprise doit être enregistrée comme l'une des quatre destinations d'alerte disponibles dans le châssis MX7000 nouvellement intégré. Si toutes les destinations d'alerte du châssis MX7000 sont déjà configurées au moment de l'intégration, la création de la stratégie d'alerte automatique échoue.

REMARQUE :

- La stratégie d'alerte sur le châssis MX7000 est uniquement propre aux traîneaux et ne s'applique pas aux autres composants du châssis, par exemple les IOM.
- Vous pouvez définir des préférences d'alerte pour le châssis MX7000 dans OpenManage Enterprise afin de recevoir toutes les alertes ou uniquement celles de la catégorie de châssis du modèle MX7000. Pour plus d'informations, voir Gestion des préférences de la console , page 164.
- Il convient d'attendre un certain délai entre l'action réelle sur les traîneaux et le déclenchement de l'actualisation de l'inventaire de châssis dans OpenManage Enterprise.
- La stratégie d'alerte créée automatiquement est supprimée si le châssis MX7000 est supprimé de l'inventaire des périphériques d'OpenManage Enterprise.

- La page Tous les périphériques indique l'**État géré** d'un châssis MX7000 correctement intégré avec la stratégie de transfert d'alertes automatique « Géré avec les alertes ». Pour plus d'informations sur l'intégration, reportez-vous à la section Intégration de périphériques , page 45

Définitions des alertes

En cliquant sur **OpenManage Enterprise** > **Alertes** > **Définitions d'alerte**, vous pouvez afficher les alertes générées en cas d'erreur ou à titre informatif. Ces messages sont :

- Appelés messages d'événement et d'erreur.
- Affichés dans l'interface graphique utilisateur (GUI) et dans l'interface de ligne de commande (CLI) pour RACADM et WS-Man.
- Enregistrés dans les fichiers journaux à titre informatif uniquement.
- Numérotés et clairement définis pour vous permettre de mettre en œuvre efficacement des actions correctives et préventives.

Un message d'erreur et d'événement comporte :

- **ID de MESSAGE** : les messages sont classés en fonction de composants tels que le BIOS, la source d'alimentation (PSU), le stockage (STR), les données du journal (LOG) et le Chassis Management Controller (CMC).
- **MESSAGE** : cause réelle d'un événement. Les événements sont uniquement déclenchés à titre informatif, ou lorsqu'il y a une erreur dans l'exécution des tâches.
- **CATÉGORIE** : classe à laquelle le message d'erreur appartient. Pour plus d'informations sur les catégories, voir le *Guide de référence des messages d'erreur et d'événement pour les serveurs Dell EMC PowerEdge*, disponible sur le site de support.
- **Action recommandée** : résolution de l'erreur via l'interface graphique utilisateur, l'interface RACADM ou des commandes WS-Man. Au besoin, il est recommandé de vous reporter aux documents sur le site de support technique ou TechCenter pour plus d'informations.
- **Description détaillée** : plus d'informations concernant un problème pour une résolution simple et rapide.

Vous pouvez afficher plus d'informations sur une alerte en utilisant des filtres tels que l'ID du message, le texte du message, la catégorie et la sous-catégorie. Pour afficher les définitions d'alertes :

1. Dans le menu **OpenManage Enterprise**, sous **Alertes**, cliquez sur **Définitions d'alertes**.

   Sous **Définitions d'alertes**, une liste de tous les messages d'alerte standard s'affiche.

2. Pour rechercher rapidement un message d'erreur, cliquez sur **Filtres avancés**.

Le volet de droite affiche des informations sur les messages d'erreur et d'événement de l'ID de message que vous avez sélectionné dans le tableau.

15

Surveillance des journaux d'audit

OpenManage Enterprise > **Surveiller** > **Journaux d'audit** répertorie les données des fichiers log pour vous aider ou les équipes de support Dell EMC lors du dépannage et de l'analyse. Un journal d'audit est enregistré lorsque :

- Un groupe est attribué ou une autorisation d'accès est modifiée.
- Le rôle d'utilisateur est modifié.
- Actions exécutées sur les périphériques surveillés par OpenManage Enterprise.

Les fichiers des journaux d'audit peuvent être exportés au format CSV. Voir Exportation de toutes les données ou des données sélectionnées , page 68.

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les restrictions basées sur le périmètre ne sont pas applicables aux journaux d'audit.

1. Pour afficher les journaux d'audit, sélectionnez **Surveillance** > **Journaux d'audit**.
   Les journaux d'audit stockés et affichés par OpenManage Enterprise sur les tâches effectuées en utilisant l'appliance s'affichent. Par exemple, les tentatives de connexion d'utilisateurs, la création de stratégies d'alerte et l'exécution de différentes tâches.
2. Pour trier les données dans l'une des colonnes, cliquez sur le titre de la colonne.
3. Pour rechercher rapidement des informations sur un journal d'audit, cliquez sur **Filtres avancés**.
   Les champs suivants s'affichent, et agissent comme des filtres pour rechercher des données rapidement.
4. Saisissez ou sélectionnez les données dans les champs suivants :
   - **Gravité** : sélectionnez le niveau de gravité des données des fichiers log. Les options possibles sont Info, Avertissement et Critique.
     - Critique : un événement inhabituel s'est produit. Une action immédiate est requise.
     - Attention : l'événement est significatif, mais ne requiert pas une action immédiate.
     - Info : tout événement exécuté avec succès.
   - **Heure de début** et **Heure de fin** : pour afficher les journaux d'audit d'une période donnée.
   - **Utilisateur** : pour afficher les journaux d'audit d'un utilisateur donné. Par exemple, Admin, Système, Gestionnaire de périphériques ou Observateur.
   - **Adresse source** : pour afficher les journaux d'audit d'un système donné. Par exemple, le système où vous vous êtes connecté à OpenManage Enterprise.
   - **Catégorie** : pour afficher les journaux d'audit du type audit ou configuration.
     - Audit : entrée générée lorsqu'un utilisateur se connecte ou se déconnecte de l'appliance OpenManage Enterprise.
     - Configuration : entrée générée lorsqu'une action est exécutée sur un appareil cible.
   - **La description contient** : saisissez le texte ou une expression contenu(e) dans les données des fichiers log que vous recherchez. Tous les journaux contenant le texte sélectionné s'affichent. Par exemple, si vous saisissez `warningSizeLimit`, tous les journaux avec ce texte s'affichent.
   - **ID de message** : saisissez l'ID de message. Si les critères de recherche correspondent, seuls les éléments qui correspondent à l'ID de message s'affichent.
5. Pour supprimer le filtre, cliquez sur **Effacer tous les filtres**.
6. Pour exporter un journal d'audit ou tous les journaux d'audit, sélectionnez **Exporter** > **Exporter la sélection** ou **Exporter** > **Exporter tous les journaux d'audit** respectivement. Pour en savoir plus sur l'exportation des journaux d'audit, voir la section Exportation de toutes les données ou des données sélectionnées , page 68.
7. Pour obtenir tous les derniers journaux de la console et créer une archive qui peut être téléchargée, cliquez sur **Dépannage** > **Créer une archive de journaux de console**.
8. Pour télécharger les archives des journaux de la console, cliquez sur **Dépannage** > **Télécharger les journaux de la console archivés**.

REMARQUE :

- actuellement, pour tout châssis M1000e découvert avec un firmware de châssis version 5.1x ou antérieure, la date de la colonne HORODATAGE sous Journaux du matériel s'affiche comme suit : 12 JAN 2013. Toutefois, pour toutes les versions de châssis VRTX et FX2, la bonne date s'affiche.

- Le fichier ne sera pas immédiatement prêt à être téléchargé, en particulier dans les cas où un grand nombre de journaux sont collectés. Le processus de collecte s'effectue en arrière-plan et une invite d'enregistrement du fichier s'affiche lorsque l'opération est terminée.

Information associée

Transmission de journaux d'audit vers des serveurs Syslog distants , page 123

Sujets :

Transmission de journaux d'audit vers des serveurs Syslog distants

Pour surveiller tous les journaux d'audit d'OpenManage Enterprise depuis des serveurs Syslog, créez une stratégie d'alerte. Tous les journaux d'audit, notamment les tentatives de connexion d'utilisateurs, la création de stratégies d'alerte et l'exécution de différentes tâches peuvent être transmis aux serveurs Syslog.

Pour créer une stratégie d'alerte afin de transmettre les journaux d'audit à des serveurs Syslog :

1. Sélectionnez **Alertes** > **Stratégies d'alerte** > **Créer**.
2. Dans la boîte de dialogue **Créer une stratégie d'alerte**, dans la section **Nom et description**, saisissez le nom et la description de la stratégie d'alerte.
   a. La case **Activer la stratégie** est cochée par défaut pour indiquer que la stratégie d'alerte sera activée une fois créée. Pour désactiver la stratégie d'alerte, décochez la case. Pour en savoir plus sur l'activation des stratégies d'alerte à une date ultérieure, voir la section Configuration et gestion des politiques d'alerte , page 121.
   b. Cliquez sur **Suivant**.
3. Dans la section **Catégorie**, développez l'arborescence **Application** et sélectionnez les catégories et sous-catégories des journaux de l'appliance. Cliquez sur **Suivant**.
4. Dans la section **Cible**, l'option **Sélectionner des périphériques** est sélectionnée par défaut. Cliquez sur **Sélectionner des périphériques** et sélectionnez des périphériques dans le volet de gauche. Cliquez sur **Suivant**.

   REMARQUE : Il n'est pas possible de sélectionner des périphériques ou des groupes cibles lors de la transmission des journaux d'audit au serveur Syslog.

5. (Facultatif) Par défaut, les stratégies d'alerte sont toujours actives. Pour limiter l'activité, dans la section **Date et heure**, sélectionnez les dates de début et de fin, puis sélectionnez le délai d'exécution.
   a. Cochez les cases correspondant aux jours auxquels les stratégies d'alerte doivent être exécutées.
   b. Cliquez sur **Suivant**.
6. Dans la section **Gravité**, sélectionnez le niveau de gravité des alertes pour lesquelles cette stratégie doit être activée.
   a. Pour sélectionner toutes les catégories de gravité, cochez la case **Toutes**.
   b. Cliquez sur **Suivant**.
7. Dans la section **Actions**, sélectionnez **Syslog**.

   Si les serveurs Syslog ne sont pas configurés dans OpenManage Enterprise, cliquez sur **Activer** et saisissez l'adresse IP de destination ou le nom d'hôte des serveurs Syslog. Pour en savoir plus sur la configuration des serveurs Syslog, voir la section Configuration des alertes SMTP, SNMP et Syslog , page 123.
8. Cliquez sur **Suivant**.
9. Dans la section **Résumé**, les détails de la stratégie d'alerte que vous avez définis s'affichent. Lisez attentivement les informations.
10. Cliquez sur **Terminer**.

La stratégie d'alerte a été créée avec succès et répertoriée dans la section **Stratégies d'alerte**.

Tâches associées

Configuration et gestion des politiques d'alerte , page 121
Surveillance des journaux d'audit , page 127

16

Utilisation des tâches pour le contrôle de périphériques

Une tâche est un ensemble d'instructions qui permet d'effectuer une action sur un ou plusieurs appareils. Les tâches comprennent la détection, la mise à jour de firmware, l'actualisation de l'inventaire des appareils, de la garantie, etc. Vous pouvez afficher l'état et les détails des tâches lancées sur les appareils et leurs composants sur la page **Tâches**. OpenManage Enterprise dispose de nombreuses tâches de maintenance internes qui sont déclenchées automatiquement par l'appliance selon une planification définie. Pour plus d'informations sur les tâches « par défaut » et leur planification, consultez Tâches et calendrier par défaut d'OpenManage Enterprise , page 131.

Conditions préalables :

Pour créer et gérer des tâches, notamment le clignotement, le contrôle de l'alimentation, la gestion des lignes de base du firmware ou la gestion de la ligne de base de conformité de la configuration, pour lesquelles la tâche de sélection d'appareil est impliquée :

- Vous devez disposer des privilèges utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Chaque type de tâche est limité aux appareils pour lesquels vous disposez :
  - d'autorisations d'accès,
  - de la possibilité d'effectuer l'action requise.

Pour créer et gérer des tâches, sélectionnez **OpenManage Enterprise** > **Surveillance** > **Tâches**. Vous pouvez effectuer les opérations suivantes sur la page **Tâches** :

- Afficher la liste des tâches en cours d'exécution, celles qui ont échoué et celles qui se sont achevées avec succès.
- Créer des tâches pour faire clignoter les voyants du périphérique, contrôler l'alimentation du périphérique et exécuter une commande à distance sur des périphériques. Voir Création d'une tâche de commande distante pour gérer les périphériques , page 134, Création de tâches pour la gestion des périphériques d'alimentation et Création d'une tâche pour faire clignoter les voyants des périphériques. Vous pouvez effectuer des actions similaires sur un serveur situé sur la page Détails du périphérique. Voir la section Affichage et configuration des périphériques individuels , page 68.
- Gérer des tâches telles que l'exécution, l'arrêt, l'activation, la désactivation ou la suppression de tâches.

Pour afficher d'autres informations sur une tâche, cochez la case correspondante, puis cliquez sur **Afficher les détails** dans le volet de droite. Voir Affichage des informations concernant une tâche.

Sujets :

Afficher les listes de tâches

Dans OpenManage Enterprise, cliquez sur **Surveillance** > **Tâches** pour afficher la liste des tâches existantes. Vous trouverez des informations sur les tâches dans les colonnes suivantes :

- **État de la tâche** : indique l'état d'exécution de la tâche.

  Voir Description des états de tâche et des types de tâches , page 130.

- **État** : indique l'état de la tâche. Les options possibles sont Activé ou Désactivé.
- **Nom de la tâche** : indique le nom de la tâche.
- **Type de tâche** : indique le type de la tâche.

Voir Description des états de tâche et des types de tâches , page 130.

- **Description** : description détaillée de la tâche.
- **Dernière exécution** : dernière période d'exécution de la tâche.

Vous pouvez également filtrer les tâches en saisissant ou en sélectionnant des valeurs dans la section **Filtres avancés**. Les informations supplémentaires suivantes peuvent être fournies pour filtrer les alertes :

- **Date de début de la dernière exécution** : date de début de la dernière exécution de la tâche.
- **Date de fin de la dernière exécution** : date de fin de la dernière exécution de la tâche.
- **Source** : les options possibles sont Tous, Généré par l'utilisateur (Par défaut) et Système.

Pour afficher d'autres informations sur une tâche, sélectionnez une tâche et cliquez sur **Afficher les détails** dans le volet de droite. Voir Affichage des informations d'une tâche individuelle , page 133.

OpenManage Enterprise fournit un rapport intégré qui affiche la liste des tâches planifiées. Cliquez sur **OpenManage Enterprise** > **Contrôler** > **Rapports** > **Rapport des tâches planifiées**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

REMARQUE : Sur les pages **Détection et planifications d'inventaire**, l'état d'une tâche planifiée est identifié par **En file d'attente** dans la colonne **ÉTAT**. Cependant, le même état est indiqué comme **Planifié** sur la page **Tâches**.

Description des états de tâche et des types de tâches

Tableau 21. États de tâches et description

Condition de la tâche	Description
Planifié	La tâche est planifiée pour une exécution à une date ou heure ultérieure.
En file d'attente	Les tâches en attente d'exécution.
Démarrage	
En cours d'exécution	La tâche est déclenchée en utilisant **Exécuter maintenant**
Terminé	La tâche a été exécutée.
Échec	L'exécution de la tâche a échoué.
Nouveau	La tâche est créée, mais n'est pas exécutée.
Terminé, mais avec des erreurs	L'exécution de la tâche a partiellement réussi et s'est terminée avec des erreurs.
Abandonné	L'exécution de la tâche a été suspendue par l'utilisateur.
Suspendu	L'exécution de la tâche a été arrêtée par l'utilisateur.
Arrêté	L'exécution de la tâche a été interrompue par l'utilisateur.
Annulé	
Non exécuté	La tâche est en file d'attente ou planifiée et n'a pas encore été exécutée.

Une tâche peut appartenir à l'un des types suivants :

Tableau 22. Types de tâche et description

Type de tâche	Description
Intégrité	Vérifie l'état d'intégrité des appareils. Voir la section États d'intégrité du périphérique , page 40.
Inventaire	Crée le rapport d'inventaire des appareils. Voir la section Gestion de l'inventaire des périphériques , page 74.
Configuration du périphérique	Crée une ligne de base de conformité de la configuration de l'appareil. Voir Gestion de la conformité de la configuration du périphérique , page 110.
Tâche de rapport	Crée des rapports sur les appareils à l'aide des champs de données intégrés ou personnalisés. Voir Rapports , page 139.

Tableau 22. Types de tâche et description (suite)

Type de tâche	Description
La garantie	Génère des données sur l'état de garantie des appareils. Voir Gestion de la garantie des périphériques , page 137.
Tâche d'intégration	Intègre les appareils détectés. Voir la section Intégration de périphériques , page 45.
Découverte	Détecte des appareils. Voir la section Détection de périphériques pour la surveillance ou la gestion , page 41.
Tâche d'exécution de la mise à jour de la console	La tâche de mise à niveau de la console est suivie à l'aide de cette tâche. Elle permet d'identifier si la mise à niveau est terminée ou a échoué.
Sauvegarde	
Profils du châssis	
Journaux de débogage	Collecte des journaux de débogage des tâches de surveillance des applications, des événements et de l'historique d'exécution des tâches.
Action du périphérique	Crée des actions sur les appareils, par exemple Activer la LED, Désactiver la LED, CLI IPMI, CLI RACADM, etc.
Diagnostic_Task	Téléchargement/exécution de tâches de diagnostic/TSR ou de Services (SupportAssist) liées à la tâche de diagnostic. Consultez Exécution et téléchargement des rapports de diagnostic.
Importation de définitions VLAN	Importation de définitions VLAN à partir d'Excel ou de MSM.
Fournisseur OpenID Connect	Configuration d'une connexion OpenID. Consultez Connexion à OpenManage Enterprise à l'aide des fournisseurs OpenID Connect.Connexion à OpenManage Enterprise à l'aide des fournisseurs Connect OpenID , page 159
PluginDownload_Task	La tâche PluginDownload fait l'objet d'un suivi et permet d'identifier si les téléchargements de plug-ins RPM sont terminés et prêts pour l'installation. Consultez Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles.
Post_Upgrade_Task	La tâche PostUpgrade fait l'objet d'un suivi pour définir les paramètres de l'appliance adoptés dans la version N-1 ou N-2. Elle exécute également la tâche de détection créée dans la version précédente pour s'assurer que tous les appareils sont répertoriés.
Tâche de rapport	La tâche de rapport fait l'objet d'un suivi lorsque l'utilisateur exécute le rapport (qu'il soit prédéfini ou personnalisé).
Restaurer	
Mise à jour des paramètres	La tâche de mise à jour des paramètres fait l'objet d'un suivi lorsque l'utilisateur applique un nouveau paramètre sous l'onglet Paramètres d'application.
Restauration du logiciel	La restauration fait l'objet d'un suivi lorsque l'utilisateur effectue une opération de restauration sur un appareil cible.
Mettre à jour	La tâche de mise à jour fait l'objet d'un suivi lorsque l'utilisateur effectue la mise à jour du firmware ou du pilote sur les appareils cibles.
Upgrade_Bundle_Download_Task	La tâche de téléchargement de mise à niveau groupée fait l'objet d'un suivi et permet d'identifier si le téléchargement de OMEnterprise RPM est terminé et prêt pour l'installation

Tâches et calendrier par défaut d'OpenManage Enterprise

OpenManage Enterprise dispose de nombreuses tâches de maintenance internes qui sont déclenchées automatiquement par l'appliance selon une planification définie.

Tableau 23. Le tableau suivant répertorie les noms des tâches par défaut d'OpenManage Enterprise et leur planification.

Nom de la tâche	Expression cron	Description de l'expression cron	Exemple
Inventaire de la configuration	0 0 0 1/1 * ? *	À 00:00:00, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mer 19 mai 2021 00:00:00 UTC
Tâche de mise à jour de la console par défaut	0 0 12 ? * LUN *	À 12:00:00, tous les lundis, tous les mois	• Lun 24 mai 2021 12:00:00 UTC • Lun 31 mai 2021 12:00:00 UTC
Tâche d'inventaire par défaut	0 0 5 * * ? *	À 05:00:00 tous les jours	• Mar 18 mai 2021 05:00:00 UTC • Mer 19 mai 2021 05:00:00 UTC
Tâche de purge de la configuration de l'appareil pour le nettoyage	0 0/1 * * * ? *	À la seconde : 00, toutes les minutes, à partir de la minute : 00, toutes les heures	• Lun 17 mai 2021 18:39:00 UTC • Lun 17 mai 2021 18:40:00 UTC
Tâche de purge de fichier pour l'utilisation du partage	0 0 0 1/1 * ? *	À 00:00:00, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mer 19 mai 2021 00:00:00 UTC
Tâche de purge de fichier pour les fichiers DUP uniques	0 0 0/4 1/1 * ? *	À la seconde : 00, à la minute : 00, toutes les 4 heures à partir de 00 h, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 20:00:00 UTC • Mar 18 mai 2021 00:00:00 UTC • Mar 18 mai 2021 04:00:00 UTC • Mar 18 mai 2021 04:00:00 UTC
Tâche d'intégrité globale	0 0 0/1 1/1 * ? *	À la seconde : 00, à la minute : 00, toutes les heures à partir de 00 h, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 19:00:00 UTC • Lun 17 mai 2021 20:00:00 UTC
Tâche de synchronisation interne	0 0/5 * 1/1 * ? *	À la seconde : 00, toutes les 5 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 18:45:00 UTC • Lun 17 mai 2021 18:50:00 UTC
Tâche de purge des mesures	0 0 * ? * *	À la seconde : 00 de la minute : 00 toutes les heures	• Lun 17 mai 2021 19:00:00 UTC • Lun 17 mai 2021 20:00:00 UTC • Lun 17 mai 2021 21:00:00 UTC
Tâche des mesures	0 0/15 * 1/1 * ? *	À la seconde : 00, toutes les 15 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 18:45:00 UTC • Lun 17 mai 2021 19:00:00 UTC
Tâche d'abonnement mobile	0 0/2 * 1/1 * ? *	À la seconde : 00, toutes les 2 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 18:54:00 UTC • Lun 17 mai 2021 18:56:00 UTC
Tâche de détection initialisée par le nœud	0 0/10 * 1/1 * ? *	À la seconde : 00, toutes les 10 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 19:00:00 UTC • Lun 17 mai 2021 19:10:00 UTC
Tâche de rotation du mot de passe	0 0 0/6 1/1 * ? *	À la seconde : 00, à la minute : 00, toutes les 6 heures à partir de 00 h, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mar 18 mai 2021 06:00:00 UTC • Mar 18 mai 2021 12:00:00 UTC
Enregistrement des mesures périodiques	0 0 3 * * ?	À 03:00:00 tous les jours	• Mar 18 mai 2021 03:00:00 UTC • Mer 19 mai 2021 03:00:00 UTC
Purger les tâches d'intégrité à la demande pour le tableau : Task	0 0 0/5 1/1 * ? *	À la seconde : 00, à la minute : 00, toutes les 5 heures à partir de 00 h, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mar 18 mai 2021 05:00:00 UTC • Mar 18 mai 2021 10:00:00 UTC
Tableau des tâches de purge : Event_Archive	0 0 18/12 ? * * *	À la seconde : 00, à la minute : 00, toutes les 12 heures à partir de 18 h, tous les jours	• Mar 18 mai 2021 18:00:00 UTC • Mer 19 mai 2021 18:00:00 UTC • Jeu 20 mai 2021 18:00:00 UTC

Tableau 23. Le tableau suivant répertorie les noms des tâches par défaut d'OpenManage Enterprise et leur planification. (suite)

Nom de la tâche	Expression cron	Description de l'expression cron	Exemple
Tableau des tâches de purge : Group_Audit	0 0 0 1/1 * ? *	À 00:00:00, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mer 19 mai 2021 00:00:00 UTC • Jeu 20 mai 2021 00:00:00 UTC
Tableau des tâches de purge : Task	0 0 0 1/1 * ? *	À 00:00:00, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mer 19 mai 2021 00:00:00 UTC • Jeu 20 mai 2021 00:00:00 UTC
Tableau des tâches de purge : announced_target	0 0 0 1/1 * ? *	À 00:00:00, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mer 19 mai 2021 00:00:00 UTC • Jeu 20 mai 2021 00:00:00 UTC
Purger la tâche pour le tableau : Core Application Log	0 0 0/5 1/1 * ? *	À la seconde : 00, à la minute : 00, toutes les 5 heures à partir de 00 h, tous les jours à partir du 1er, tous les mois	• Mar 18 mai 2021 00:00:00 UTC • Mar 18 mai 2021 05:00:00 UTC
Purger la tâche pour le tableau : Event	0 0/30 * 1/1 * ? *	À la seconde : 00, toutes les 30 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 19:30:00 UTC • Lun 17 mai 2021 20:00:00 UTC • Lun 17 mai 2021 20:30:00 UTC
Purger la tâche pour le tableau : Infrastructure Device	0 0/30 * 1/1 * ? *	À la seconde : 00, toutes les 30 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 19:30:00 UTC • Lun 17 mai 2021 20:00:00 UTC • Lun 17 mai 2021 20:30:00 UTC
Tâche d'interrogation d'abonnement	0 0/30 * 1/1 * ? *	À la seconde : 00, toutes les 30 minutes à partir de la minute : 00, toutes les heures, tous les jours à partir du 1er, tous les mois	• Lun 17 mai 2021 19:30:00 UTC • Lun 17 mai 2021 20:00:00 UTC • Lun 17 mai 2021 20:30:00 UTC

Affichage des informations d'une tâche individuelle

1. Sur la page **Tâches**, cochez la case correspondant à la tâche.
2. Dans le volet de droite, cliquez sur **Afficher les détails**.
   Sur la page **Détails de la tâche**, les informations sur la tâche s'affichent.
3. Cliquez sur **Redémarrer la tâche** si l'état d'une tâche est Arrêté, En échec ou Nouveau.
   Un message indique que l'exécution de la tâche a commencé.

   La section **Historique d'exécution** répertorie les informations sur les exécutions réussies de la tâche. La section **Détails d'exécution** répertorie les périphériques sur lesquels la tâche a été exécutée, ainsi que le temps nécessaire pour l'exécution.

   REMARQUE : Si une tâche de mesure corrective de la configuration est arrêtée, l'état global de la tâche est indiqué comme « Arrêté », mais la tâche continue de s'exécuter. Cependant, l'état est En cours d'exécution dans la section **Historique d'exécution**.
4. Pour exporter les données vers un fichier Excel, cochez la case correspondante ou toutes les cases, puis cliquez sur **Exporter**. Voir Exportation de toutes les données ou des données sélectionnées , page 68.

Création d'une tâche pour activer les voyants de périphérique

Les étapes suivantes expliquent comment faire clignoter les voyants des périphériques spécifiés à l'aide de l'Assistant Clignotement des périphériques.

Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16

1. L'Assistant Clignotement des périphériques peut être activé de l'une des manières suivantes :
   a. Dans la page Tâches (**OpenManage Enterprise** > **Surveiller** > **Tâches**), cliquez sur **Créer**, puis sélectionnez **Faire clignoter les périphériques**.
   b. Dans la page Tous les périphériques (**OpenManage Enterprise** > **Périphériques**), sélectionnez les périphériques, puis cliquez sur le menu déroulant **Plus d'actions**, **Activer la LED** ou **Désactiver la LED**.
2. Dans la boîte de dialogue **Assistant Clignotement des périphériques** :
   a. Dans la section **Options** :
      i. Dans la zone **Nom de tâche**, saisissez un nom de tâche.
      ii. Dans le menu déroulant **Durée du clignotement des voyants**, sélectionnez les options pour faire clignoter les voyants pendant une durée définie, pour les allumer ou pour les éteindre.
      iii. Cliquez sur **Suivant**.
   b. Dans la section **Cible**, sélectionnez les périphériques ou les groupes cible, puis cliquez sur **Suivant**. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.
   c. Dans le menu déroulant **Planifier** , sélectionnez **Exécuter maintenant**, **Exécuter plus tard** ou **Exécuter selon la planification**. Voir Définitions de champs de tâche de planification , page 180.
3. Cliquez sur **Terminer**.
   Une tâche Faire clignoter la LED est créée et répertoriée dans la page Tâches (**OpenManage Enterprise** > **Surveiller** > **Tâches**) colonne **ÉTAT DE LA TÂCHE**.

Création d'une tâche pour gérer les périphériques d'alimentation

REMARQUE : Des actions de contrôle de l'alimentation peuvent être effectuées uniquement sur les appareils qui sont détectés et gérés avec iDRAC (hors bande).

1. Cliquez sur **Créer**, puis sélectionnez **Périphériques de contrôle de l'alimentation**.
2. Dans la boîte de dialogue **Assistant Périphériques de contrôle de l'alimentation** :
   a. Dans la section **Options** :
      i. Saisissez le nom de tâche dans **Nom de tâche**.
      ii. Dans le menu déroulant **Options d'alimentation**, sélectionnez l'une des tâches : **Mettre sous tension**, **Mettre hors tension** ou **Cycle d'alimentation**.
      iii. Cliquez sur **Suivant**.
   b. Dans la section **Cible**, sélectionnez les périphériques cible, puis cliquez sur **Suivant**. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.
   c. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
3. Cliquez sur **Terminer**.
   La tâche est créée et répertoriée dans la liste des tâches et identifiée par un état approprié dans la colonne **ÉTAT DE LA TÂCHE**.
4. Si la tâche est planifiée pour plus tard, mais que vous voulez l'exécuter immédiatement :
   - Sur la page Tâches, cochez la case correspondant à la tâche planifiée.
   - Cliquez sur **Exécuter maintenant**. La tâche est exécutée et l'état est mis à jour.
   - Pour afficher les données de la tâche, cliquez sur **Afficher les détails** dans le volet de droite. Voir Affichage des informations d'une tâche individuelle , page 133.

Création d'une tâche de commande distante pour gérer les périphériques

À l'aide de l'Assistant Tâche de ligne de commande, vous pouvez créer des tâches de commande distante pour gérer les périphériques cibles à distance.

1. Cliquez sur **Créer**, puis sélectionnez **Commande distante sur les périphériques**.
2. Dans la boîte de dialogue **Assistant Tâche de ligne de commande**, dans la section **Options** :
   a. Saisissez le nom de tâche dans **Nom de tâche**.

b. Dans le menu déroulant Interface, sélectionnez l'une des interfaces en fonction des périphériques cibles que vous souhaitez gérer :
   - **CLI IPMI** : pour les serveurs iDRAC et les serveurs autres que Dell.
   - **CLI RACADM** : pour les iDRAC détectés à l'aide du protocole WSMAN.
   - **SSH CLI** : pour les serveurs Linux détectés à l'aide du protocole SSH.

c. Dans le champ **Arguments**, saisissez la commande. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.

   REMARQUE : Les commandes de la zone Arguments sont exécutées une à la fois.

d. Cliquez sur **Suivant**.
   Une coche verte située en regard d'**Options** signifie que les données nécessaires sont fournies.

3. Dans la section **Cible**, sélectionnez les périphériques cible, puis cliquez sur **Suivant**. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.
4. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
5. Cliquez sur **Terminer**.
   La tâche est créée et répertoriée dans la liste des tâches et identifiée par un état approprié dans la colonne **ÉTAT DE LA TÂCHE**.
6. Si la tâche est planifiée pour plus tard, mais que vous voulez l'exécuter immédiatement :
   - Sur la page Tâches, cochez la case correspondant à la tâche planifiée.
   - Cliquez sur **Exécuter maintenant**. La tâche est exécutée et l'état est mis à jour.
   - Pour afficher les données de la tâche, cliquez sur **Afficher les détails** dans le volet de droite. Voir Affichage des informations d'une tâche individuelle , page 133.

Création d'une tâche pour modifier le type de plug-in de la console virtuelle

Vous pouvez modifier le type de plug-in de la console virtuelle pour le définir sur HTML5 pour plusieurs appareils. La mise à jour vers HTML5 peut fournir une meilleure expérience de navigation. Pour effectuer la mise à jour, procédez comme suit :

1. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Tâches**
2. Cliquez sur **Créer**, puis sélectionnez **Modifier le plug-in de la console virtuelle sur des périphériques**.
3. Dans la boîte de dialogue **Assistant Modifier le plug-in de console virtuelle**, dans la section **Options** :
   a. Saisissez le nom de tâche dans **Nom de tâche**. Par défaut, le type de plug-in affiche HTML5.
   b. Cliquez sur **Suivant**.
4. Dans la section **Tâche cible**, sélectionnez les périphériques cibles et cliquez sur **Suivant**. Voir Sélection de périphériques et de groupes de périphériques cibles , page 135.
   a. Cliquez sur **Suivant**.
5. Dans la section **Planification**, exécutez la tâche immédiatement ou planifiez-la pour plus tard. Voir Définitions de champs de tâche de planification , page 180.
6. Cliquez sur **Terminer**.
   La tâche est créée et répertoriée dans la liste des tâches et identifiée par un état approprié dans la colonne **ÉTAT DE LA TÂCHE**.
7. Si la tâche est planifiée pour plus tard, mais que vous voulez l'exécuter immédiatement :
   - Sur la page Tâches, cochez la case correspondant à la tâche planifiée.
   - Cliquez sur **Exécuter maintenant**. La tâche est exécutée et l'état est mis à jour.
   - Pour afficher les données de la tâche, cliquez sur **Afficher les détails** dans le volet de droite. Voir Affichage des informations d'une tâche individuelle , page 133.

Sélection de périphériques et de groupes de périphériques cibles

Par défaut, **Sélectionner des périphériques** est sélectionné pour indiquer que la tâche peut être exécutée sur les périphériques. Vous pouvez également exécuter une tâche sur des groupes de périphériques en sélectionnant **Sélectionner des groupes**.

REMARQUE : Les groupes de périphériques et les périphériques affichés sont régis par l'accès opérationnel basé sur le périmètre dont l'utilisateur dispose pour les périphériques. Pour plus d'informations, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Cliquez sur **Sélectionner des périphériques**.

   Dans la boîte de dialogue **Tâche cible**, le volet de gauche répertorie les périphériques surveillés par OpenManage Enterprise. Dans le volet en cours, la liste des périphériques associés à chaque groupe et les détails des périphériques s'affichent. Pour obtenir la description des champs, voir Liste des périphériques , page 62. Pour en savoir plus sur les groupes de périphériques, voir Organisation des périphériques dans des groupes , page 55.
2. Cochez la case correspondant à un périphérique et cliquez sur **OK**.
   Les périphériques sélectionnés s'affichent dans la section **Tous les périphériques sélectionnés** du groupe sélectionné.

Gestion des tâches

Une fois que des tâches ont été créées et s'affichent sur la page **Tâches**, vous pouvez les gérer comme suit.

- **Exécuter des tâches** : cochez la case correspondant à une tâche, puis cliquez sur **Exécuter maintenant** pour exécuter la tâche sur les appareils cibles. Vous pouvez exécuter une tâche quand elle est à l'état Activé.
- **Activer des tâches** : cochez la case correspondant à une tâche, puis cliquez sur **Activer**.
- **Désactiver des tâches** : cochez la case correspondant à une tâche, puis cliquez sur **Désactiver**.
  REMARQUE : Vous ne pouvez désactiver que les tâches planifiées. Vous ne pouvez pas désactiver les tâches actives et à l'État « En cours d'exécution ».
- **Arrêter des tâches** : cochez la case correspondant à une tâche, puis cliquez sur **Arrêter**. Vous pouvez arrêter une tâche quand elle est en cours d'exécution.
- **Supprimer** : cochez la case correspondant à une tâche, puis cliquez sur **Supprimer**.

17

Gestion de la garantie des périphériques

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

En cliquant sur **OpenManage Enterprise** > **Surveiller** > **Garantie**, vous pouvez afficher les états de garantie de tous les appareils surveillés par OpenManage Enterprise qui sont dans votre périmètre. Par exemple, un administrateur disposant d'un accès à tous les groupes de périphériques affichera les informations de garantie de tous les périphériques, mais les gestionnaires de périphériques ne verront que celles des périphériques qui se trouvent dans leur périmètre.

Vous pouvez également exporter les données sélectionnées ou toutes les données vers une feuille Excel à des fins statistiques et d'analyse. La page Garantie affiche les détails suivants :

- **ÉTAT** de la garantie
  REMARQUE : L'état de la garantie est déterminé par les paramètres sélectionnés par l'administrateur. Voir Gestion des paramètres de garantie , page 168
  -  correspond à un état **Critique**, ce qui signifie que la garantie a expiré.
  -  correspond à un état **Avertissement**, ce qui signifie que la garantie expire bientôt.
  -  correspond à un état **Normal**, ce qui signifie que la garantie est active.
- **NUMÉRO DE SÉRIE**
- **MODÈLE D'APPAREIL**
- **TYPE DE PÉRIPHÉRIQUE**
- **TYPE DE GARANTIE** :
  - Initiale : garantie fournie lors de l'achat d'OpenManage Enterprise.
  - Étendue : garantie étendue suite à l'expiration de la période de garantie initiale.
- **DESCRIPTION DU NIVEAU DE SERVICE** : indique le contrat de niveau de service (SLA) associé à la garantie du périphérique.
- **JOURS RESTANTS** : nombre de jours avant l'expiration de la garantie. Vous pouvez définir les jours limites pour recevoir une alerte. Voir Gestion des paramètres de garantie , page 168.

OpenManage Enterprise fournit un rapport intégré concernant les garanties qui doivent expirer dans les 30 prochains jours. Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Rapports** > **Garanties expirant dans les 30 prochains jours**. Cliquez sur **Exécuter**. Voir Exécution des rapports , page 140.

Pour filtrer des données du tableau, cliquez sur **Filtres avancés**. Voir la section consacrée aux filtres avancés dans Présentation de l'interface graphique d'OpenManage Enterprise–Tech Release , page 36.

L'état de la garantie de tous les périphériques découverts est collecté automatiquement une fois par semaine par une tâche de garantie intégrée. Vous pouvez également lancer manuellement la tâche de garantie en cliquant sur **Actualiser la garantie** dans l'angle supérieur droit.

Pour exporter toutes les données de garantie ou les données sélectionnées, cliquez sur **Exporter**. Voir Exportation de toutes les données ou des données sélectionnées , page 68.

Tâches associées

Affichage et renouvellement de la garantie des appareils , page 138

Sujets :

Affichage et renouvellement de la garantie des appareils

Cliquez sur **OpenManage Enterprise** > **Surveiller** > **Garantie** pour obtenir la liste des états de garantie de tous les appareils surveillés par OpenManage Enterprise, ainsi que leur numéro de série, leur nom de modèle, leur type, leur garantie associée et les informations relatives au niveau de service. Pour obtenir la description des champs, voir Gestion de la garantie des périphériques , page 137.

Pour afficher les informations relatives à la garantie d'un appareil et renouveler celle-ci :

- Cochez la case correspondant au périphérique. Dans le volet de droite, l'état de la garantie et d'autres informations importantes concernant l'appareil, comme le code de niveau de service, le prestataire de services, la date de début de garantie, la date de fin de garantie, etc. s'affichent.
- Il est possible de renouveler les garanties expirées en cliquant sur **Renouvellement de la garantie Dell pour l'appareil**, ce qui vous redirige vers le site de support Dell EMC sur lequel vous pouvez gérer la garantie de votre appareil.
- Cliquez sur **Actualiser la garantie** dans l'angle supérieur droit pour actualiser le tableau de garantie. Les états de garantie passent automatiquement de Critique  à Normal  pour tous les appareils dont les garanties sont renouvelées. Un nouveau journal des alertes de Garantie de l'appareil, contenant le nombre total de garanties expirées dans la console, est généré chaque fois qu'un clic est effectué sur **Actualiser la garantie**. Pour plus d'informations sur les journaux d'alerte, consultez Affichage des journaux d'alertes.
- Pour trier les données du tableau par colonne, cliquez sur le titre de la colonne.
- Cliquez sur le bouton **Filtres avancés** pour personnaliser.

Information associée

Gestion de la garantie des périphériques , page 137

18

Rapports

En cliquant sur le menu **OpenManage Enterprise** > **Contrôler** > **Rapports**, vous pouvez générer des rapports personnalisés pour afficher tous les détails de périphérique. Les rapports vous permettent d'afficher les données concernant les périphériques, les tâches, les alertes et d'autres éléments de votre datacenter. Ces rapports sont intégrés et définis par l'utilisateur. Vous pouvez modifier ou supprimer uniquement les rapports définis par l'utilisateur. Les définitions et les critères utilisés pour un rapport intégré ne peuvent pas être modifiés ou supprimés. Un aperçu du rapport sélectionné dans la liste des rapports s'affiche dans le volet de droite.

Les rapports et les données affichés sur la page Rapports dépendent des privilèges d'utilisateur basés sur le périmètre dont vous disposez dans OpenManage Enterprise. Par exemple, les gestionnaires de périphériques ont accès uniquement aux rapports qu'ils ont créés en plus des rapports intégrés. En outre, le rapport généré par un utilisateur contient les données des périphériques qui se trouvent dans le périmètre de cet utilisateur. Par exemple, les rapports générés par les gestionnaires de périphériques administrateur et « non restreints » contiennent des données sur tous les groupes de périphériques. Toutefois, les rapports générés par les gestionnaires de périphériques dont le périmètre est restreint possèderaient des données concernant uniquement les périphériques et/ou les groupes de périphériques qui se trouvent dans leur périmètre.

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Tableau 24. Privilèges d'accès basés sur le rôle pour la gestion des rapports dans OpenManage Enterprise

Rôle utilisateur...	Tâches de rapport autorisées...
Administrateurs et gestionnaires de périphériques	Exécuter, créer, modifier, copier, envoyer par e-mail, télécharger et exporter
Observateurs	Exécuter, envoyer par e-mail, exporter, afficher et télécharger

Avantages de la fonction Rapports :

- Créez des critères de rapport en utilisant jusqu'à 20 filtres
- Vous pouvez filtrer les données en fonction des noms de colonne de votre choix
- Les rapports peuvent être affichés, téléchargés et envoyés par courrier électronique
- Envoyez les rapports à un maximum de 20 à 30 destinataires simultanément
- Si vous estimez que la génération de rapports prend beaucoup de temps, vous pouvez arrêter le processus
- Les rapports générés sont automatiquement traduits dans la langue définie à l'installation d'OpenManage Enterprise.
- Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport

Actuellement, les rapports intégrés suivants peuvent être générés pour extraire des informations sur les points suivants :

- Catégorie de périphériques : actif, FRU, firmware, conformité du firmware/pilote, tâches planifiées, résumé des alertes, disque dur, boîtier modulaire, carte NIC, disque virtuel, garantie et licence.
- Catégorie des alertes : alertes hebdomadaires

Tâches associées

Exécution des rapports , page 140
Exécution et envoi de rapports par e-mail , page 140
Modifier des rapports , page 141
Supprimer des rapports , page 141

Sujets :

- Supprimer des rapports
- Création de rapports
- Exportation des rapports sélectionnés

Exécution des rapports

Dans la page Rapports (**OpenManage Enterprise** > **Surveiller** > **Rapports**), vous pouvez exécuter, afficher et télécharger les rapports intégrés ou les rapports que vous avez créés.

Lorsque vous exécutez un rapport, les 20 premières lignes sont affichées et les résultats peuvent être paginés. Pour afficher toutes les lignes en même temps, téléchargez le rapport. Pour modifier cette valeur, voir Exportation de toutes les données ou des données sélectionnées , page 68. Les données affichées dans les résultats ne peuvent pas être triées, car elles sont définies dans la requête utilisée pour créer un rapport. Pour trier les données, modifiez la requête du rapport ou exportez-les au format Excel. Il est conseillé de ne pas exécuter plus de cinq (5) rapports à la fois, car la création de rapports consomme des ressources système. Ce nombre dépend néanmoins des périphériques détectés, des champs utilisés et du nombre de tableaux joints pour générer le rapport. Une tâche Rapports est créée et exécutée à la demande de génération d'un rapport. Pour plus d'informations sur les privilèges basés sur des rôles pour générer des rapports, voir Création de rapports , page 142.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les rapports générés par les gestionnaires de périphériques n'auront que des données relatives aux périphériques qui sont dans leur périmètre.
- Il est déconseillé d'exécuter fréquemment un rapport, car cela consomme des ressources de traitement et de données.
- Pour un rapport dont la catégorie est « Périphérique », les premières colonnes sont par défaut : Nom du périphérique, Modèle du périphérique et Numéro de série du périphérique. Vous pouvez exclure certaines colonnes pendant la personnalisation de votre rapport.

Pour exécuter un rapport, sélectionnez le rapport et cliquez sur **Exécuter**. Sur la page **Rapports <nom du rapport>**, le rapport s'affiche sous forme de tableau avec les champs définis pour la création du rapport.

Pour télécharger un rapport :

1. Cliquez sur **Télécharger**.
2. Dans la boîte de dialogue **Télécharger le rapport**, sélectionnez le type de fichier de sortie, puis cliquez sur **Terminer**. Le fichier de sortie sélectionné s'affiche. Vous pouvez actuellement exporter un rapport aux formats de fichier XML, PDF, Excel, CSV. Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport.

Pour envoyer un rapport par e-mail :

1. Cliquez sur **Envoyer par e-mail**.
2. Dans la boîte de dialogue **Envoyer le rapport par e-mail**, sélectionnez le format de fichier, saisissez l'adresse e-mail du destinataire, puis cliquez sur **Terminer**. Le rapport est envoyé par e-mail. Vous pouvez envoyer les rapports par e-mail à 20 ou 30 destinataires à la fois.
3. Si l'adresse e-mail n'est pas configurée, cliquez sur **Accéder aux Paramètres SMTP**. Pour plus d'informations sur la configuration des propriétés SMTP, voir Définition des informations d'identification SNMP , page 167.

REMARQUE : Si un autre utilisateur essaie de supprimer le rapport déjà généré que vous êtes en train de télécharger ou d'exécuter, les deux tâches sont achevées avec succès.

Information associée

Rapports , page 139

Exécution et envoi de rapports par e-mail

Vous pouvez exécuter le rapport et l'envoyer par e-mail à entre 20 et 30 destinataires à la fois.

REMARQUE : L'opération d'envoi d'e-mail peut échouer avec de nombreux rapports, si la taille du message dépasse la taille de message fixe définie sur le serveur SMTP. Dans ces cas, envisagez de réinitialiser la limite de taille des messages du serveur SMTP, puis réessayez.

1. Sélectionnez le rapport et cliquez sur **Exécuter et envoyer par e-mail**.
2. Dans la boîte dialogue **Envoyer le rapport par e-mail** :
   a. Dans le menu déroulant **Format**, sélectionnez l'un des formats de fichier dans lequel le rapport doit être généré : HTML, CSV, PDF ou MS-Excel.
   b. Dans la zone **À**, entrez l'adresse e-mail du destinataire. Si l'adresse e-mail n'est pas configurée, cliquez sur **Accéder aux Paramètres SMTP**. Pour plus d'informations sur la configuration des propriétés SMTP, voir Définition des informations d'identification SNMP , page 167.
   c. Cliquez sur **Terminer**.
   Le rapport est envoyé par e-mail et enregistré dans les journaux d'audit.

Information associée

Rapports , page 139

Modifier des rapports

Seuls les rapports créés par l'utilisateur peuvent être modifiés.

1. Sélectionnez le rapport, puis cliquez sur **Modifier**.
2. Dans la boîte de dialogue **Définition de rapport**, modifiez les paramètres. Voir la rubrique Création de rapports.
3. Cliquez sur **Enregistrer**.
   Les informations mises à jour sont enregistrées. Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport.
   REMARQUE : Lors de la modification d'un rapport personnalisé, si la catégorie est modifiée, les champs associés sont également supprimés.

Information associée

Rapports , page 139

Copie de rapports

Seuls les rapports créés par l'utilisateur peuvent être copiés.

1. Sélectionnez le rapport, cliquez sur **Plus d'actions**, puis cliquez sur **Copier**.
2. Dans la boîte de dialogue **Copier la définition de rapport**, entrez un nouveau nom pour le rapport copié.
3. Cliquez sur **Enregistrer**.
   Les informations mises à jour sont enregistrées. Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport.

Supprimer des rapports

Seuls les rapports créés par l'utilisateur peuvent être supprimés. Si une définition de rapport est supprimée, l'historique de rapports associé est supprimé et toute exécution de rapport à l'aide de cette définition de rapport est également interrompue.

1. Dans le menu **OpenManage Enterprise**, dans la section **Surveiller**, sélectionnez **Rapports**.
   Une liste des rapports disponibles de périphériques s'affiche.
2. Sélectionnez le rapport, cliquez sur **Plus d'actions**, puis cliquez sur **Supprimer**.
   REMARQUE : Si un autre utilisateur essaie de supprimer le rapport déjà généré que vous êtes en train de télécharger ou d'exécuter, les deux tâches sont achevées avec succès.
3. Dans la boîte de dialogue **Supprimer la définition de rapport**, lorsque vous êtes invité à indiquer si le rapport doit être supprimé ou non, cliquez sur **Oui**.

Le rapport est supprimé de la liste des rapports et le tableau est mis à jour. Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport.

Information associée

Rapports , page 139

Création de rapports

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Les rapports générés par les gestionnaires de périphériques n'auront que des données relatives aux groupes de périphériques qui sont dans leur périmètre.
- Certains tableaux contiennent des données spécifiques aux types d'appareils ce qui aura pour effet de verrouiller le rapport pour le type d'appareil donné. Le fait de combiner les colonnes spécifiques à l'appareil à partir de plusieurs tableaux de différents types (par exemple les serveurs et les châssis) se traduit par un rapport non valide sans résultat.

Bien que les rapports aient des définitions par défaut (critères de filtre) pour générer des rapports, vous pouvez personnaliser les critères pour créer vos propres définitions, puis générer des rapports personnalisés. Les champs ou colonnes que vous souhaitez afficher dans votre rapport dépendent de la catégorie que vous sélectionnez. Vous ne pouvez sélectionner qu'une seule catégorie à la fois. La disposition des colonnes dans un rapport peut être modifiée par une opération de glisser-déplacer. Également :

- Les noms des rapports doivent être uniques
- La définition du rapport doit avoir au moins un champ et une catégorie
- Pour les rapports ayant les catégories Périphérique et Alerte, l'un des champs obligatoires doit correspondre au nom du périphérique ou au groupe de périphériques

Par défaut, **Périphériques** est sélectionné en tant que catégorie et le nom du périphérique, le numéro de série du périphérique ainsi que les colonnes du modèle du périphérique s'affichent dans le volet en cours. Si vous choisissez une autre catégorie lors de la modification des critères du rapport, un message s'affiche indiquant que les champs par défaut seront supprimés. Chaque catégorie a des propriétés prédéfinies qui peuvent être utilisées en tant que titres de colonne où les données sont filtrées en utilisant les critères que vous définissez. Exemple de types de catégorie :

- Tâches : nom de la tâche, type de tâche, état de la tâche et tâche interne.
- Groupes : état du groupe, description du groupe, type d'appartenance au groupe, nom du groupe et type de groupe.
- Alertes : état de l'alerte, gravité de l'alerte, nom du catalogue, type d'alerte, sous-catégorie d'alerte et informations relatives au périphérique.
- Périphériques : alerte, catalogue d'alertes, ventilateur du châssis, logiciel de périphérique, et ainsi de suite. Ces critères ont une classification supplémentaire reposant sur les données qui peuvent être filtrées et les rapports qui peuvent être générés.

Tableau 25. Privilèges d'accès basés sur des rôles pour générer des rapports OpenManage Enterprise

Rôle utilisateur...	Tâches de rapport autorisées...
Administrateurs et gestionnaires de périphériques	Exécuter, créer, modifier, copier, envoyer par e-mail, télécharger et exporter
Observateurs	Exécuter, envoyer par e-mail, exporter, afficher et télécharger

1. Cliquez sur **Rapports** > **Créer**.
2. Dans la boîte dialogue **Définition de rapport** :
   a. Saisissez le nom et la description du nouveau rapport à définir.
   b. Cliquez sur **Suivant**.
3. Dans la section **Générateur de rapports** :
   a. Dans le menu déroulant **Catégorie**, sélectionnez la catégorie Rapport.
      - Si vous sélectionnez Périphérique en tant que catégorie, sélectionnez le groupe de périphériques également.
      - Si nécessaire, modifiez les critères de filtre. Voir la section Sélection d'un critère de requête , page 58.

b. Dans la section **Sélectionner les colonnes**, cochez les cases des champs qui doivent s'afficher en tant que colonnes des rapports.
Le nom des champs sélectionnés s'affiche dans la section **Ordre des colonnes**.

c. Vous pouvez personnaliser le rapport en :
   - Utilisant les cases **Trier par** et **Direction**.
   - Faisant glisser les champs vers le haut ou le bas dans la section **Ordre des colonnes**.

4. Cliquez sur **Terminer**.
Le rapport est généré et répertorié dans la liste de rapports. Vous pouvez exporter le rapport à des fins d'analyse. Voir la section Exportation de toutes les données ou des données sélectionnées , page 68. Une entrée de journal d'audit est créée à chaque fois que vous générez, modifiez, supprimez ou copiez une définition de rapport.

Sélection des critères de requête lors de la création de rapports

Définissez des filtres lorsque vous créez des critères de requête pour :

- Générer des rapports personnalisés. Voir Création de rapports , page 142.
- Créer des groupes de périphériques basés sur des requêtes sous GROUPES PERSONNALISÉS. Voir Création d'un groupe de périphériques de requête , page 58.

Pour définir un critère de requête, utilisez deux options :

- **Sélectionner une requête existante à copier** : par défaut, OpenManage Enterprise intègre une liste de modèles de requête que vous pouvez copier pour créer votre propre critère de requête. Vous pouvez utiliser au maximum 20 critères (filtres) lors de la définition d'une requête. Pour ajouter des filtres, sélectionnez des éléments dans le menu déroulant **Sélectionner un type**.
- **Sélectionner un type** : pour créer un critère de requête, utilisez les attributs répertoriés dans ce menu déroulant. Les éléments présents dans le menu dépendent des périphériques surveillés par OpenManage Enterprise. Lorsqu'un type de requête est sélectionné, seuls les opérateurs appropriés s'affichent, tels que =, >, < et null, en fonction du type de requête. Cette méthode est recommandée pour la définition des critères de requête lors de la création de rapports personnalisés.

  REMARQUE : Lorsque vous évaluez une requête avec plusieurs conditions, l'ordre d'évaluation est identique à celui de SQL. Pour spécifier un ordre particulier pour l'évaluation des conditions, ajoutez ou supprimez des parenthèses lors de la définition la requête.

REMARQUE : Une fois sélectionnés, les filtres d'un critère de requête existant sont uniquement copiés virtuellement pour créer un nouveau critère de requête. Les filtres par défaut associés à un critère de requête existant ne sont pas modifiés. Les filtres définis d'un critère de requête intégré sont utilisés comme point de départ pour la construction d'un critère de requête personnalisé. Par exemple :

1. *Requête1* est un critère de requête intégré composé du filtre prédéfini suivant : `Task Enabled=Yes`.
2. Pour copier les propriétés du filtre de *Requête1*, créer *Requête2*, puis personnaliser le critère de requête, ajoutez un autre filtre : `Task Enabled=Yes` ET `(Task Type=Discovery)`.
3. Ensuite, ouvrez *Requête1*. Son critère de filtre reste `Task Enabled=Yes`.

1. Dans la boîte de dialogue **Sélection de critères de requête**, sélectionnez des éléments du menu déroulant selon que vous souhaitez créer un critère de requête pour générer des groupes de requêtes ou des rapports.
2. Pour ajouter ou supprimer un filtre, cliquez respectivement sur le symbole plus ou sur la corbeille.
3. Cliquez sur **Terminer**.
Un critère de requête est généré et sauvegardé dans la liste des requêtes existantes. Une entrée est créée dans le journal d'audit et s'affiche dans la liste des journaux d'audit. Voir Surveillance des journaux d'audit , page 127.

Exportation des rapports sélectionnés

1. Cochez les cases correspondant aux rapports à exporter, cliquez sur **Plus d'actions**, puis sur **Exporter les rapports sélectionnés**.
Actuellement, vous ne pouvez pas exporter tous les rapports à la fois.
2. Dans la boîte de dialogue **Exporter les rapports sélectionnés**, sélectionnez l'un des formats de fichier suivants dans lequel le rapport doit être exporté : HTML, CSV ou PDF.
3. Cliquez sur **Terminer**.
Dans la boîte de dialogue, ouvrez ou enregistrez le fichier dans un emplacement connu à des fins d'analyse et statistiques.

19

Gestion des fichiers MIB

REMARQUE : Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Il est possible que les outils tiers présents dans votre datacenter puissent générer des alertes qui sont essentielles pour vos opérations. Ces alertes sont stockées dans les fichiers MIB (Management Information Base) qui sont définis et utilisés par différents outils de fabricants. Cependant, OpenManage Enterprise vous permet également de gérer ces fichiers de telle sorte que les fichiers MIB non issus de Dell EMC puissent être importés, analysés et utilisés par OpenManage Enterprise pour gérer les périphériques. OpenManage Enterprise prend en charge SMI1 et SMI2. OpenManage Enterprise fournit des fichiers MIB intégrés qui peuvent être utilisés pour les périphériques Dell EMC. Ces fichiers MIB sont en lecture seule et ne peuvent pas être modifiés.

REMARQUE : Seuls les MIB valides dotés d'interruptions sont traités par OpenManage Enterprise.

Les MIB sont gérées :

- Importation de fichiers MIB , page 144
- Suppression de fichiers MIB , page 146
- Résolution des types de MIB , page 146

En cliquant sur **OpenManage Enterprise** > **Contrôler** > **MIB**, vous pouvez gérer les fichiers MIB utilisés par OpenManage Enterprise et d'autres outils de gestion des systèmes dans le datacenter. Un tableau répertorie les fichiers MIB disponibles avec les propriétés suivantes. Cliquez sur l'en-tête de colonne pour trier les données.

Tableau 26. Accès basés sur des rôles pour les fichiers MIB dans OpenManage Enterprise

Fonctionnalités d'OpenManage Enterprise	Contrôle d'accès basé sur les rôles des fichiers MIB		
	Admin	Gestionnaire de périphériques	Observateur
Afficher les interruptions ou les MIB	O	O	O
Importer une MIB. Modifier les interruptions.	O	N	N
Supprimer MIB	O	N	N
Modifier les interruptions	O	N	N

Pour télécharger les fichiers MIB intégrés d'OpenManage Enterprise, cliquez sur **Télécharger MIB**. Les fichiers sont enregistrés dans le dossier qui a été indiqué.

Sujets :

Importation de fichiers MIB

Flux de processus idéal d'importation MIB : **l'utilisateur charge un fichier MIB dans OpenManage Enterprise** > **OpenManage Enterprise analyse le fichier MIB** > **OpenManage Enterprise recherche des interruptions similaires déjà disponibles dans la base de données** > **OpenManage Enterprise affiche les données de fichiers MIB**. La taille maximale du

fichier MIB importable est de 3 Mo. L'historique du journal d'audit OpenManage Enterprise enregistre chaque importation et suppression de fichiers MIB.

REMARQUE :

- Pour effectuer des tâches sur OpenManage Enterprise, vous devez disposer des privilèges utilisateur basés sur les rôles et de l'accès opérationnel basé sur le périmètre pour les périphériques. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16
- Un seul fichier MIB peut être importé à la fois.

1. Cliquez sur **MIB** > **Importer des fichiers MIB**.
2. Dans la boîte de dialogue **Importer des fichiers MIB**, dans la section **Charger des fichiers MIB**, cliquez sur **Choisir un fichier** pour sélectionner un fichier MIB.

   Si des instructions d'importation de MIB sont résolues par des MIB externes, un message s'affiche.

   a. Cliquez sur **Résoudre les types**. Résolvez les types de MIB. Voir Suppression de fichiers MIB , page 146.
   b. Cliquez sur **Terminer**. Si Dell EMC est propriétaire du fichier MIB, un message indique que le MIB est fourni avec le produit et ne peut pas être modifié.
3. Cliquez sur **Suivant**.
4. Dans la section **Afficher les interruptions**, une liste de fichiers MIB s'affiche avec les informations suivantes :
   - Catégorie d'alerte de l'interruption. Vous pouvez modifier la catégorie afin de l'aligner sur les définitions de catégorie OpenManage Enterprise. Voir Modification des interruptions MIB , page 145.
   - Le nom de l'interruption est en lecture seule. Défini par le périphérique tiers.
   - Niveaux de gravité d'une alerte : Critique, Avertissement, Information et Normal.
   - Message d'alerte associé à une alerte.
   - L'OID d'interruption est en lecture seule et unique.
   - « Nouveau » indique que l'interruption est importée pour la première fois par OpenManage Enterprise. Les interruptions déjà importées sont indiquées comme « Importé ». « Remplacer » indique les interruptions dont la définition est réécrite en raison d'une opération d'importation.

   Pour modifier les catégories d'alerte par défaut ou le niveau de gravité d'un fichier MIB, voir Modification des interruptions MIB , page 145. Pour supprimer des fichiers MIB, cochez les cases correspondantes, puis cliquez sur **Supprimer l'interruption**. Les fichiers MIB sont supprimés et la liste de fichiers MIB est mise à jour.
5. Cliquez sur **Terminer**. Les fichiers MIB sont analysés, importés dans OpenManage Enterprise, puis répertoriés sous l'onglet **MIN**.

REMARQUE : Si vous importez un fichier MIB, puis l'importez à nouveau, l'état MIB affiche **IMPORTÉ**. Toutefois, si vous réimportez un fichier MIB supprimé, l'état d'interruption indique **NOUVEAU**.

REMARQUE : Les interruptions déjà importées dans OpenManage Enterprise ne peuvent pas être importées.

REMARQUE : Les fichiers MIB fournis par défaut avec OpenManage Enterprise ne sont pas importables.

REMARQUE : Les événements générés après l'importation de l'interruption sont formatés et affichés en fonction de la nouvelle définition.

Modification des interruptions MIB

1. Sélectionnez le rapport, puis cliquez sur **Modifier**.
2. Dans la boîte de dialogue **Modifier les interruptions MIB** :
   a. Sélectionnez ou saisissez des données dans les champs :
      - Sélectionnez la nouvelle catégorie d'alerte à affecter à l'alerte. Par défaut, OpenManage Enterprise affiche quelques catégories d'alerte intégrées.
      - Saisissez le composant d'alerte.
      - Le nom de l'interruption est en lecture seule, car il est généré par l'outil tiers.
      - Sélectionnez le niveau de gravité à affecter à l'alerte. Par défaut, OpenManage Enterprise affiche quelques catégories d'alerte intégrées.
      - Un message qui décrit l'alerte.
   b. Cliquez sur **Terminer**.

L'interruption est modifiée et la liste d'interruptions mise à jour s'affiche.

REMARQUE : Vous ne pouvez pas modifier plus d'une alerte à la fois. Les interruptions importées dans OpenManage Enterprise ne peuvent pas être modifiées.

3. Dans la boîte de dialogue **Définition de rapport**, modifiez les paramètres. Voir la rubrique Création de rapports.
4. Cliquez sur **Enregistrer**.
   Les informations mises à jour sont enregistrées.

Suppression de fichiers MIB

REMARQUE : Vous ne pouvez pas supprimer un fichier MIB qui a des définitions d'interruption utilisées par l'une des stratégies d'alerte. Voir Stratégies d'alerte , page 120.

REMARQUE : Les événements reçus avant la suppression d'un fichier MIB ne sont pas affectés par cette dernière. Mais les événements générés après la suppression auront des interruptions non formatées.

1. Dans la colonne **NOM DE FICHIER MIB**, développez le dossier, puis sélectionnez les fichiers MIB.
2. Cliquez sur **Supprimer MIB**.
3. Dans la boîte de dialogue **Supprimer MIB**, cochez les cases des MIB à supprimer.
4. Cliquez sur **Supprimer**.
   Les fichiers MIB sont supprimés et le tableau MIB est mis à jour.

Résolution des types de MIB

1. Importez les fichiers MIB. Voir Importation de fichiers MIB , page 144.
   Si le type de fichier MIB n'est pas résolu, la boîte de dialogue **Types non résolus** répertorie les types de fichier MIB non résolus, indiquant que les types de fichier MIB seront importés uniquement s'ils sont résolus.
2. Cliquez sur **Résoudre les types**.
3. Dans la boîte de dialogue **Résoudre les types**, cliquez sur **Sélectionner des fichiers**, puis sélectionnez les fichiers manquants.
4. Dans la boîte de dialogue **Importer des fichiers MIB**, cliquez sur **Suivant**. S'il reste des types de fichier MIB manquants, la boîte de dialogue **Types non résolus** répertorie à nouveau les types de fichier MIB manquants. Répétez les étapes 1 à 3.
5. Une fois tous les types de fichier MIB non résolus sont résolus, cliquez sur **Terminer**. Terminez le processus d'importation. Voir Importation de fichiers MIB , page 144.

Téléchargement d'un fichier MIB OpenManage Enterprise

1. Sur la page **Surveiller**, cliquez sur **MIB**.
2. Développez et sélectionnez un fichier MIB OpenManage Enterprise, puis cliquez sur **Télécharger MIB**.

   REMARQUE : Vous pouvez télécharger uniquement les fichiers MIB associés à OpenManage Enterprise.

20

Gestion des paramètres de l'appliance OpenManage Enterprise

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : Pour plus d'informations sur les navigateurs pris en charge, voir la *Matrice de support d'OpenManage Enterprise* disponible sur le site de support.

En cliquant sur **OpenManage Enterprise** > **Paramètres de l'application**, vous pouvez :

- Configurer et gérer les paramètres réseau d'OpenManage Enterprise, tels que IPv4, IPv6, l'heure et les paramètres de proxy. Voir la rubriqueConfiguration des paramètres du réseau.
- Ajouter, activer, modifier et supprimer des utilisateurs. Voir la rubrique Gestion des utilisateurs.
- Définir l'intégrité du périphérique et les propriétés de surveillance du tableau de bord. Voir la rubrique Gestion des préférences de la console.
- Gérer les stratégies de connexion utilisateur et de verrouillage. Voir la rubrique Définition des propriétés de sécurité de connexion.
- Afficher le certificat SSL actuel, puis générer une requête de signature de certificat (RSC). Voir Génération et téléchargement de la requête de signature de certificat , page 163.
- Configurer les propriétés de messagerie, SNMP, syslog pour gérer les alertes. Voir Configuration des alertes SMTP, SNMP et Syslog , page 123.
- Définir les paramètres Trap Forward et l'écouteur SNMP. Voir la rubrique Gestion des alertes entrantes.
- Définir les informations d'identification et l'heure pour recevoir une notification sur l'expiration de la garantie. Voir la rubrique Gestion des paramètres de garantie.
- Définir les propriétés pour vérifier la disponibilité d'une version mise à jour, puis mettre à jour la version OpenManage Enterprise. Voir Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168.
- Définir les informations d'identification de l'utilisateur pour exécuter une commande distante à l'aide de RACADM et IPMI. Voir la rubrique Exécution des scripts et commandes distantes.
- Définir et recevoir des notifications d'alertes sur votre téléphone portable. Voir Paramètres d'OpenManage Mobile , page 175.

Tâches associées

Suppression de services d'annuaire , page 159

Sujets :

Configuration des paramètres OpenManage Enterprise

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

1. Pour afficher uniquement les paramètres réseau actuels de toutes les connexions réseau actives, tels que le nom de domaine DNS, le FQDN et les paramètres IPv4 et IPv6, développez **Paramètres actuels**.
2. Pour configurer le délai d'expiration de la session et le nombre maximal de sessions pour les utilisateurs de l'API et de l'interface Web d'OpenManage Enterprise, développez **Configuration du délai d'expiration de la session** et procédez comme suit :
   a. Cochez la case **Activer** pour activer le Délai d'expiration universel et saisissez la valeur du **Délai d'expiration (de 1 à 1 440)**. La valeur du délai d'expiration peut être définie de 1 minute à 1 440 minutes (24 heures). Par défaut, le Délai d'expiration universel est grisé. L'activation du Délai d'expiration universel désactive les champs API et Interface Web.
   b. Modifiez les valeurs du **Délai d'expiration (de 1 à 1 440)** et du **Nombre maximal de sessions (1 à 100)** de l'API. Ces attributs sont par défaut définis respectivement sur 30 minutes et 100.
   c. Modifiez les valeurs du **Délai d'expiration (de 1 à 1 440)** et du **Nombre maximal de sessions (1 à 100)** de l'interface Web. Ces attributs sont par défaut définis respectivement sur 30 minutes et 100.
   d. Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Abandonner** pour conserver les valeurs par défaut.
3. L'heure du système actuelle et la source (fuseau horaire local ou IP du serveur NTP) s'affichent. Pour configurer le fuseau horaire du système, la date, l'heure et la synchronisation du serveur NTP, développez **Configuration horaire**.
   a. Sélectionnez le fuseau horaire souhaité dans la liste déroulante.
   b. Saisissez la date ou cliquez sur l'icône **Calendrier** pour sélectionner la date.
   c. Saisissez l'heure au format hh:mm:ss.
   d. Pour la synchronisation avec un serveur NTP, cochez la case **Utiliser NTP**, puis saisissez l'adresse du serveur NTP principal.
      Vous pouvez configurer jusqu'à trois serveurs NTP avec OpenManage Entreprise.
      REMARQUE : Les paramètres **Date** et **Heure** ne sont pas disponibles lorsque l'option **Utiliser NTP** est sélectionnée.
   e. Cliquez sur **Appliquer**.
   f. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.
4. Pour configurer les paramètres de proxy d'OpenManage Enterprise, développez **Configuration du proxy**.
   a. Cochez la case **Activer les paramètres de proxy HTTP** pour configurer le proxy HTTP, puis saisissez l'adresse proxy HTTP et le numéro de port HTTP.
   b. Cochez la case **Activer l'authentification proxy** pour activer les informations d'identification du proxy, puis saisissez le nom d'utilisateur et le mot de passe.
   c. Cochez la case **Ignorer la validation de certificat** si le proxy configuré intercepte le trafic SSL et n'utilise pas de certificat tiers de confiance. Cette option permet d'ignorer les vérifications de certificat intégrées utilisées pour la garantie et la synchronisation de catalogue.
   d. Cliquez sur **Appliquer**.
   e. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Pour connaître toutes les tâches que vous pouvez effectuer à l'aide de la fonctionnalité Paramètres de l'application, voir Gestion des paramètres de l'appliance OpenManage Enterprise , page 147.

Gestion des utilisateurs OpenManage Enterprise

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Toute modification apportée au rôle d'utilisateur n'affecte pas la session active du ou des utilisateurs affectés et prend effet lors de la prochaine connexion.
- Si un utilisateur de gestionnaire de périphériques est rétrogradé au rôle observateur, ce dernier perd l'accès à toutes les entités détenues, telles que les tâches, les modèles de firmware ou de configuration et les lignes de base, les stratégies d'alerte et les profils. Ces entités ne peuvent être gérées que par l'administrateur et ne peuvent pas être restaurées même lorsque le même utilisateur est promu du rôle d'observateur au rôle de gestionnaire de périphériques.

En cliquant sur **OpenManage Enterprise** > **Paramètres de l'application** > **Utilisateurs**, vous pouvez :

- Afficher, ajouter, activer, modifier, désactiver ou supprimer des utilisateurs locaux d'OpenManage Enterprise. Pour en savoir plus, reportez-vous à Ajout et modification des utilisateurs locaux d'OpenManage Enterprise
- Attribuer des rôles OpenManage Enterprise aux utilisateurs Active Directory en important les groupes de répertoires. Les utilisateurs de répertoires Active Directory et LDAP peuvent attribuer un rôle d'administrateur, de gestionnaire de périphériques ou d'observateur dans OpenManage Enterprise. Pour en savoir plus, voir Importation de groupes AD et LDAP , page 154
- Voir les détails sur les utilisateurs connectés, puis arrêter (mettre fin à) une session utilisateur.
- Gérer les services d'annuaire. Pour en savoir plus, voir Ajout ou modification de groupes Active Directory à utiliser avec les services d'annuaire , page 157
- Afficher, ajouter, activer, modifier, désactiver ou supprimer des fournisseurs OpenID Connect (PingFederate et/ou Key Cloak). Pour en savoir plus, voir Connexion à OpenManage Enterprise à l'aide des fournisseurs Connect OpenID , page 159

Par défaut, la liste des utilisateurs s'affiche sous **Utilisateurs**. Le volet de droite affiche les propriétés d'un nom d'utilisateur sélectionné dans le volet en cours.

- **NOM D'UTILISATEUR** : avec les utilisateurs que vous avez créés, OpenManage Enterprise affiche les rôles d'utilisateurs par défaut suivants, qui ne peuvent pas être modifiés ou supprimés : admin, système et root. Cependant, vous pouvez modifier les informations d'identification de connexion en sélectionnant le nom d'utilisateur par défaut et en cliquant sur **Modifier**. Voir Activation d'utilisateurs OpenManage Enterprise , page 153. Les caractères recommandés pour les noms d'utilisateur sont les suivants :
  - 0-9
  - A–Z
  - a–z
  - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
  - Les caractères recommandés pour les mots de passe sont les suivants :
    - 0-9
    - A–Z
    - a–z
    - ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >
- **TYPE D'UTILISATEUR** : indique si l'utilisateur est connecté en local ou à distance.
- **ACTIVÉ** : indique avec une coche lorsque l'utilisateur est activé pour effectuer des tâches de gestion OpenManage Enterprise. Voir Activation d'utilisateurs OpenManage Enterprise , page 153 et Désactivation d'utilisateurs OpenManage Enterprise , page 153.
- **RÔLE** : indique le rôle de l'utilisateur dans OpenManage Enterprise. Par exemple, Administrateur et Gestionnaire de périphériques OpenManage Enterprise. Voir Types de rôles d'utilisateur OpenManage Enterprise , page 15.

Références connexes

Désactivation d'utilisateurs OpenManage Enterprise , page 153
Activation d'utilisateurs OpenManage Enterprise , page 153

Tâches associées

Suppression de services d'annuaire , page 159
Suppression d'utilisateurs OpenManage Enterprise , page 154
Mettre fin à des sessions utilisateur , page 156

Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise

OpenManage Enterprise possède un contrôle d'accès basé sur les rôles (RBAC) qui définit clairement les privilèges utilisateur pour les trois rôles intégrés : Administrateur, Gestionnaire de périphériques et Observateur. En outre, l'utilisation du contrôle d'accès basé sur le périmètre (SBAC) permet à un administrateur de limiter les groupes de périphériques auxquels un gestionnaire de périphériques a accès. Les rubriques suivantes décrivent en détail les fonctions RBAC et SBAC.

Privilèges du contrôle d'accès basé sur les rôles (RBAC) dans OpenManage Enterprise

Les utilisateurs se voient attribuer des rôles qui déterminent leur niveau d'accès aux paramètres de l'appliance et aux fonctionnalités de gestion des périphériques. Cette fonctionnalité est intitulée Contrôle d'accès basé sur les rôles. La console applique le privilège demandé pour une action spécifique avant d'autoriser cette action. Pour plus d'informations sur la gestion des utilisateurs sur OpenManage Enterprise, voir Gestion des utilisateurs OpenManage Enterprise , page 148.

Ce tableau répertorie les divers privilèges qui sont activés pour chaque rôle.

Tableau 27. Privilèges d'utilisateur basés sur des rôles dans OpenManage Enterprise

Fonctionnalités d'OpenManage Enterprise	Description des privilèges	Niveaux d'utilisateur pour l'accès à OpenManage Enterprise		
		Admin	Gestionnaire de périphériques	Observateur
configuration d'appliance	Paramètres de l'appliance globale impliquant la configuration de l'appliance.	O	N	N
Configuration de la sécurité	Paramètres de sécurité de l'appliance	O	N	N
Gestion des alertes	Actions/gestion des alertes	O	N	N
Gestion de la structure	Actions/gestion de la structure	O	N	N
Gestion du réseau	Actions/gestion du réseau	O	N	N
Gestion des groupes	Créer, lire, mettre à jour et supprimer (CRUD = Create, Read, Update, Delete) pour les groupes statiques et dynamiques	O	N	N
Gestion de la détection	Opérations CRUD sur les tâches de détection, exécution de tâches de détection	O	N	N
Gestion d'inventaire	Opérations CRUD sur les tâches d'inventaire, exécution de tâches d'inventaire	O	N	N
Gestion des interruptions	Importation de MIB, modification d'interruption	O	N	N
Gestion des déploiements automatiques	Gestion des opérations de configuration de déploiement automatique	O	N	N
Configuration de la surveillance	Politiques d'alerte, transfert, SupportAssist, etc.	O	O	N
Bouton d'alimentation	Redémarrage/cycle d'alimentation de l'appareil	O	O	N
Configuration de périphérique	Configuration de l'appareil, application de modèles, gestion/ migration de l'identité d'E/S, adressage du stockage (pour les appareils de stockage), etc.	O	O	N
Déploiement des systèmes d'exploitation	Déploiement du système d'exploitation, adressage de LUN, etc.	O	O	N
Mise à jour de l'appareil	Mise à jour de firmware de l'appareil, application des lignes de base mises à jour, etc.	O	O	N
Gestion des modèles	Création/gestion de modèles	O	O	N
Gestion des lignes de base	Création/gestion de politiques de ligne de base de firmware/ configuration	O	O	N
Gestion de l'alimentation	Définition de budgets d'alimentation	O	O	N
Gestion des tâches	Exécution/gestion de tâches	O	O	N

Tableau 27. Privilèges d'utilisateur basés sur des rôles dans OpenManage Enterprise (suite)

Fonctionnalités d'OpenManage Enterprise	Description des privilèges	Niveaux d'utilisateur pour l'accès à OpenManage Enterprise		
		Admin	Gestionnaire de périphériques	Observateur
Gestion des rapports	Opérations CRUD sur les rapports	O	O	N
Exécution des rapports	Exécution des rapports	O	O	O
Afficher	Affichage de toutes les données, exécution/gestion des rapports, etc.	O	O	O

Contrôle d'accès basé sur le périmètre (SBAC) dans OpenManage Enterprise

En utilisant la fonction de contrôle d'accès basé sur les rôles (RBAC), les administrateurs peuvent attribuer des rôles lors de la création d'utilisateurs. Les rôles déterminent leur niveau d'accès aux paramètres de l'appliance et aux fonctionnalités de gestion des périphériques. Le contrôle d'accès basé sur le périmètre (SBAC) est une extension de la fonction RBAC qui permet à un administrateur de restreindre un rôle de gestionnaire de périphériques à un sous-ensemble de groupes de périphériques appelé périmètre.

Lors de la création ou de la mise à jour d'un utilisateur gestionnaire de périphériques, les administrateurs peuvent attribuer le périmètre afin de limiter l'accès opérationnel du gestionnaire de périphériques à un ou plusieurs groupes de systèmes, groupes personnalisés et/ou groupes de plug-ins.

Les rôles Administrateur et Observateur possèdent un périmètre illimité. Cela signifie qu'ils disposent d'un accès opérationnel tel que spécifié par les privilèges de RBAC à toutes les entités de périphériques et de groupes.

Le périmètre peut être mis en œuvre comme suit :

1. Créer ou modifier un utilisateur
2. Attribuer un rôle Gestionnaire de périphériques
3. Attribuer le périmètre afin de limiter l'accès opérationnel

Pour plus d'informations sur la gestion des utilisateurs, voir Gestion des utilisateurs OpenManage Enterprise , page 148.

Lorsqu'un utilisateur gestionnaire de périphériques avec un périmètre attribué se connecte, le gestionnaire de périphériques peut uniquement voir et gérer les périphériques définis. En outre, le gestionnaire de périphériques peut voir et gérer des entités telles que les tâches, les modèles de firmware ou de configuration et les lignes de base, les stratégies d'alerte, les profils, etc. associés aux périphériques définis, uniquement si le gestionnaire de périphériques possède l'entité (il l'a créée ou la détient). Pour plus d'informations sur les entités qu'un gestionnaire de périphériques peut créer, reportez-vous à la section *Privilèges du contrôle d'accès basé sur les rôles dans OpenManage Enterprise*.

Par exemple, en cliquant sur **Configuration** > **Modèles**, un utilisateur gestionnaire de périphériques peut afficher les modèles par défaut et personnalisés appartenant à l'utilisateur gestionnaire de périphériques. En outre, l'utilisateur gestionnaire de périphériques peut effectuer d'autres tâches, comme RBAC le privilégie, sur les modèles qu'il possède.

En cliquant sur **Configuration** > **Pools d'identités**, un utilisateur gestionnaire de périphériques peut voir toutes les identités créées par un administrateur ou l'utilisateur gestionnaire de périphériques. Le gestionnaire de périphériques peut également effectuer des actions sur les identités spécifiées par le privilège RBAC. Toutefois, le gestionnaire de périphériques peut uniquement consulter l'utilisation de ces identités qui sont associées aux périphériques dans le périmètre du gestionnaire de périphériques.

De même, en cliquant sur **Configuration** > **Pools VLAN**, le gestionnaire de périphériques peut voir tous les VLAN créés par l'administrateur et les exporter. Le gestionnaire de périphériques ne peut pas effectuer d'autres opérations. Si le gestionnaire de périphériques possède un modèle, il peut le modifier pour utiliser les réseaux VLAN, mais il ne peut pas modifier le réseau VLAN.

Dans OpenManage Enterprise, le périmètre peut être attribué lors de la création d'un utilisateur local ou de l'importation d'un utilisateur AD/LDAP. L'attribution du périmètre aux utilisateurs OIDC peut être effectuée uniquement sur les fournisseurs Open ID Connect (OIDC).

SBAC pour les utilisateurs locaux :

Lors de la création ou de la modification d'un utilisateur local doté du rôle Gestionnaire de périphériques, l'administrateur peut sélectionner un ou plusieurs groupes de périphériques qui définissent le périmètre du gestionnaire de périphériques.

Par exemple, vous (en tant qu'administrateur) créez un utilisateur Gestionnaire de périphériques nommé dm1 et attribuez le groupe *g1* présent sous des groupes personnalisés. Ensuite, dm1 aura un accès opérationnel à tous les périphériques dans *g1* uniquement. L'utilisateur dm1 ne pourra pas accéder à d'autres groupes ou entités lié(e)s à d'autres périphériques.

En outre, avec SBAC, dm1 ne pourra pas non plus voir les entités créées par d'autres gestionnaires de périphériques (disons dm2) sur le même groupe *g1*. Cela signifie que l'utilisateur Gestionnaire de périphériques ne pourra voir que les entités appartenant à l'utilisateur.

Par exemple, vous (en tant qu'administrateur) créez un autre utilisateur gestionnaire de périphériques nommé dm2 et attribuez le même groupe *g1* présent sous des groupes personnalisés. Si dm2 crée un modèle de configuration, des lignes de base de configuration ou des profils pour les périphériques dans *g1*, dm1 n'aura pas accès à ces entités et vice versa.

Un gestionnaire de périphériques avec le périmètre défini sur Tous les périphériques a un accès opérationnel, tel que spécifié par les privilèges de RBAC, à tous les périphériques et toutes les entités de groupe appartenant au gestionnaire de périphériques.

SBAC pour les utilisateurs d'AD/LDAP :

Lors de l'importation ou de la modification des groupes AD/LDAP, les administrateurs peuvent attribuer des périmètres à des groupes d'utilisateurs dotés du rôle Gestionnaire de périphériques. Si un utilisateur est membre de plusieurs groupes AD, chacun doté d'un rôle Gestionnaire de périphériques, et que chaque groupe AD a des attributions de périmètre distinctes, le périmètre de l'utilisateur correspond à l'union des périmètres de ces groupes AD.

Par exemple :

- L'utilisateur dm1 est membre de deux groupes AD (*RR5-Floor1-LabAdmins* et *RR5-Floor3-LabAdmins*). Les deux groupes AD ont reçu le rôle Gestionnaire de périphériques. Les attributions de périmètre pour les groupes AD sont les suivantes : *RR5-Floor1-LabAdmins* obtient *ptlab-servers* et *RR5-Floor3-LabAdmins* obtient *smdlab-servers*. Désormais, le périmètre du gestionnaire de périphériques dm1 est l'union de *ptlab-servers* et de *smdlab-servers*.
- L'utilisateur dm1 est membre de deux groupes AD (*adg1* et *adg2*). Les deux groupes AD ont reçu le rôle gestionnaire de périphériques, avec des attributions de périmètre pour les groupes AD, comme suit : *adg1* a accès à *g1* et *adg2* a accès à *g2*. Si *g1* est le super-ensemble de *g2*, le périmètre de dm1 correspond au périmètre plus étendu (*g1*, à tous ses groupes enfants et tous les périphériques de noeud feuille).

Lorsqu'un utilisateur est membre de plusieurs groupes AD ayant des rôles différents, le rôle de fonctionnalité supérieure est prioritaire (dans l'ordre Administrateur, Gestionnaire de périphériques, Observateur).

Un gestionnaire de périphériques avec périmètre illimité dispose d'un accès opérationnel tel que spécifié par les privilèges de RBAC à toutes les entités de périphériques et de groupes.

REMARQUE : Après la mise à niveau d'OpenManage Enterprise depuis la version 3.5 ou une version antérieure, les gestionnaires de périphériques AD/LDAP et OIDC (PingFederate ou KeyCloak) doivent recréer toutes les entités de la version précédente, puisque ces entités ne sont disponibles que pour les administrateurs après la mise à niveau. Pour en savoir plus, consultez les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC pour les utilisateurs d'OIDC :

L'attribution du périmètre aux utilisateurs d'OIDC n'a pas lieu dans la console OME. Vous pouvez attribuer des périmètres aux utilisateurs d'OIDC au niveau d'un fournisseur OIDC lors de la configuration de l'utilisateur. Lorsque l'utilisateur se connecte avec les informations d'identification du fournisseur OIDC, le rôle et l'attribution du périmètre seront disponibles pour OME. Pour en savoir plus sur la configuration des périmètres et rôles utilisateur, voir Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161.

REMARQUE : Si PingFederate est utilisé en tant que fournisseur OIDC, seuls les rôles d'administrateur peuvent être utilisés. Pour en savoir plus, consultez la section Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161 et les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfert de propriété : l'administrateur peut transférer les ressources dont il est propriétaire d'un gestionnaire de périphériques (source) vers un autre gestionnaire de périphériques. Par exemple, un administrateur peut transférer toutes les ressources attribuées à partir d'un dm1 source vers dm2. Un gestionnaire de périphériques avec des entités détenues, telles que les lignes de base du firmware et/ou de configuration, les modèles de configuration, les stratégies d'alerte et les profils est considéré comme un utilisateur source éligible. Le transfert de propriété transfère uniquement les entités et non les groupes de périphériques (périmètre) appartenant à un gestionnaire de périphériques vers un autre. Pour plus d'informations, voir Transfert de propriété des entités du gestionnaire de périphériques , page 155.

Références connexes

Types de rôles d'utilisateur OpenManage Enterprise , page 15

Ajout et modification des utilisateurs locaux d'OpenManage Enterprise

Cette procédure est spécifique à l'ajout et à la modification des utilisateurs locaux seulement. Lors de la modification des utilisateurs locaux, vous pouvez modifier toutes les propriétés des utilisateurs. Cependant, pour les utilisateurs d'Active Directory, seuls le rôle et les groupes de périphériques (dans le cas d'un Gestionnaire de périphériques) peuvent être modifiés. Pour intégrer les services d'Active

Directory à OpenManage Enterprise et pour importer les utilisateurs d'Active Directory, reportez-vous à Intégration de services d'annuaire dans OpenManage Enterprise , page 156 et Importation de groupes AD et LDAP , page 154.

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Vous ne pouvez pas activer, désactiver ou supprimer les utilisateurs admin/system/root. Vous pouvez modifier le mot de passe uniquement en cliquant sur **Modifier** dans le volet de droite.

1. Sélectionnez **Paramètres d'application** > **Utilisateurs** > **Utilisateurs** > **Ajouter**.
2. Dans la boîte de dialogue **Ajouter un nouvel utilisateur** :
   a. Sous **Détails de l'utilisateur**, sélectionnez Administrateur, Gestionnaire de périphériques ou Observateur dans le menu déroulant **Rôle utilisateur**.

      Pour plus d'informations, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

      Par défaut, la case **Activé** est cochée pour indiquer que les privilèges d'utilisateur actuellement en cours de configuration sont activés pour un utilisateur.

   b. Pour les rôles de Gestionnaire de périphériques, le champ d'application est défini par défaut sur **Tous les appareils** (champ d'application non restreint). Toutefois, l'administrateur peut restreindre le champ d'application en choisissant l'option **Sélectionner des groupes**, puis un ou plusieurs groupes de périphériques.
   c. Sous **Informations d'identification**, saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis saisissez à nouveau le mot de passe dans les champs **Confirmer le mot de passe**.

      REMARQUE : Le nom d'utilisateur doit contenir uniquement des caractères alphanumériques (mais le trait de soulignement est autorisé) et le mot de passe doit contenir au moins un caractère en majuscule, en minuscule, un chiffre et un caractère spécial.

3. Cliquez sur **Terminer**.
   Un message s'affiche pour indiquer que l'utilisateur a été enregistré avec succès. Une tâche est démarrée pour créer un nouvel utilisateur. À la fin de la tâche, le nouvel utilisateur est créé et affiché dans la liste des utilisateurs.

Modification des propriétés utilisateur OpenManage Enterprise

1. Sur la page **Paramètres d'application**, sous **Utilisateurs**, cochez la case correspondant à l'utilisateur.
2. Exécutez les tâches décrites dans Ajout et modification des utilisateurs locaux d'OpenManage Enterprise , page 152.
   Les données mises à jour sont enregistrées.

   REMARQUE : Lorsque vous modifiez le rôle d'un utilisateur, les privilèges disponibles pour le nouveau rôle sont automatiquement appliqués. Par exemple, si vous définissez un administrateur en tant que gestionnaire de périphériques, les droits d'accès et privilèges prévus pour un administrateur seront automatiquement activés pour le gestionnaire de périphériques.

Activation d'utilisateurs OpenManage Enterprise

Cochez la case correspondant au nom d'utilisateur et cliquez sur **Activer**. L'utilisateur est activé et une coche s'affiche dans la cellule correspondante de la colonne **ACTIVÉ**. Si l'utilisateur est déjà activé lors de la création du nom d'utilisateur, le bouton **Activer** est grisé.

Tâches associées

Suppression de services d'annuaire , page 159
Suppression d'utilisateurs OpenManage Enterprise , page 154
Mettre fin à des sessions utilisateur , page 156

Information associée

Gestion des utilisateurs OpenManage Enterprise , page 148

Désactivation d'utilisateurs OpenManage Enterprise

Cochez la case correspondant au nom d'utilisateur, puis cliquez sur **Désactiver**. L'utilisateur est désactivé, et la coche disparaît dans la cellule correspondante de la colonne **ACTIVÉ**. Si l'utilisateur est désactivé lors de la création du nom d'utilisateur, le bouton **Désactiver** est grisé.

Tâches associées

Suppression de services d'annuaire , page 159
Suppression d'utilisateurs OpenManage Enterprise , page 154
Mettre fin à des sessions utilisateur , page 156

Information associée

Gestion des utilisateurs OpenManage Enterprise , page 148

Suppression d'utilisateurs OpenManage Enterprise

1. Cochez la case correspondant à l'utilisateur, puis cliquez sur **Supprimer**.
2. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**.

Références connexes

Désactivation d'utilisateurs OpenManage Enterprise , page 153
Activation d'utilisateurs OpenManage Enterprise , page 153

Information associée

Gestion des utilisateurs OpenManage Enterprise , page 148

Importation de groupes AD et LDAP

REMARQUE :

- Les utilisateurs qui ne possèdent pas des droits d'Administrateur ne peuvent pas activer ou désactiver des utilisateurs AD (Active Directory) ou le protocole LDAP (Lightweight Directory Access Protocol).
- Avant d'importer des groupes Active Directory dans OpenManage Enterprise, vous devez inclure les groupes d'utilisateurs dans un GROUPE UNIVERSEL lors de la configuration d'Active Directory.
- les utilisateurs des répertoires AD et LDAP peuvent être importés et attribués à l'un des rôles d'OpenManage Enterprise (Admin, Gestionnaire de périphériques ou Observateur). La fonction d'authentification unique (SSO) s'arrête après l'ouverture d'une session sur la console. Les actions exécutées sur les périphériques nécessitent un compte doté de privilèges sur le périphérique.
- Après la mise à niveau d'OpenManage Enterprise depuis la version 3.5 ou une version antérieure, les gestionnaires de périphériques AD/LDAP et OIDC (PingFederate ou KeyCloak) doivent recréer toutes les entités de la version précédente, puisque ces entités ne sont disponibles que pour les administrateurs après la mise à niveau. Pour en savoir plus, consultez les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

1. Cliquez sur **Importer un groupe de répertoire**.
2. Dans la boîte de dialogue **Importer Active Directory** :
   a. Dans le menu déroulant **Source d'annuaire**, sélectionnez une source AD ou LDAP qui doit être importée pour ajouter des groupes. Pour ajouter des répertoires, voir Ajout ou modification de groupes Active Directory à utiliser avec les services d'annuaire , page 157.
   b. Cliquez sur **Saisie des informations d'identification**.
   c. Dans la boîte de dialogue, entrez le nom d'utilisateur et le mot de passe du domaine dans lequel l'annuaire est enregistré. Utilisez les info-bulles pour entrer la syntaxe correcte.
   d. Cliquez sur **Terminer**.
3. Dans la section **Groupes disponibles** :
   a. Dans la zone **Recherche d'un groupe**, entrez les premières lettres du nom de groupe disponible dans l'annuaire testé. Tous les noms de groupes qui commencent par le texte entré sont répertoriés sous NOM DE GROUPE.
   b. Sélectionnez les cases correspondant aux groupes à importer, puis cliquez sur les boutons **>>** ou **<<** pour ajouter ou supprimer des groupes.

4. Dans la section **Groupes à importer** :
   a. Cochez les cases des groupes, puis sélectionnez un rôle dans le menu déroulant Affecter un rôle au groupe. Pour plus d'informations sur l'accès basé sur les rôles, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
   b. Cliquez sur **Affecter un rôle**.
   Les utilisateurs du groupe sous le service d'annuaire sélectionné sont attribués aux rôles utilisateur sélectionnés.
   c. Pour le rôle de gestionnaire de périphériques, le champ d'application est défini par défaut sur **Tous les appareils**. Toutefois, l'administrateur peut restreindre le champ d'application en choisissant l'option **Affecter une portée**, puis un ou plusieurs groupes de périphériques.
5. Répétez les étapes 3 et 4, si nécessaire.
6. Cliquez sur **Importer**.
   Les groupes d'annuaire sont importés et affichés dans la liste d'utilisateurs. Toutefois, tous les utilisateurs de ces groupes se connectent à OpenManage Enterprise à l'aide de leurs informations d'identification et de leur nom d'utilisateur de domaine.

Il est possible qu'un utilisateur de domaine, par exemple john_smith, soit membre de plusieurs groupes d'annuaire, et également que ces groupes se voient attribuer des rôles différents. Dans ce cas, plusieurs rôles tels que le gestionnaire de périphériques et l'observateur s'affichent lorsque vous survolez le nom d'utilisateur dans le coin droit de l'en-tête de l'appliance. Ces utilisateurs reçoivent le rôle au niveau le plus élevé pour tous les groupes de répertoire dont ils sont membres.

- Exemple 1 : l'utilisateur est membre de trois groupes avec les rôles d'administrateur, de gestionnaire de périphériques et d'observateur. Dans ce cas, l'utilisateur devient un administrateur.
- Exemple 2 : l'utilisateur est membre de trois groupes de gestionnaires de périphériques et d'un groupe d'observateurs. Dans ce cas, l'utilisateur devient un gestionnaire de périphériques avec accès à l'union des groupes de périphériques des trois rôles de gestionnaire de périphériques.

Transfert de propriété des entités du gestionnaire de périphériques

Cette rubrique décrit comment un administrateur peut transférer des entités telles que des tâches, des modèles de firmware ou de configuration et des lignes de base, des stratégies d'alerte et des profils créés par un gestionnaire de périphériques vers un autre gestionnaire de périphériques. L'administrateur peut déclencher une opération de transfert de propriété lorsqu'un gestionnaire de périphériques quitte l'organisation.

REMARQUE :

- Pour exécuter cette tâche sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur administrateur. Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Le transfert de propriété transfère uniquement les entités et non les groupes de périphériques (périmètre) appartenant à un gestionnaire de périphériques vers un autre.
- Avant qu'un transfert de propriété des entités soit lancé, l'administrateur doit d'abord réaffecter les groupes de périphériques appartenant à l'ancien gestionnaire de périphériques à celui qui va prendre le relais.
- Si la propriété des entités est transférée à un groupe d'utilisateurs Active Directory, la propriété est transférée à tous les membres de ce groupe AD.

Pour transférer la propriété des entités (tâches, modèles de firmware ou de configuration et lignes de base, stratégies d'alerte et profils) d'un gestionnaire de périphériques à un autre, procédez comme suit :

1. Lancez l'Assistant Transfert de propriété en cliquant sur **OpenManage Enterprise** > **Paramètres d'application** > **Utilisateurs** > **Transfert de propriété**.
2. Dans la liste déroulante **Utilisateur source**, sélectionnez le gestionnaire de périphériques à partir duquel la propriété des entités doit être transférée.

   REMARQUE : L'utilisateur source répertorie uniquement les gestionnaires de périphériques supprimés, OIDC,Active Directory ou locaux, qui sont associés à des entités telles que des tâches, des modèles de firmware ou de configuration, des stratégies d'alerte et des profils.

3. Dans la liste déroulante **Utilisateur cible**, sélectionnez le gestionnaire de périphériques auquel les entités seront transférées.
4. Cliquez sur **Terminer**, puis sur **Oui** dans le message d'invite.

Toutes les entités détenues, telles que les tâches, les modèles de firmware ou de configuration, les stratégies d'alerte et les profils sont transférées depuis le gestionnaire de périphériques « source » vers le gestionnaire de périphériques « cible ».

Mettre fin à des sessions utilisateur

1. Cochez la case correspondant au nom d'utilisateur, puis cliquez sur **Terminer**.
2. Lorsque le programme vous invite à confirmer, cliquez sur **OUI**.
   La session utilisateur sélectionnée est fermée et l'utilisateur est déconnecté.

Références connexes

Désactivation d'utilisateurs OpenManage Enterprise , page 153
Activation d'utilisateurs OpenManage Enterprise , page 153

Information associée

Gestion des utilisateurs OpenManage Enterprise , page 148

Intégration de services d'annuaire dans OpenManage Enterprise

Les services d'annuaire vous permettent d'importer des groupes d'annuaire d'AD ou de LDAP pour les utiliser sur la console. OpenManage Enterprise prend en charge l'intégration des services de répertoire suivants :

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP LDAP

Conditions préalables/attributs pris en charge pour l'intégration de LDAP

Tableau 28. Conditions préalables d'OpenManage Enterprise/attributs pris en charge pour l'intégration de LDAP

	Attribut de la connexion utilisateur	Attribut d'appartenance au groupe.	Certificats requis
AD/LDAP	Cn, sAMAccountName	Membre	• Le certificat de contrôleur de domaine doit avoir un FQDN. Le champ SAN peut être défini sur IPv4 et/ou IPv6 ou FQDN. • Seul le format de certificat Base64 est pris en charge
OpenLDAP	uid, sn	Uniquemember	Seul le format de certificat PEM est pris en charge.
PHP LDAP	uid	MemberUid	

Conditions préalables à remplir par l'utilisateur pour l'intégration du service d'annuaire

Vous devez vous assurer que les conditions préalables suivantes sont remplies avant d'entreprendre l'intégration du service d'annuaire :

1. L'utilisateur BindDN et l'utilisateur choisi pour la « connexion de test » doivent être identiques.
2. Si l'Attribut de la connexion utilisateur est renseigné, seule la valeur de nom d'utilisateur correspondante affectée à l'attribut est autorisée pour la connexion de l'appliance.
3. L'utilisateur choisi pour la connexion de test doit faire partie d'un groupe autre que celui par défaut dans LDAP.
4. L'Attribut d'appartenance au groupe doit avoir le nom « UserDN » ou le nom abrégé (utilisé pour la connexion) de l'utilisateur.
5. Lorsque MemberUid est utilisé en tant qu'Attribut d'appartenance au groupe, le nom d'utilisateur utilisé pour la connexion de l'appliance est considéré comme sensible à la casse dans certaines configurations de LDAP.

6. Lorsqu'un filtre de recherche est utilisé dans la configuration de LDAP, la connexion n'est pas autorisée pour les utilisateurs qui ne remplissent pas les critères de recherche mentionnés.
7. La recherche de groupe ne fonctionnera que si les groupes sont affectés à des utilisateurs sous l'Attribut d'appartenance au groupe fourni.

REMARQUE : Si OpenManage Enterprise est hébergée sur un réseau IPv6, l'authentification SSL par rapport au contrôleur de domaine à l'aide de FQDN échouerait si l'IPv4 est définie comme adresse préférée dans DNS. Pour éviter cet échec, procédez à l'une des opérations suivantes :

- L'adresse préférée dans DNS doit être définie sur IPv6 lorsque vous y êtes invité avec FQDN.
- Dans le champ SAN du certificat DC, IPv6 doit apparaitre.

Pour utiliser les services d'annuaire, procédez comme suit :

- Ajoutez une connexion à un annuaire. Voir Ajout ou modification de groupes Active Directory à utiliser avec les services d'annuaire , page 157.
- Importez des groupes d'annuaire et affectez un rôle spécifique à tous les utilisateurs du groupe. Voir Importation de groupes AD et LDAP , page 154.
- Pour les gestionnaires de périphériques, modifiez le groupe de répertoire pour ajouter les groupes que le gestionnaire de périphériques peut gérer. Voir Ajout et modification des utilisateurs locaux d'OpenManage Enterprise , page 152.

Ajout ou modification de groupes Active Directory à utiliser avec les services d'annuaire

1. Cliquez sur **Paramètres de l'application** > **Utilisateurs** > **Services d'annuaire**, puis cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Se connecter au service d'annuaire**, par défaut, **AD** est sélectionné pour indiquer que le type d'annuaire est Active Directory (AD) :

   REMARQUE : Pour créer un groupe d'utilisateurs LDAP à l'aide des services d'annuaire, voir Ajout ou modification des groupes Lightweight Directory Access Protocol à utiliser avec les services d'annuaire , page 158.

   a. Saisissez le nom souhaité pour le répertoire AD.
   b. Sélectionnez la méthode de recherche des contrôleurs de domaine :
      - **DNS** : dans la case **Méthode**, saisissez le nom de domaine pour interroger le serveur DNS pour les contrôleurs de domaine.
      - **Manuel** : dans la case **Méthode**, saisissez le FQDN ou l'adresse IP du contrôleur de domaine. Pour plusieurs serveurs, un maximum de trois serveurs est pris en charge. Utilisez une liste séparée par des virgules.
   c. Dans la zone **Domaine du groupe**, entrez le domaine du groupe comme suggéré dans la syntaxe de l'info-bulle.
3. Dans la section **Options avancées** :
   a. Par défaut, le numéro de port de l'adresse du catalogue global affiche la valeur 3269. Pour l'accès au contrôleur de domaine, saisissez 636 comme numéro de port.

      REMARQUE : Seuls les ports LDAPS sont pris en charge.

   b. Saisissez le délai d'expiration du réseau et le délai d'expiration de la recherche en secondes. La durée d'expiration maximale prise en charge est de 300 secondes.
   c. Pour télécharger un certificat SSL, sélectionnez **Validation de certificat** et cliquez sur **Sélectionner un fichier**. Le certificat doit être un certificat d'AC racine codé au format Base64.

   L'onglet **Tester la connexion** s'affiche.
4. Cliquez sur **Tester la connexion**.
5. Dans la boîte de dialogue, saisissez le **nom d'utilisateur** et le **mot de passe** du domaine auquel se connecter.

   REMARQUE : Le **nom d'utilisateur** doit être défini au format UPN (nom d'utilisateur@domaine) ou NetBIOS (domaine\nom d'utilisateur).
6. Cliquez sur **Tester la connexion**.
   Dans la boîte de dialogue **Informations sur le service d'annuaire**, un message s'affiche pour indiquer que la connexion est établie.
7. Cliquez sur **OK**.
8. Cliquez sur **Terminer**.
   Une tâche est créée et exécutée pour ajouter l'annuaire demandé dans la liste des services d'annuaire.

1. Dans la colonne **NOM DE L'ANNUAIRE**, sélectionnez l'annuaire. Les propriétés du service d'annuaire s'affichent dans le volet de droite.
2. Cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Se connecter au service d'annuaire**, modifiez les données et cliquez sur **Terminer**. Les données sont mises à jour et enregistrées.

Ajout ou modification des groupes Lightweight Directory Access Protocol à utiliser avec les services d'annuaire

1. Cliquez sur **Paramètres de l'application** > **Utilisateurs** > **Services d'annuaire**, puis cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Se connecter au service d'annuaire**, sélectionnez **LDAP** comme type d'annuaire.

   REMARQUE : Pour créer un groupe d'utilisateurs AD à l'aide des services d'annuaire, voir Ajout ou modification de groupes Active Directory à utiliser avec les services d'annuaire , page 157.

   a. Saisissez le nom souhaité pour le répertoire LDAP.
   b. Sélectionnez la méthode de recherche des contrôleurs de domaine :
      - **DNS** : dans la case **Méthode**, saisissez le nom de domaine pour interroger le serveur DNS pour les contrôleurs de domaine.
      - **Manuel** : dans la case **Méthode**, saisissez le FQDN ou l'adresse IP du contrôleur de domaine. Pour plusieurs serveurs, un maximum de trois serveurs est pris en charge. Utilisez une liste séparée par des virgules.
   c. Saisissez le nom unique (DN) de liaison LDAP et le mot de passe.

      REMARQUE : La liaison anonyme n'est pas prise en charge pour AD LDS.

3. Dans la section **Options avancées** :
   a. Par défaut, le numéro de port LDAP affiche la valeur 636. Pour modifier, saisissez un numéro de port.

      REMARQUE : Seuls les ports LDAPS sont pris en charge.

   b. Pour qu'il corresponde à la configuration LDAP sur le serveur, saisissez le groupe DN de base à rechercher.
   c. Saisissez les **Attributs d'utilisateur** déjà configurés dans le système LDAP. Il est recommandé que celui-ci soit unique dans le nom unique de base sélectionné. Sinon, configurez un filtre de recherche pour vous assurer qu'il est unique. Si le nom unique de l'utilisateur ne peut être identifié de façon spécifique par une combinaison attribut et un filtre de recherche, la connexion échoue.

      REMARQUE : Les attributs d'utilisateur doivent être configurés dans le système LDAP utilisé pour la requête avant l'intégration aux services de répertoire.

      REMARQUE : Vous devez définir les attributs d'utilisateur sur **cn** ou **sAMAccountName** pour la configuration AD LDS et **UID** pour la configuration LDAP.

   d. Dans la zone **Attribut d'appartenance au groupe**, saisissez l'attribut qui stocke les groupes et les informations du membre dans le répertoire.
   e. Saisissez le délai d'expiration du réseau et le délai d'expiration de la recherche en secondes. La durée d'expiration maximale prise en charge est de 300 secondes.
   f. Pour télécharger un certificat SSL, sélectionnez **Validation de certificat** et cliquez sur **Sélectionner un fichier**. Le certificat doit être un certificat d'AC racine codé au format Base64.

   Le bouton **Tester la connexion** est activé.
4. Cliquez sur **Tester la connexion**, puis saisissez les informations d'identification de liaison du domaine auquel vous souhaitez vous connecter.

   REMARQUE : Lors du test de connexion, assurez-vous que le **nom d'utilisateur test** correspond à la valeur de l'**attribut de connexion utilisateur** saisi précédemment.
5. Cliquez sur **Tester la connexion**.
   Dans la boîte de dialogue **Informations sur le service d'annuaire**, un message s'affiche pour indiquer que la connexion est établie.
6. Cliquez sur **OK**.
7. Cliquez sur **Terminer**.
   Une tâche est créée et exécutée pour ajouter l'annuaire demandé dans la liste des services d'annuaire.

1. Dans la colonne **NOM DE L'ANNUAIRE**, sélectionnez l'annuaire. Les propriétés du service d'annuaire s'affichent dans le volet de droite.

2. Cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Se connecter au service d'annuaire**, modifiez les données et cliquez sur **Terminer**. Les données sont mises à jour et enregistrées.

Suppression de services d'annuaire

Cochez la case correspondant aux services d'annuaire à supprimer, puis cliquez sur **Supprimer**.

Références connexes

Désactivation d'utilisateurs OpenManage Enterprise , page 153
Activation d'utilisateurs OpenManage Enterprise , page 153

Information associée

Gestion des paramètres de l'appliance OpenManage Enterprise , page 147
Gestion des utilisateurs OpenManage Enterprise , page 148

Connexion à OpenManage Enterprise à l'aide des fournisseurs Connect OpenID

Vous pouvez vous connecter à l'aide des fournisseurs OpenID Connect (OIDC). Les fournisseurs OpenID Connect sont les logiciels d'identité et de gestion des utilisateurs qui permettent aux utilisateurs d'accéder en toute sécurité aux applications. Actuellement, OpenManage Enterprise prend en charge PingFederate et Keycloak.

AVERTISSEMENT : Les rôles d'utilisateur et les périmètres par défaut sont rétablis lors de la nouvelle inscription du client avec le fournisseur OIDC PingFederate (PingIdentity). Ce problème peut entraîner la réinitialisation des privilèges et du périmètre des rôles non-administrateurs (gestionnaire de périphériques et observateur) à ceux de l'administrateur. Le réenregistrement de la console de l'appliance à l'aide du fournisseur OIDC est déclenché en cas de mise à niveau de l'appliance, modification de la configuration réseau ou modification du certificat SSL.

Pour éviter tout problème de sécurité après l'un des événements de réenregistrement mentionnés ci-dessus, l'administrateur doit reconfigurer tous les ID client OpenManage Enterprise sur le site PingFederate. En outre, il est fortement recommandé de créer des ID client uniquement pour les utilisateurs administrateurs dotés de Pingfederate jusqu'à ce que ce problème soit résolu.

REMARQUE :

- Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir la section Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Vous pouvez ajouter un maximum de quatre ID de fournisseur OpenID Connect à l'appliance.
- Après la mise à niveau d'OpenManage Enterprise depuis la version 3.5 ou une version antérieure, les gestionnaires de périphériques AD/LDAP et OIDC (PingFederate ou KeyCloak) doivent recréer toutes les entités de la version précédente, puisque ces entités ne sont disponibles que pour les administrateurs après la mise à niveau. Pour en savoir plus, consultez les notes de mise à jour sur https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

Conditions préalables :

Avant d'activer la connexion au fournisseur OpenID Connect, vous devez effectuer les opérations suivantes :

1. **Ajouter un fournisseur OIDC dans OpenManage Enterprise** : dans les paramètres d'application OpenManage Enterprise, ajoutez un fournisseur OpenID Connect. Lorsque vous ajoutez le fournisseur OpenID Connect, un **ID client** est généré pour le fournisseur OpenID Connect. Pour plus d'informations, voir : Ajouter un fournisseur OpenID Connect à OpenManage Enterprise , page 160.
2. **Configurer le fournisseur OpenID Connect à l'aide de l'ID client** : dans le fournisseur OpenID Connect, localisez l'ID client et définissez un rôle de connexion (administrateur, gestionnaire d'appareil ou observateur) en ajoutant et en mappant l'étendue nommée **dxcua** (revendication Dell étendue pour l'authentification de l'utilisateur). Pour de plus amples informations, consultez :
   - Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161

- Configurer une stratégie de fournisseur Connect OpenID dans Keycloak pour un accès basé sur des rôles à OpenManage Enterprise , page 161

Lorsque vous ajoutez un fournisseur OpenID Connect dans OpenManage Enterprise, il est répertorié sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect**. Les informations suivantes concernant le fournisseur OIDC s'affichent :

- Nom : nom du fournisseur de OpenID Connect lorsqu'il a été ajouté à l'appliance
- Activé : une coche sur ce champ indique que le fournisseur OpenID Connect est activé dans l'appliance
- URI de découverte : l'URI (Uniform Resource Identifier) du fournisseur OpenID Connect
- État d'enregistrement : peut être l'une des valeurs suivantes :
  - Réussite : indique que l'enregistrement avec le fournisseur OpenID Connect a fonctionné.
  - Échec : indique l'échec de l'enregistrement auprès du fournisseur de OpenID Connect. Un échec d'enregistrement du fournisseur OpenID Connect ne sera pas autorisé, même lorsqu'il est activé.
  - En cours : cet état s'affiche lorsque l'appliance tente de s'enregistrer auprès du fournisseur OpenID Connect.

Dans le panneau de droite, l'ID client, l'état d'enregistrement et l'URI de découverte s'affichent pour le fournisseur OpenID Connect sélectionné. Vous pouvez cliquer sur **Voir les détails** pour afficher les détails du certificat du fournisseur OpenID Connect.

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect**, vous pouvez effectuer les opérations suivantes :

- Ajouter un fournisseur OpenID Connect à OpenManage Enterprise , page 160
- Modifier les informations d'un fournisseur OpenID Connect dans OpenManage Enterprise , page 162
- Test de l'état de l'enregistrement d'OpenManage Enterprise avec le fournisseur OpenID Connect , page 162
- Activer les fournisseurs OpenID Connect , page 162
- Désactiver les fournisseurs OpenID Connect , page 163
- Supprimer des fournisseurs OpenID Connect , page 162

Ajouter un fournisseur OpenID Connect à OpenManage Enterprise

L'ajout, l'activation et l'enregistrement d'un fournisseur OpenID Connect (Keycloak ou PingFederate) permet la connexion d'un client autorisé à OpenManage Enterprise. Cela génère un ID client.

Pour ajouter un fournisseur OpenID Connect à OpenManage Enterprise, accédez à la page **Paramètres d'application** > **Utilisateurs** > **Fournisseur OpenID Connect**, puis procédez comme suit :

REMARQUE : Vous pouvez ajouter un maximum de quatre clients OpenID Connect.

1. Cliquez sur **Ajouter** pour activer la page Ajouter un fournisseur OpenID Connect.
2. Remplissez les informations suivantes dans les champs correspondants :
   a. Nom : nom du client OIDC.
   b. URI de découverte : Uniform Resource Identifier du fournisseur OIDC
   c. Type d'authentification : choisissez l'une des méthodes suivantes, que le jeton d'accès doit utiliser pour accéder à l'appliance :
      i. Token d'accès initial : fournissez le jeton d'accès initial
      ii. Nom d'utilisateur et mot de passe : fournissez le nom d'utilisateur et le mot de passe
   d. (Facultatif) Case à cocher Validation de certificat : vous pouvez cocher cette case et télécharger le certificat du fournisseur OIDC en cliquant sur **Parcourir** et en localisant le certificat ou en faisant glisser le certificat dans la case « ligne brisée ».
   e. (Facultatif) Tester la connexion : cliquez sur **Tester la connexion URI et SSL** pour tester la connexion au fournisseur OpenID Connect.
      REMARQUE : Le test de connexion ne dépend pas du nom d'utilisateur et du mot de passe ou des informations de jeton d'accès initial, car il vérifie uniquement la validité de l'URI de découverte fourni.
   f. (Facultatif) Case à cocher Activé : vous pouvez cocher cette case pour autoriser les jetons d'accès client autorisés à se connecter à l'appliance.
3. Cliquez sur **Terminer**.

Le fournisseur OpenID Connect qui vient d'être ajouté est répertorié dans la page Paramètres de l'application > Utilisateurs > Fournisseurs OpenID Connect et l'ID client peut être situé dans le panneau de droite.

Étapes suivantes :

Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise , page 161

Configurer une stratégie de fournisseur Connect OpenID dans Keycloak pour un accès basé sur des rôles à OpenManage Enterprise , page 161

Configurer une règle de fournisseur de OpenID Connect dans PingFederate pour un accès basé sur des rôles à OpenManage Enterprise

Pour activer la connexion OpenManage Enterprise OpenID Connect à l'aide de PingFederate, vous devez ajouter et mapper une étendue **dxcua** (réclamation étendue Dell pour l'authentification utilisateur) à l'ID client et définir les privilèges utilisateur comme suit :

AVERTISSEMENT : Les rôles d'utilisateur et les périmètres par défaut sont rétablis lors de la nouvelle inscription du client avec le fournisseur OIDC PingFederate (PingIdentity). Ce problème peut réinitialiser les privilèges et le périmètre des rôles non-administrateurs (gestionnaire de périphériques et observateur) à ceux de l'administrateur. Le réenregistrement de la console de l'appliance à l'aide du fournisseur OIDC est déclenché en cas de mise à niveau de l'appliance, modification de la configuration réseau ou modification du certificat SSL.

Pour éviter tout problème de sécurité après l'un des événements de réenregistrement mentionnés ci-dessus, l'administrateur doit reconfigurer tous les ID client OpenManage Enterprise sur le site PingFederate. En outre, il est fortement recommandé de créer des ID client uniquement pour les utilisateurs administrateurs dotés de Pingfederate jusqu'à ce que ce problème soit résolu.

REMARQUE :

- L'algorithme d'attribution par défaut doit être RS256 (Signature RSA avec SHA-256).

1. Ajoutez une étendue « exclusive » ou « par défaut » appelée **dxcua** sous Gestion de l'étendue dans les paramètres OAuth.
2. Mappez l'étendue créée dans **Gestion des stratégies OpenID Connect** > **Stratégie** en suivant les étapes ci-dessous :
   a. Activer **Inclure les informations utilisateur dans le jeton**
   b. Dans le champ Étendue de l'attribut, ajoutez l'étendue et la valeur de l'attribut en tant que **dxcua**.
   c. Dans le champ Exécution du contrat, ajoutez dxcua et sélectionnez le type « Texte ». Définissez ensuite les privilèges d'utilisateur pour la connexion du fournisseur OpenManage Enterprise OpenID Connect à l'aide de l'un des attributs suivants :
      i. Administrateur : `dxcua : [{"Role": "AD"}]`
      ii. Gestionnaire d'appareils : `dxcua : [{"Role": "DM"}]`
      REMARQUE : Pour limiter l'accès au gestionnaire de périphériques et sélectionner des groupes de périphériques, par exemple G1 et G2, dans OpenManage Enterprise utilisez `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
      iii. Observateur : `dxcua : [{"Role": "VE"}]`
   d. Si une étendue « exclusive » est configurée après l'enregistrement du client dans OpenManage Enterprise, modifiez le client configuré dans PingFederate et activez l'étendue exclusive « dxcua » créée.
3. L'**enregistrement du client dynamique** doit être activé dans PingFederate pour l'enregistrement du client Enterprise OpenManage. Si l'option « Demander un jeton d'accès initial » n'est pas sélectionnée dans les paramètres du client du fournisseur OpenID Connect, l'enregistrement fonctionnera avec le nom d'utilisateur et le mot de passe. Si l'option est activée, l'enregistrement ne fonctionne qu'avec le jeton d'accès initial.

Configurer une stratégie de fournisseur Connect OpenID dans Keycloak pour un accès basé sur des rôles à OpenManage Enterprise

Pour activer la connexion OpenManage Enterprise OpenID Connect à l'aide de Keycloak, vous devez d'abord ajouter et mapper une étendue **dxcua** à l'ID client et définir les privilèges utilisateur comme suit :

REMARQUE : Les URI de découverte spécifiés dans l'Assistant de configuration du fournisseur OpenID Connect doivent avoir un point de terminaison valide du fournisseur répertorié.

1. Dans la section Attributs des utilisateurs Keycloak, définissez la « Clé et valeur » pour les rôles de connexion OpenManage Enterprise à l'aide de l'un des attributs suivants :
   - Administrateur : `dxcua : [{"Role": "AD"}]`
   - Gestionnaire d'appareils : `dxcua : [{"Role": "DM"}]`
     REMARQUE : Pour limiter l'accès au gestionnaire de périphériques et sélectionner des groupes de périphériques, par exemple G1 et G2, dans OpenManage Enterprise utilisez `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
   - Observateur : `dxcua : [{"Role": "VE"}]`

2. Une fois que le client est enregistré dans Keycloak, dans la section Mappeurs, ajoutez un type de mappeur « Attribut d'utilisateur » avec les valeurs ci-dessous :
   - Nom : dxcua
   - Type de mappeur : attribut d'utilisateur
   - Attribut d'utilisateur : dxcua
   - Nom de la revendication de jeton : dxcua
   - Type de Json de revendication : chaîne
   - Ajouter à un jeton d'ID : activer
   - Ajouter au jeton d'accès : activer
   - Ajouter aux informations de l'utilisateur : activer

Test de l'état de l'enregistrement d'OpenManage Enterprise avec le fournisseur OpenID Connect

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect**, effectuez les opérations suivantes :

1. Sélectionnez un fournisseur OpenID Connect.
2. Dans le panneau de droite, cliquez sur **Tester l'état de l'enregistrement**.

   REMARQUE : Le test de connexion ne dépend pas du nom d'utilisateur et du mot de passe ou des informations de jeton d'accès initial, car il ne vérifie que la validité de l'URI de découverte.

L'état le plus récent de l'enregistrement (« Réussite » ou « Échec ») avec le fournisseur OIDC est mis à jour.

Modifier les informations d'un fournisseur OpenID Connect dans OpenManage Enterprise

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect**, effectuez les opérations suivantes :

1. Sélectionnez un fournisseur OpenID Connect.
2. Cliquez sur **Modifier** dans le volet de droite.
3. En fonction de l'état d'enregistrement du client du fournisseur OpenID Connect, vous pouvez effectuer les opérations suivantes :
   a. Si l'état de l'enregistrement est défini sur « Réussite », seules les cases à cocher de Validation de certification, Tester la connexion et Activé peuvent être modifiées.
   b. Si l'état de l'enregistrement est défini sur « Échec », vous pouvez modifier les cases à cocher Nom d'utilisateur, Mot de passe, Validation de certification, Tester la connexion et Activé.
4. Cliquez sur **Terminer** pour implémenter ou cliquez sur **Annuler** pour annuler vos modifications.

Activer les fournisseurs OpenID Connect

Si la connexion d'un fournisseur OpenID Connect n'était pas activée au moment où il a été ajouté à l'appliance, puis pour activer la connexion, vous devez l'activer dans l'appliance.

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect** , effectuez les opérations suivantes :

1. Sélectionnez le ou les fournisseurs OpenID Connect.
2. Cliquez sur **Activer**.

L'activation des fournisseurs OpenID Connect dans OpenManage Enterprise permet aux jetons d'accès client autorisés de se connecter à l'appliance.

Supprimer des fournisseurs OpenID Connect

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect**, effectuez les opérations suivantes :

1. Sélectionnez le ou les fournisseurs OpenID Connect.
2. Cliquez sur **Supprimer**.

Désactiver les fournisseurs OpenID Connect

Sur la page **Paramètres d'application** > **Utilisateurs** > **Fournisseurs OpenID Connect** , effectuez les opérations suivantes :

1. Sélectionnez le ou les fournisseurs OpenID Connect.
2. Cliquez sur **Désactiver**.

Le jeton d'accès client des fournisseurs OIDC désactivés sera rejeté par l'appliance.

Certificats de sécurité

En cliquant sur **Paramètre d'application SecuritéCertificats**, vous pouvez afficher les informations relatives au certificat SSL actuellement disponible pour le périphérique.

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Pour générer une requête de signature de certificat (RSC), voir Génération et téléchargement de la requête de signature de certificat , page 163.

Génération et téléchargement de la requête de signature de certificat

Pour générer une requête de signature de certificat (RSC) pour votre périphérique, puis faire une demande de certificat SSL :

REMARQUE : Vous devez générer la RSC depuis l'appliance OpenManage Enterprise uniquement.

1. Cliquez sur **Générer une requête de signature de certificat**.
2. Dans la boîte de dialogue **Générer une requête de signature de certificat**, entrez les informations dans les champs.
3. Cliquez sur **Générer**.
   Une RSC est créée et s'affiche dans la boîte de dialogue **Requête de signature de certificat**. Une copie de la RSC est également envoyée à l'adresse e-mail que vous avez fournie dans votre demande.
4. Dans la boîte de dialogue **Requête de signature de certificat**, copiez les données de la RSC et remettez-les à l'autorité de certification (AC) lors de la demande d'un certificat SSL.
   - Pour télécharger la RSC, cliquez sur **Télécharger la requête de signature de certificat**.
   - Cliquez sur **Terminer**.

Attribution d'un certificat WebServer à OpenManage Enterprise à l'aide des services de certificats Microsoft

1. Générez et téléchargez la Demande de signature de certificat (CSR) dans OpenManage Enterprise. Voir Génération et téléchargement de la requête de signature de certificat , page 163
2. Ouvrez une session Web sur le serveur de certification (https://x.x.x.x/certsrv), puis cliquez sur le lien **Demander un certificat**.
3. Sur la page Demander un certificat, cliquez sur le lien **Envoyer une demande de certificat avancée**.
4. Sur la page Demande de certificat avancée, cliquez sur **Envoyer une demande de certificat à l'aide d'un fichier CMC ou PKCS#10 codé en base 64 ou envoyer une demande de renouvellement à l'aide d'un lien de fichier PKCS#7 codé en base 64**.
5. Sur la page Envoyer une demande de certificat ou une demande de renouvellement, procédez comme suit :
   a. Dans le champ **Demande de certificat codé en base 64 (fichier CMC ou PKCS#10 ou PKCS#7)**, copiez et collez l'intégralité du contenu de la CSR téléchargé.
   b. Dans **Modèle de certificat** , sélectionnez **Serveur Web**.
   c. Cliquez sur **Envoyer** pour émettre un certificat.
6. Sur la page Certificat émis, sélectionnez l'option **Codé en base 64**, puis cliquez sur le lien **Télécharger le certificat** pour télécharger le certificat.
7. Téléchargez le certificat dans OpenManage en accédant à la page **Paramètres de,l'application** > **Sécurité** > **Certificats**, puis en cliquant sur **Télécharger**.

Gestion des préférences de la console

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

En cliquant sur **OpenManage Enterprise** > **Paramètres d'application** > **Préférences de la console**, vous pouvez définir les propriétés par défaut de l'interface graphique utilisateur d'OpenManage Enterprise. Par exemple, le délai par défaut après lequel l'intégrité d'un dispositif est automatiquement vérifiée et mise à jour sur le tableau de bord, et les paramètres préférés utilisés pour détecter un périphérique. Les options suivantes sont disponibles :

1. **Paramètres de rapport** : pour définir le nombre maximal de lignes que vous pouvez afficher dans les rapports OpenManage Enterprise :
   a. Développez **Paramètres de rapport**.
   b. Entrez un nombre dans la zone **Nombre limite de lignes des rapports**. La limite par défaut est définie sur 1 000 lignes. Toutefois, le nombre maximal de lignes autorisées est de 2 milliards.
   c. Cliquez sur **Appliquer**. Une tâche est exécutée et le paramètre est appliqué.
2. **Intégrité du périphérique** : pour définir le délai au terme duquel l'intégrité des périphériques doit être automatiquement surveillée et mise à jour dans le tableau de bord OpenManage Enterprise :
   a. Développez **Intégrité du périphérique**.
   b. Entrez la fréquence à laquelle l'intégrité du périphérique doit être enregistrée et les données stockées.
   c. Sélectionnez :
      - **Dernière connue** : affiche la dernière intégrité de périphérique enregistrée lorsque la connexion électrique a été perdue.
      - **Inconnue** : affiche la dernière intégrité de périphérique enregistrée lorsque l'état du périphérique est devenu « Inconnu ». OpenManage Enterprise cesse de reconnaître un périphérique lorsque la connexion à iDRAC est perdue et que le périphérique n'est plus surveillé par OpenManage Enterprise.
   d. Cliquez sur **Appliquer** pour enregistrer les modifications apportées aux paramètres ou sur **Abandonner** pour réinitialiser les valeurs par défaut.
3. **Paramètres de détection** : à développer pour définir la dénomination des périphériques utilisée par OpenManage Enterprise pour identifier les iDRAC et autres périphériques détectés à l'aide des paramètres **Dénomination des appareils serveurs** et **Dénomination des appareils généraux**.

   REMARQUE : Les choix de dénomination des appareils dans les paramètres Dénomination des appareils serveurs et Dénomination des appareils généraux sont indépendants l'un de l'autre et n'ont pas d'incidence l'un sur l'autre.

   a. Le paramètre **Dénomination des appareils généraux** s'applique à tous les appareils détectés autres que les iDRAC. Sélectionnez l'un des modes de dénomination suivants :
      - **DNS** pour utiliser le nom DNS.
      - **Instrumentation (NetBIOS)** pour utiliser le nom NetBIOS.

      REMARQUE :
      - Le paramètre par défaut pour la dénomination d'appareils généraux est **DNS**.
      - Si l'un des appareils découverts n'a pas de nom DNS ou NetBIOS correspondant au paramètre, l'appliance identifie ces types d'appareils à l'aide de leurs adresses IP.
      - Lorsque l'option **Instrumentation (NetBIOS)** est sélectionnée dans le paramètre **Dénomination des appareils généraux**, le **Nom du châssis** des appareils de châssis s'affiche comme le nom de l'appareil sur la page Tous les appareils.

   b. La **Dénomination des appareils serveurs** s'applique uniquement aux iDRAC. Sélectionnez l'un des modes de dénomination suivants pour les iDRAC détectés :
      - **Nom d'hôte iDRAC** pour utiliser le nom d'hôte de l'iDRAC.
      - **Nom d'hôte du système** pour utiliser le nom d'hôte du système.

      REMARQUE :
      - La préférence par défaut de dénomination des appareils iDRAC est le **nom d'hôte du système**.
      - Si l'un des iDRAC n'a pas de nom d'hôte d'iDRAC ou de système correspondant au paramètre, l'appliance identifie ces iDRAC à l'aide de leurs adresses IP.

   c. Pour indiquer les noms d'hôte de périphériques non valides et les adresses MAC communes, développez **Paramètres avancés** :
      i. Saisissez au moins un nom d'hôte non valide (si vous en indiquez plusieurs, séparez-les par une virgule) dans **Nom d'hôte d'appareil non valide**. Par défaut, la liste des noms d'hôte de périphérique non valides est remplie.
      ii. Entrez les adresses MAC courantes séparées par une virgule dans **Adresses MAC courantes**. Par défaut, la liste des adresses MAC courantes est remplie.
   d. Cliquez sur **Appliquer** pour enregistrer les modifications apportées aux paramètres ou sur **Abandonner** pour réinitialiser les valeurs par défaut.

4. **Détection initiée par serveur** : sélectionnez l'une des stratégies d'approbation de détection suivantes :
   - **Automatique** : pour permettre aux serveurs dotés du firmware iDRAC 4.00.00.00, qui se trouvent sur le même réseau que la console, d'être détectés automatiquement par la console.
   - **Manuelle** : pour que les serveurs soient détectés manuellement par l'utilisateur.
   - Cliquez sur **Appliquer** pour enregistrer les modifications ou sur **Abandonner** pour réinitialiser les valeurs par défaut.
5. **Préférences d'intégration du châssis MX7000** : spécifiez l'un des comportements de transfert d'alertes suivants sur le châssis MX7000 lors de son intégration :
   - Recevoir toutes les alertes
   - Recevoir les alertes de la catégorie « châssis » uniquement
6. **Paramètres SMB** : sélectionnez l'une des versions Server Message Block (SMB) à utiliser pour la communication réseau :
   - **Désactiver V1** : SMBv1 est désactivé. Il s'agit de la sélection par défaut dans l'appliance.
   - **Activer V1** : pour activer SMBv1.

   REMARQUE : Assurez-vous d'activer SMBv1 dans les **Paramètres SMB** avant de commencer toute tâche exigeant une communication avec des châssis ou serveurs PowerEdge YX2X et YX3X dotés d'iDRAC version 2.50.50.50 et versions antérieures. Pour en savoir plus, voir Gestion des préférences de la console , page 164 et Convention de dénomination générique pour les serveurs Dell EMC PowerEdge , page 185.
7. **Paramètres de l'expéditeur de l'e-mail** : pour définir l'adresse de l'utilisateur qui envoie un e-mail :
   a. Saisissez une adresse e-mail dans la zone **ID de l'e-mail de l'expéditeur**.
   b. Cliquez sur **Appliquer** pour enregistrer les modifications ou sur **Abandonner** pour réinitialiser les valeurs par défaut.
8. **Format de transfert des interruptions** : pour définir le format de transfert des interruptions, procédez comme suit :
   a. Sélectionnez l'une des options suivantes :
      - **Format d'origine (valide pour les traps SNMP uniquement)** : pour conserver les données des interruptions en l'état.
      - **Normalisé (valide pour tous les événements)** : pour normaliser les données des interruptions. Lorsque le format de transfert des interruptions est défini sur « Normalisé », l'agent de réception, tel que le journal syslog, reçoit une balise contenant l'adresse IP du périphérique à partir de laquelle l'alerte a été transférée.
   b. Cliquez sur **Appliquer** pour enregistrer les modifications ou sur **Abandonner** pour réinitialiser les valeurs par défaut.
9. **Paramètres de collecte des mesures** : pour définir la fréquence de la maintenance et de la purge des données de l'extension PowerManager, procédez comme suit :
   a. Dans la zone **Intervalle de purge des données**, saisissez la fréquence de suppression des données de PowerManager. Vous pouvez saisir des valeurs comprises entre 30 et 365 jours.
   b. Cliquez sur **Appliquer** pour enregistrer les modifications ou sur **Abandonner** pour réinitialiser les paramètres aux valeurs par défaut.

Définition des propriétés de sécurité de connexion

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

REMARQUE : les utilisateurs des répertoires AD et LDAP peuvent être importés et attribués à l'un des rôles d'OpenManage Enterprise (Admin, Gestionnaire de périphériques ou Observateur).

En cliquant sur **OpenManage Enterprise** > **Paramètres d'application** > **Sécurité**, vous pouvez sécuriser votre OpenManage Enterprise soit en spécifiant la **Limitation de la plage d'adresses IP autorisées**, soit via une **Politique de verrouillage de la connexion**.

- Développez **Limitation de la plage d'adresses autorisées** :

  REMARQUE : Lorsque la « Limitation de la plage d'adresses autorisées » est configurée dans l'appliance, toute connexion entrante à l'appliance, comme la réception des alertes, la mise à jour du firmware et les identités réseau, est bloquée pour les périphériques qui se trouvent en dehors de la plage donnée. Toutefois, toute connexion sortante de l'appliance fonctionnera sur tous les périphériques.

  1. Pour spécifier la plage d'adresses IP qui doit être autorisée à accéder à OpenManage Enterprise, cochez la case **Activer la plage IP**.
  2. Dans la zone **Plage d'adresses IP (CIDR)**, saisissez la plage des adresses IP.

     REMARQUE : Une seule plage d'adresses IP est autorisée.
  3. Cliquez sur **Appliquer**. Pour réinitialiser les paramètres par défaut des propriétés, cliquez sur **Annuler**.

     REMARQUE : Le bouton **Appliquer** ne sera pas activé si vous saisissez plusieurs plages d'adresses IP dans la zone **Plage d'adresses IP (CIDR)**.

- Développez **Politique de verrouillage de connexion** :
  1. Cochez la case **Par nom d'utilisateur** pour éviter qu'un nom d'utilisateur spécifique ne se connecte à OpenManage Enterprise.
  2. Cochez la case **Par adresse IP** pour éviter qu'une adresse IP spécifique ne se connecte à OpenManage Enterprise.
  3. Dans la zone **Nombre d'échecs de verrouillage**, entrez le nombre de tentatives infructueuses au bout desquelles OpenManage Enterprise doit empêcher l'utilisateur d'essayer de s'identifier à nouveau. Valeur par défaut : 3 tentatives.
  4. Dans la zone **Fenêtre d'échec de verrouillage**, entrez la durée pour laquelle OpenManage Enterprise doit afficher des informations concernant une tentative infructueuse.
  5. Dans la zone **Temps de pénalité de verrouillage**, entrez la durée pendant laquelle l'utilisateur n'est plus autorisé à réessayer de se connecter après plusieurs tentatives infructueuses.
  6. Cliquez sur **Appliquer**. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Personnalisation de l'affichage des alertes

1. Cliquez sur **OpenManage Enterprise** > **Paramètres d'application>Alertes**, puis développez les **Paramètres d'affichage des alertes**.
2. Sélectionnez une des options suivantes :
   a. **Toutes** : pour activer l'affichage des alertes acquittées et non acquittées.
   b. **Non acquittées** : pour activer l'affichage des alertes non acquittées uniquement.

      REMARQUE : Par défaut, les **Paramètres d'affichage des alertes** sont définis sur **Non acquittées**.

   c. **Acquittées** : pour activer l'affichage des alertes acquittées uniquement.
3. Cliquez sur **Appliquer**.

   Les modifications apportées aux paramètres d'affichage des alertes sont susceptibles d'affecter les pages suivantes d'OpenManage Enterprise :
   - L'angle supérieur droit de toutes les pages d'OpenManage Enterprise. Voir Présentation de l'interface graphique d'OpenManage Enterprise–Tech Release , page 36.
   - La page Tableau de bord. Voir Surveillance des appareils à l'aide du tableau de bord OpenManage Enterprise , page 38.
   - La page Appareils. Voir Graphique circulaire , page 39.
   - Le tableau **Journal des alertes** situé sous la page Alertes. Voir Affichage des journaux d'alertes , page 118.

Configuration des alertes SMTP, SNMP et Syslog

En cliquant sur **OpenManage Enterprise** > **Paramètres de l'application** > **Alertes**, vous pouvez configurer l'adresse e-mail (SMTP) qui reçoit les alertes système, les destinations de transfert des alertes SNMP et les propriétés de transfert Syslog. Pour gérer ces paramètres, vous devez disposer d'informations d'identification OpenManage Enterprise de niveau administrateur.

Pour configurer et authentifier le serveur SMTP qui gère la communication par e-mail entre les utilisateurs et OpenManage Enterprise :

REMARQUE : OpenManage Enterprise ne peut pas envoyer d'e-mail à un serveur SMTP interne disposant d'un certificat émis par une autorité de certification racine interne.

1. Développez **Configuration des e-mails**.
2. Saisissez l'adresse réseau du serveur SMTP qui envoie les e-mails.
3. Pour authentifier le serveur SMTP, cochez la case **Activer l'authentification** et saisissez le nom d'utilisateur et le mot de passe.
4. Par défaut, le numéro de port SMTP à atteindre est 25. Si nécessaire, modifiez-le.
5. Cochez la case **Utiliser SSL** pour sécuriser votre transaction SMTP.
6. Pour vérifier si le serveur SMTP fonctionne correctement, cliquez sur la case à cocher **Envoyer un e-mail test** et saisissez un **Destinataire d'e-mail**.
7. Cliquez sur **Appliquer**.
8. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Pour configurer le transfert des alertes SNMP :

1. Développez **Configuration du transfert des alertes SNMP**.
2. Cochez la case **ACTIVÉ** pour activer les interruptions SNMP respectives afin d'envoyer des alertes en cas d'événements prédéfinis.
3. Dans la zone **ADRESSE DE DESTINATION**, saisissez l'adresse IP du périphérique de destination qui doit recevoir l'alerte.

   REMARQUE : La saisie de l'adresse IP de la console n'est pas autorisée pour éviter la duplication des alertes.

4. Dans le menu **VERSION SNMP**, sélectionnez le type de version SNMP : SNMPv1, SNMPv2 ou SNMPv3 et renseignez les champs suivants :
   a. Dans la zone CHAÎNE DE COMMUNAUTÉ, saisissez la chaîne de la communauté SNMP du périphérique qui doit recevoir l'alerte.
   b. Si nécessaire, modifiez le NUMÉRO DE PORT. Le numéro de port par défaut pour les interruptions SNMP est le 162. Voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
   c. Si SNMPv3 est sélectionné, fournissez les informations supplémentaires suivantes :
      i. NOM D'UTILISATEUR : fournissez un nom d'utilisateur.
      ii. TYPE D'AUTHENTIFICATION : dans la liste déroulante, sélectionnez SHA, MD_5 ou Aucun.
      iii. PHRASE SECRÈTE D'AUTHENTIFICATION : fournissez une phrase secrète d'authentification comportant au moins huit caractères.
      iv. TYPE DE CONFIDENTIALITÉ : dans la liste déroulante, sélectionnez DES, AES_128 ou Aucun.
      v. PHRASE SECRÈTE DE CONFIDENTIALITÉ : fournissez une phrase secrète de confidentialité contenant au moins huit caractères.
5. Pour tester un message SNMP, cliquez sur le bouton **Envoyer** de l'interruption correspondante.
6. Cliquez sur **Appliquer**. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Pour mettre à jour la configuration de transfert Syslog, procédez comme suit :

1. Développez **Configuration des transferts Syslog**.
2. Cochez la case pour activer la fonctionnalité Syslog sur le serveur respectif dans la colonne **SERVEUR**.
3. Dans la zone **NOM DE L'HÔTE/ADRESSE DE DESTINATION**, saisissez l'adresse IP du périphérique qui doit recevoir les messages Syslog.
4. Le numéro de port par défaut lorsque UDP est utilisé est le 514. Si nécessaire, modifiez-le, en saisissant ou en effectuant une sélection dans la zone. Voir Protocoles et ports pris en charge dans OpenManage Enterprise , page 32.
5. Cliquez sur **Appliquer**.
6. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

Gestion des alertes entrantes

REMARQUE : Pour exécuter des tâches sur OpenManage Enterprise, vous devez disposer des droits d'utilisateur nécessaires. Voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

En cliquant sur **OpenManage Enterprise** > **Paramètres d'application** > **Alertes entrantes**, vous pouvez configurer les propriétés TrapForward et définir l'utilisateur qui reçoit les alertes SNMPv3 entrantes.

- Pour définir les informations d'identification SNMP pour les alertes entrantes :

1. Cochez la case **Activation de SNMPV3**.
2. Cliquez sur **Informations d'identification**.
3. Dans la boîte de dialogue **Informations d'identification SNMP** :
   a. Dans la zone **Nom d'utilisateur**, entrez l'ID de connexion de l'utilisateur qui gère les paramètres OpenManage Enterprise.
   b. Dans le menu déroulant **Type d'authentification**, sélectionnez l'algorithme **SHA** ou **MD_5** comme type d'authentification.
   c. Dans la zone **Phrase secrète d'authentification**, entrez la phrase secrète concernant SHA ou MD_5 selon votre sélection.
   d. Dans le menu déroulant **Type de confidentialité**, sélectionnez DES ou AES_128 comme norme de chiffrement.
   e. Dans la zone **Phrase secrète de confidentialité**, entrez la phrase secrète en fonction de votre type de confidentialité.
   f. Cliquez sur **Enregistrer**.
4. Dans la case **Communauté**, entrez la chaîne de communauté qui recevra les interruptions SNMP.
5. Par défaut, le numéro de port SNMP pour les interruptions entrantes est 162. Modifiez le numéro de port.
6. Cliquez sur **Appliquer**.
   Les informations d'identification et paramètres SNMP sont enregistrés.
7. Pour réinitialiser les paramètres aux attributs par défaut, cliquez sur **Ignorer**.

   REMARQUE : Si les paramètres d'alerte SNMPv3 sont configurés avant la mise à niveau de l'appliance, vous devez reconfigurer les paramètres en fournissant le nom d'utilisateur, la phrase de passe d'authentification et la phrase de passe de confidentialité pour continuer à recevoir les alertes. Si le problème persiste, redémarrez les services à l'aide de l'interface texte utilisateur (TUI).

8. Cliquez sur **Appliquer** pour enregistrer les modifications ou sur **Abandonner** pour annuler.

Définition des informations d'identification SNMP

1. Cliquez sur **Informations d'identification**.
2. Dans la boîte de dialogue **Informations d'identification SNMP** :
   a. Dans la zone **Nom d'utilisateur**, entrez l'ID de connexion de l'utilisateur gérant les paramètres OpenManage Enterprise.
   b. Dans le menu déroulant **Type d'authentification**, sélectionnez l'algorithme **SHA** ou **MD_5** comme type d'authentification.
   c. Dans la zone **Phrase secrète d'authentification**, entrez la phrase secrète concernant SHA ou MD_5 selon votre sélection.
   d. Dans le menu déroulant **Type de confidentialité**, sélectionnez DES ou AES_128 comme norme de cryptage.
   e. Dans la zone **Phrase secrète de confidentialité**, entrez la phrase secrète en fonction de votre type de confidentialité.
3. Cliquez sur **Enregistrer**.

Gestion des paramètres de garantie

Les **Paramètres de garantie** déterminent l'affichage des statistiques concernant la garantie par OpenManage Enterprise sur le widget Alertes de la page d'accueil, le tableau d'affichage d'alertes sur toutes les pages, la page Garantie et les rapports.

Pour modifier les paramètres de garantie :

1. Cliquez sur **OpenManage Enterprise** > **Paramètres d'application** > **Garantie**
2. Cliquez sur **Paramètres de garantie** pour activer la boîte de dialogue.
3. Dans la case **Afficher un avertissement si les garanties expirent dans les X prochains jours**, saisissez le nombre de jours. Vous pouvez saisir une valeur de 0 à 1 000 (inclus). La valeur définie par défaut est 90 jours. Les garanties expirant en fonction de ce paramètre sont représentés par le message ⚠ dans le rapport et le widget.
4. Dans les options **Masquer les garanties expirées** vous pouvez sélectionner l'une des options suivantes :
   a. **Toutes** : pour masquer l'affichage de toutes les garanties « initiales », ainsi que les garanties « étendues » qui ont expiré.
   b. **Initiale uniquement** : pour masquer uniquement les garanties initiales qui ont expiré.
   c. **Aucune** : pour afficher toutes les garanties expirées.
5. Cliquez sur **Appliquer** ou **Abandonner** afin d'enregistrer les paramètres de garantie ou d'abandonner les modifications et de conserver les anciens paramètres.

Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles

À partir de la page **Console et plug-ins,** vous pouvez vérifier et mettre à jour la version d'OpenManage Enterprise, et installer et mettre à jour les plug-ins. Accédez à la page **Console et plug-ins**, cliquez sur **Paramètres de l'application** > **Console et plug-ins**.

Sur la page **Console et plug-ins**, vous pouvez effectuer les opérations suivantes :

- Afficher la version actuelle de votre OpenManage Enterprise, vérifier si des mises à jour sont disponibles, puis effectuer une mise à niveau vers une version plus récente. Vous pouvez cliquer sur le bouton **Paramètres de mise à jour** pour :
  - Choisir de rechercher les mises à jour automatiquement ou manuellement.
  - Choisir entre les modes Dell.com (En ligne) ou Partage réseau (Hors ligne) pour la mise à jour de l'appliance.

    Pour plus d'informations sur la mise à niveau à partir de dell.com ou d'un partage réseau, voir Configuration et mise à niveau d'OpenManage Enterprise à l'aide de la méthode en ligne , page 169 ou Configuration d'OpenManage Enterprise et mise à niveau hors ligne à l'aide d'un partage réseau , page 170 respectivement.

- Cliquez sur **Installer** en regard du plug-in que vous souhaitez installer pour améliorer les fonctionnalités de l'appliance. Pour plus d'informations sur l'installation des plug-ins, voir Plug-in

  REMARQUE :
  - La licence OpenManage Enterprise Advanced est requise pour que les plug-ins soient entièrement fonctionnels après l'installation. Pour plus d'informations sur les plug-ins, reportez-vous à la documentation correspondante, disponible sur le site de support technique Dell.
  - L'installation d'un plug-in sur OpenManage Enterprise entraîne le redémarrage des services de l'appliance.
- Une fois les plug-ins installés, vous pouvez effectuer les opérations suivantes :
  - Désactiver le plug-in. Voir Désactivation d'un plug-in , page 173
  - Activer le plug-in. Voir Activation d'un plug-in , page 173
  - Désinstaller le plug-in. Voir Désinstallation d'un plug-in , page 173

Recommandations de mise à niveau et conditions préalables

Les administrateurs doivent tenir compte des points suivants avant d'effectuer la mise à jour vers la dernière version :

- Prenez un snapshot de la machine virtuelle de la console, qui servira de sauvegarde en cas de problème inattendu. Prévoyez une interruption de service plus longue si nécessaire.
- Prévoyez au moins une heure pour le processus de mise à jour. Prévoyez plus de temps si vous devez télécharger la mise à jour via une connexion réseau lente.
- Assurez-vous qu'aucune tâche de configuration, de déploiement ou d'extension (plug-in) de périphériques n'est en cours ou prévue pendant l'interruption de service planifiée. Toutes les tâches ou règles actives ou planifiées sont interrompues sans autre avertissement lors de la mise à jour.
- Prévenez les autres utilisateurs de la console qu'une mise à jour imminente est planifiée.
- En cas d'échec de la mise à niveau, l'appliance redémarre. Il est recommandé de rétablir le snapshot de VM et de refaire une mise à niveau.

REMARQUE :

- Seules les versions 3.5 et ultérieures d'OpenManage Enterprise peuvent être directement mises à jour vers la version 3.7 en utilisant la méthode **Automatique** > **En ligne**.
- Les versions d'OpenManage Enterprise antérieures à la version 3.4, par exemple les versions 3.3.x et 3.2, doivent d'abord être mises à jour vers la version 3.4, puis vers la version 3.5 avant d'envisager une mise à niveau vers la version 3.7.
- La version OpenManage Enterprise—Tech Release doit d'abord être mise à niveau vers les versions 3.0 ou 3.1 d'OpenManage Enterprise.
- Lorsque vous mettez à jour OpenManage Enterprise avec plus de 8 000 périphériques détectés, la tâche de mise à jour dure deux à trois heures. Pendant ce temps, il se peut que les services ne répondent pas. Il est donc recommandé de redémarrer l'appliance de manière appropriée. Après le redémarrage, le fonctionnement normal de l'appliance est restauré.
- L'ajout d'une deuxième interface réseau ne doit être effectué qu'après l'exécution complète des tâches de mise à niveau post-console. Une tentative d'ajout d'une deuxième carte NIC alors que la tâche post-mise à niveau est en cours ne sera pas efficace.
- Vous pouvez vous connecter immédiatement après la mise à jour de l'appliance et vous n'avez pas besoin d'attendre que l'inventaire soit totalement effectué. Après la mise à jour, la tâche de découverte s'exécute en arrière-plan et vous pouvez voir occasionnellement sa progression.
- Cliquer sur **Mettre à jour** lancerait une tâche de téléchargement de l'offre groupée de mise à niveau. Cette tâche se termine automatiquement une fois que tous les fichiers de mise à jour ont été téléchargés, et vous ne pouvez pas l'interrompre.
- Après la mise à niveau d'OpenManage Enterprise vers la version 3.7, les utilisateurs du Gestionnaire de périphériques migré possèdent un périmètre illimité et ont accès à tous les périphériques par défaut. Si nécessaire, les administrateurs peuvent attribuer des périmètres selon les besoins à l'aide de la fonctionnalité SBAC. Pour plus d'informations sur la fonctionnalité SBAC, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.

Configuration et mise à niveau d'OpenManage Enterprise à l'aide de la méthode en ligne

Vous pouvez mettre à niveau OpenManage Enterprise en ligne, de manière automatique ou manuelle, à partir de Dell.com (https://downloads.dell.com/openmanage_enterprise).

- Vous devez disposer de privilèges d'administration pour exécuter la mise à niveau. Pour plus d'informations sur les privilèges, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Assurez-vous que l'appliance OpenManage Enterprise peut accéder à Dell.com et à la mise à jour prévue.

La mise à niveau d'OpenManage Enterprise est un processus en deux étapes. Tout d'abord, Configuration de l'appliance pour la mise à jour en ligne , page 170 pour spécifier comment obtenir les mises à jour et la méthode associée, puis Mise à niveau d'OpenManage Enterprise à l'aide de la méthode en ligne , page 170 à partir de la page Console et plug-ins. La configuration des paramètres de mise à jour est un processus unique. Une fois les paramètres de mise à jour configurés, vous pouvez cliquer sur l'icône Actualiser dans la section Mise à jour pour voir si une version mise à jour peut être téléchargée.

Configuration de l'appliance pour la mise à jour en ligne

1. Cliquez sur **Paramètres de l'application** > **Console et extension** > **Paramètres de mise à jour**.
2. Dans **Comment rechercher des mises à jour**, sélectionnez l'une des options suivantes :
   - **Automatique** : l'appliance vérifie automatiquement la disponibilité des mises à jour tous les lundis dans la source spécifiée dans la zone **Où rechercher des mises à jour**.
   - **Manuelle :** l'utilisateur doit vérifier manuellement la disponibilité de la mise à jour à partir de la source spécifiée dans **Où rechercher des mises à jour** en cliquant sur l'icône Actualiser la liste dans la section Mises à jour de la page Console et plug-ins.
3. Dans **Où rechercher des mises à jour**, sélectionnez **dell.com** pour spécifier l'emplacement à partir duquel l'appliance recherchera les mises à jour.
4. Facultatif : Cochez la case **Démarrer automatiquement la mise à jour de la console à l'issue du téléchargement** pour lancer une installation de la mise à jour de la console dès la fin du téléchargement du package de mise à jour. Vous pouvez également lancer la mise à jour manuellement.
5. Cliquez sur **Appliquer**.

   L'appliance recherche les mises à jour directement à partir de https://downloads.dell.com/openmanage_enterprise.

Mise à jour de l'appliance à l'aide de la méthode en ligne

Mise à niveau d'OpenManage Enterprise à l'aide de la méthode en ligne

Avant de commencer la mise à jour à partir de dell.com, vérifiez les points suivants :

- Vérifiez que les paramètres de mise à jour sont configurés pour la mise à jour en ligne. Voir Configuration et mise à niveau d'OpenManage Enterprise à l'aide de la méthode en ligne , page 169.
- Assurez-vous d'avoir passé en revue toutes les conditions préalables et recommandations de mise à niveau, comme indiqué dans Recommandations de mise à niveau et conditions préalables , page 169.
- Veillez à prendre un snapshot de la machine virtuelle de la console, qui servira de sauvegarde en cas de problème inattendu. Prévoyez une interruption de service plus longue si nécessaire.

1. En fonction des paramètres de mise à jour, l'appliance vérifie la disponibilité d'une mise à jour et, si une nouvelle version est disponible, une bannière contenant les informations relatives à la nouvelle version de la mise à niveau s'affiche. Dans cette bannière, l'administrateur peut choisir d'ignorer la notification, d'être rappelé ultérieurement ou de cliquer sur **Afficher maintenant** pour obtenir des informations détaillées telles que la version et la taille des mises à jour disponibles sur la page **Paramètres d'application** > **Console et plug-ins**. La section OpenManage Enterprise de la page Console et plug-ins affiche toutes les nouvelles fonctionnalités et améliorations de la mise à jour disponible.
2. Cliquez sur **Mise à jour**, puis sur **Télécharger la console** pour télécharger le package à partir de la source spécifiée.

   REMARQUE :
   - Cliquez sur **Mettre à jour** pour lancer une tâche de téléchargement de l'offre groupée de mise à niveau. Cette tâche se termine automatiquement une fois que tous les fichiers de mise à jour ont été téléchargés et elle ne peut pas être arrêtée.
   - En cas d'échec de la mise à niveau, l'appliance redémarre. Il est recommandé de rétablir le snapshot de la machine virtuelle et d'effectuer une nouvelle mise à niveau.

3. Si la case **Démarrer automatiquement la mise à jour de la console à l'issue du téléchargement** est cochée dans les paramètres de mise à jour, la mise à niveau démarre automatiquement dès la fin du téléchargement du package de mise à jour. Sinon, cliquez sur **Mettre à jour la console** pour effectuer la mise à jour.

Configuration d'OpenManage Enterprise et mise à niveau hors ligne à l'aide d'un partage réseau

Vous devez configurer un partage réseau local et télécharger manuellement le package de mise à jour si vous n'êtes pas automatiquement connecté à Dell.com. Un journal d'audit est créé après chaque recherche manuelle de mise à jour.

Avant de commencer la mise à jour à partir d'un partage réseau :

- Vous devez disposer de privilèges d'administration pour exécuter la mise à niveau. Pour plus d'informations sur les privilèges, voir Contrôle d'accès basé sur les rôles et le périmètre dans OpenManage Enterprise , page 16.
- Assurez-vous que vous avez lu les recommandations générales de mise à niveau et les conditions préalables, comme indiqué dans Recommandations de mise à niveau et conditions préalables , page 169.

- Pour les mises à jour hors ligne (partage réseau), l'administrateur doit créer des structures de dossier appropriées selon la mise à niveau nécessaire (minimale ou complète), télécharger les fichiers applicables depuis https://downloads.dell.com et les enregistrer sur le partage réseau. Pour en savoir plus sur la mise à jour d'OpenManage Enterprise vers la dernière version et sur la structure des dossiers autorisée pour les mises à jour, consultez le livre blanc technique « Upgrade the Dell EMC OpenManage Enterprise appliance version » (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) sur le site de support.
- Prenez un snapshot de la machine virtuelle de la console, qui servira de sauvegarde en cas de problème inattendu. (Prévoyez une interruption de service plus longue pour cela si nécessaire.)
- En cas d'échec de la mise à niveau, l'appliance redémarre. Il est recommandé de rétablir le snapshot de VM et de refaire une mise à niveau.
- L'ajout d'une deuxième interface réseau ne doit être effectué qu'après l'exécution complète des tâches de mise à niveau post-console. Une tentative d'ajout d'une deuxième carte NIC alors que la tâche post-mise à niveau est en cours ne sera pas efficace.
- Assurez-vous que les certificats de sécurité sont signés par une autorité de certification tierce de confiance lorsque vous utilisez la méthode de mise à jour HTTPS.

REMARQUE :

- Les versions d'OpenManage Enterprise antérieures à la version 3.4, par exemple les versions 3.3x et 3.2, doivent d'abord être mises à jour vers la version 3.4, puis vers la version 3.5 avant d'envisager une mise à niveau vers la version 3.7 via un partage de fichiers réseau (NFS) partagé.
- La mise à jour directe vers la version OpenManage Enterprise—Tech Release n'est pas prise en charge. La version de Tech Release doit d'abord être mise à niveau vers la version 3.0 ou 3.1 d'OpenManage Enterprise.
- Lors de la mise à jour des partages locaux pour une mise à niveau manuelle des versions sans extensions/plug-in installés (par exemple, 3.1 et 3.2), le journal d'audit affiche des entrées d'avertissement telles que : « Impossible de récupérer le fichier source de type Extension Catalog car le fichier n'existe pas » et « Échec de l'état du téléchargement d'Extension Catalog ». Ces messages d'erreur n'ont pas d'impact fonctionnel sur le processus de mise à niveau et peuvent être ignorés.

La mise à niveau d'OpenManage Enterprise à partir d'un partage réseau est un processus en deux étapes. Tout d'abord, Configuration de l'appliance pour la mise à jour à partir d'un partage réseau , page 171 pour spécifier comment obtenir les mises à jour et la méthode associée, puis Mise à jour de l'appliance à partir d'un partage réseau , page 171 à partir de la page Console et plug-ins.

Configuration de l'appliance pour la mise à jour à partir d'un partage réseau

1. Téléchargez les fichiers correspondants à partir de https://downloads.dell.com et enregistrez-les sur un partage réseau conservant la même structure de dossiers et auquel la console peut accéder.

   Pour en savoir plus sur la mise à jour d'OpenManage Enterprise vers la dernière version et sur la structure des dossiers autorisée pour les mises à jour, consultez le livre blanc technique « Upgrade the Dell EMC OpenManage Enterprise appliance version » (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) sur le site de support.
2. Cliquez sur **Paramètres de l'application** > **Console et extension** > **Paramètres de mise à jour**.
3. Dans **Comment rechercher des mises à jour**, sélectionnez l'une des options suivantes :
   - **Automatique** : l'appliance vérifie automatiquement la disponibilité des mises à jour tous les lundis dans la source spécifiée dans la zone **Où rechercher des mises à jour**.
   - **Manuelle :** l'utilisateur doit vérifier manuellement la disponibilité de la mise à jour à partir de la source spécifiée dans **Où rechercher des mises à jour** en cliquant sur l'icône Actualiser la liste dans la section Mises à jour de la page Console et plug-ins.
4. Dans **Où rechercher des mises à jour**, sélectionnez l'option **Partage réseau** pour spécifier l'emplacement à partir duquel l'appliance recherchera les mises à jour.
   a. Dans **Chemin local**, spécifiez un chemin NFS, HTTP ou HTTPS contenant les fichiers téléchargés. Le format d'un partage réseau est le suivant : `nfs://<IP Address>/<Folder_Name>, http://<IP Address>/<Folder_Name>, or https://<IP Address>/<Folder_Name>`.
   b. Pour vérifier la connexion au partage réseau spécifié, cliquez sur **Tester maintenant**.
5. Facultatif : Cochez la case **Démarrer automatiquement la mise à jour de la console à l'issue du téléchargement** pour lancer une installation de la mise à jour de la console dès la fin du téléchargement du package de mise à jour. Vous pouvez également lancer la mise à jour manuellement.
6. Cliquez sur **Appliquer**.

Mise à jour de l'appliance à partir d'un partage réseau

- Assurez-vous que vous avez lu les conditions préalables et les recommandations mentionnées dans Recommandations de mise à niveau et conditions préalables , page 169.
- Vérifiez que les paramètres de mise à jour sont configurés pour la mise à jour à partir d'un partage réseau. Voir *Configuration de l'appliance pour la mise à jour à partir d'un partage réseau*.

1. En fonction des paramètres de mise à jour, l'appliance vérifie la disponibilité d'une mise à jour et, si une nouvelle version est disponible, une bannière contenant les informations relatives à la nouvelle version de la mise à niveau s'affiche. Dans cette bannière, l'administrateur peut choisir d'ignorer la notification et d'être rappelé ultérieurement, ou cliquer sur **Afficher maintenant** pour obtenir des informations détaillées telles que la version et la taille des mises à jour disponibles sur la page **Paramètres d'application** > **Console et plug-ins**. La section OpenManage Enterprise de la page Console et plug-ins affiche toutes les nouvelles fonctionnalités et améliorations de la mise à jour disponible.
2. Cliquez sur **Mise à jour**, puis sur **Télécharger la console** pour télécharger le package à partir de la source spécifiée.

   REMARQUE :
   - Cliquez sur **Mettre à jour** pour lancer une tâche de téléchargement de l'offre groupée de mise à niveau. Cette tâche se termine automatiquement une fois que tous les fichiers de mise à jour ont été téléchargés et elle ne peut pas être arrêtée.
   - Si le téléchargement de la mise à jour rencontre un problème lors de la connexion via le proxy, décochez les paramètres de proxy, puis réessayez de la télécharger.

3. Si la case **Démarrer automatiquement la mise à jour de la console à l'issue du téléchargement** est cochée dans les paramètres de mise à jour, la mise à niveau démarre automatiquement dès la fin du téléchargement du package de mise à jour. Sinon, cliquez sur **Mettre à jour la console** pour effectuer la mise à jour.

Connectez-vous après avoir procédé à la mise à jour et confirmez que le produit fonctionne comme prévu. Vérifiez si le journal d'audit contient des avertissements ou des erreurs liés à la mise à jour. S'il contient des erreurs, exportez le journal d'audit et enregistrez-le pour le support technique.

Une fois l'appliance mise à jour :
- Effacez le cache du navigateur. Si vous n'effacez pas le cache du navigateur, les nouvelles tâches risquent d'échouer après la mise à jour.
- Si vous effectuez une mise à niveau à partir d'OpenManage Enterprise version 3.1, il est recommandé de reconfigurer ou d'importer les groupes Active Directory pour optimiser les performances.
- Vous pouvez vous connecter immédiatement après la mise à jour de l'appliance et vous n'avez pas besoin d'attendre que l'inventaire soit totalement effectué. Après la mise à jour, la tâche de découverte s'exécute en arrière-plan et vous pouvez voir occasionnellement sa progression.

Installation d'un plug-in

Vous pouvez installer les plug-ins CloudIQ, Power Manager, OpenManage Enterprise Services (anciennement SupportAssist-Enterprise) et Update Manager en fonction de vos besoins afin d'améliorer les fonctionnalités d'OpenManage Enterprise.

- Pour installer les plug-in OpenManage Enterprise à partir de Dell.com, assurez-vous que l'appliance OpenManage Enterprise peut accéder à downloads.dell.com.
- Pour installer les plug-in OpenManage Enterprise à partir d'un partage réseau local, téléchargez manuellement le package sur votre partage réseau et mettez à jour le site sur la page Paramètres de mise à jour d'OpenManage Enterprise.

Pour plus d'informations sur la configuration des paramètres de mise à jour, reportez-vous à Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168.

REMARQUE : L'installation d'un plug-in sur OpenManage Enterprise entraîne le redémarrage des services de l'appliance.

Pour installer un plug-in, procédez comme suit :

1. Dans OpenManage Enterprise, cliquez sur **Paramètres de l'application** > **Console et plug-ins**.
   La page **Console et plug-ins** s'affiche.
2. Dans la section **Plug-ins**, cliquez sur **Installer** pour le plug-in que vous souhaitez installer.
   L'Assistant **Installation du plug-in** s'affiche.
3. Dans la liste **Version(s) disponible(s)**, sélectionnez la version que vous souhaitez installer.
4. Vérifiez la liste des conditions préalables mentionnées dans la section **Conditions préalables** pour vous assurer que vous les respectez, puis cliquez sur **Télécharger le plug-in**.

   REMARQUE : Les listes des conditions préalables changent lorsque vous sélectionnez la version du plug-in que vous souhaitez installer.

L'opération d'installation valide les conditions préalables à l'installation du plug-in. Si les conditions préalables à l'installation ne sont pas remplies, un message d'erreur approprié s'affiche.

Une fois le plug-in téléchargé, l'indicateur d'état affiché dans la partie supérieure du plug-in passe de **Disponible** à **Téléchargé**.

5. Pour installer le plug-in OpenManage Enterprise, dans l'Assistant **Installer le plug-in**, cliquez sur **Installer le plug-in**.
6. Un formulaire de consentement s'affiche pour vous informer du contrat de licence utilisateur final (EULA). Cliquez sur **Accepter** pour poursuivre l'installation du plug-in.
   Les informations sur le nombre d'utilisateurs connectés à OpenManage Enterprise, les tâches en cours et les tâches de planification sont affichées dans la boîte de dialogue de **confirmation**.
7. Pour confirmer l'installation, sélectionnez l'option **Je confirme avoir capturé le snapshot de l'appliance OpenManage Enterprise avant de procéder à l'installation du plug-in**, puis cliquez sur **Confirmer l'installation**.
   L'état de l'opération d'installation s'affiche. Une fois l'installation du plug-in réussie, l'indicateur d'état affiché dans la partie supérieure de la section du plug-in passe de **Disponible** ou **Téléchargé** à **Installé**.

Désactivation d'un plug-in

Désactive toutes les fonctionnalités du plug-in sur OpenManage Enterprise.

REMARQUE : La désactivation d'un plug-in sur OpenManage Enterprise entraîne le redémarrage des services de l'appliance.

1. Dans OpenManage Enterprise, cliquez sur **Paramètres de l'application** > **Console et plug-ins**.
   L'onglet **Console et plug-ins** s'affiche.
2. Dans la section **Plug-ins**, cliquez sur **Désactiver** pour le plug-in que vous souhaitez désactiver.
   L'Assistant **Désactiver le plug-in** s'affiche.
3. Pour désactiver le plug-in, cliquez sur **Désactiver le plug-in**.
   Les informations sur le nombre d'utilisateurs connectés à OpenManage Enterprise, les tâches en cours et les tâches de planification sont affichées dans la boîte de dialogue de **confirmation**.
4. Pour confirmer, sélectionnez l'option **Je confirme avoir capturé le snapshot de l'appliance OpenManage Enterprise avant de procéder à l'installation du plug-in.**, puis cliquez sur **Confirmer la désactivation**.

REMARQUE : Après avoir désactivé le plug-in, vous ne pouvez plus voir les informations ou les pages associées au plug-in sur OpenManage Enterprise.

Désinstallation d'un plug-in

Désinstalle et supprime toutes les données collectées par le plug-in.

1. Dans OpenManage Enterprise, cliquez sur **Paramètres de l'application** > **Console et plug-ins**.
   L'onglet **Console et plug-ins** s'affiche.
2. Dans la section **Plug-ins**, cliquez sur **Désinstaller** pour le plug-in que vous souhaitez désinstaller.
   L'Assistant **Désinstaller le plug-in** s'affiche.
3. Pour désinstaller le plug-in d'OpenManage Enterprise, cliquez sur **Désinstaller le plug-in**.
   Les informations sur le nombre d'utilisateurs connectés à OpenManage Enterprise, les tâches en cours et les tâches de planification sont affichées dans la boîte de dialogue de **confirmation**.
4. Pour confirmer la désinstallation, sélectionnez l'option **Je confirme avoir capturé le snapshot de l'appliance OpenManage Enterprise avant de procéder à l'installation du plug-in.**, puis cliquez sur **Confirmer la désinstallation**.

Toutes les fonctionnalités et données associées au plug-in seront désinstallées.

Activation d'un plug-in

Toutes les pages du plug-in s'affichent sous OpenManage Enterprise et la fonctionnalité de plug-in est activée sous OpenManage Enterprise.

REMARQUE : L'activation d'un plug-in sur OpenManage Enterprise entraîne le redémarrage des services de l'appliance.

1. Dans OpenManage Enterprise, cliquez sur **Paramètres de l'application** > **Console et plug-ins**.
   L'onglet **Console et plug-ins** s'affiche.
2. Dans la section **Plug-ins**, cliquez sur **Activer** pour le plug-in que vous souhaitez activer.
   L'Assistant **Activer le plug-in** s'affiche.

3. Pour activer le plug-in, cliquez sur **Activer le plug-in**.
   Les informations sur le nombre d'utilisateurs connectés à OpenManage Enterprise, les tâches en cours et les tâches de planification sont affichées dans la boîte de dialogue de **confirmation**.
4. Pour confirmer, sélectionnez l'option **Je confirme avoir capturé le snapshot de l'appliance OpenManage Enterprise avant de procéder à l'installation du plug-in.**, puis cliquez sur **Confirmer l'activation**.

Mise à jour d'un plug-in

En fonction des paramètres de mise à jour, l'appliance vérifie la disponibilité d'une mise à jour des plug-in installés. Si une nouvelle version est disponible, une bannière contenant les informations relatives à la nouvelle version de la mise à niveau s'affiche. Dans cette bannière, l'administrateur peut choisir d'ignorer la notification, d'être rappelé ultérieurement ou de cliquer sur **Afficher maintenant** pour obtenir des informations détaillées telles que la version et la taille des mises à jour disponibles sur la page **Paramètres d'application** > **Console et plug-ins**. La section Plug-in de la page Console et Plug-in affiche toutes les nouvelles fonctionnalités et améliorations de la mise à jour disponible.

Avant de mettre à jour un plug-in, assurez-vous que les paramètres de mise à jour sont configurés comme indiqué dans la section Vérification et mise à jour de la version d'OpenManage Enterprise et des plug-ins disponibles , page 168.

Pour mettre à jour un plug-in, procédez comme suit :

1. Dans la section Plug-in, cliquez sur **Mise à jour disponible** pour le plug-in que vous souhaitez mettre à jour.
   La page **Mettre à jour le plug-in** s'affiche.
2. Sélectionnez la version du plug-in, puis cliquez sur **Télécharger le plug-in**.
   Le plug-in est téléchargé et l'état du téléchargement s'affiche sur une bande de couleur verte.
3. Pour mettre à jour le plug-in, cliquez sur **Mettre à jour le plug-in**.
   Dans la fenêtre **Confirmation**, sélectionnez l'option **Je confirme avoir capturé le snapshot de l'appliance OpenManage Enterprise avant de procéder à la mise à jour du plug-in**, puis cliquez sur **Mettre à jour**.

Une fois l'opération de mise à jour terminée, la version s'affiche dans la section Plug-in.

Exécution des commandes et scripts distants

Lorsque vous obtenez une interruption SNMP, vous pouvez exécuter un script sur OpenManage Enterprise. Cette opération configure une règle qui ouvre un ticket sur votre système de génération de tickets tiers à des fins de gestion des alertes. Vous pouvez créer et stocker un maximum de **quatre** commandes à distance.

REMARQUE : Les caractères spéciaux suivants ne sont pas pris en charge dans les paramètres RACADM et IPMI CLI : **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * et **'**.

1. Cliquez sur **Paramètres d'application** > **Exécution de script**.
2. Dans la section **Paramètres de commandes distantes**, procédez comme suit :
   a. Pour ajouter une commande à distance, cliquez sur **Créer**.
   b. Dans le champ **Nom de la commande**, saisissez le nom de la commande.
   c. Sélectionnez l'un des types de commande suivants :
      i. Script
      ii. RACADM
      iii. Outil IPMI
   d. Si vous sélectionnez **Script**, procédez comme suit :
      i. Dans la boîte de dialogue **Adresse IP**, saisissez l'adresse IP.
      ii. Sélectionnez la méthode d'authentification : **Mot de passe** ou **Clé SSH**.
      iii. Saisissez le **nom d'utilisateur** et le **mot de passe** ou la **clé SSH**.
      iv. Dans le champ **Commande**, saisissez les commandes.
         - Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.
         - La substitution de jeton dans les scripts est possible. Voir Substitution de jeton dans les scripts distants et la stratégie d'alerte , page 182
      v. Cliquez sur **Terminer**.
   e. Si vous sélectionnez **RACADM**, procédez comme suit :
      i. Dans le champ **Nom de la commande**, saisissez le nom de la commande.
      ii. Dans le champ **Commande**, saisissez les commandes. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.

iii. Cliquez sur **Terminer**.

f. Si vous sélectionnez **Outil IPMI**, procédez comme suit :

i. Dans le champ **Nom de la commande**, saisissez le nom de la commande.

ii. Dans le champ **Commande**, saisissez les commandes. Il est possible de saisir un maximum de 100 commandes, à raison d'une commande par ligne.

iii. Cliquez sur **Terminer**.

3. Pour modifier un paramètre d'une commande à distance, sélectionnez cette dernière, puis cliquez sur **Modifier**.
4. Pour supprimer un paramètre d'une commande à distance, sélectionnez cette dernière, puis cliquez sur **Supprimer**.

Paramètres d'OpenManage Mobile

OpenManage Mobile (OMM) est une application de gestion de systèmes qui vous permet d'effectuer en toute sécurité un sous-ensemble de tâches de surveillance et de résolution des datacenters sur une ou plusieurs consoles OpenManage Enterprise et/ou des iDRAC (integrated Dell Remote Access Controllers) à l'aide de votre périphérique Android ou iOS. OMM vous permet de :

- Recevoir des notifications d'alerte depuis OpenManage Enterprise.
- Afficher les informations relatives au groupe, au périphérique, aux alertes et au journal.
- Allumer/éteindre ou redémarrer un serveur.

Par défaut, les notifications Push sont activées pour toutes les alertes et les alertes critiques. Ce chapitre fournit des informations sur les paramètres OMM que vous pouvez configurer via la console OpenManage Enterprise. Il fournit également des informations nécessaires pour dépanner OMM.

REMARQUE : Pour plus d'informations sur l'installation et l'utilisation d'OMM, consultez le *Guide d'utilisation d'OpenManage Mobile* sur Dell.com/OpenManageManuals.

Tâches associées

Activation ou désactivation des notifications d'alerte pour OpenManage Mobile , page 175
Activation ou désactivation des abonnés à OpenManage Mobile , page 176
Suppression d'un abonné OpenManage Mobile , page 176
Affichage de l'état du service de notification d'alerte , page 177
Dépannage OpenManage Mobile , page 178

Information associée

Activation ou désactivation des notifications d'alerte pour OpenManage Mobile , page 175
Activation ou désactivation des abonnés à OpenManage Mobile , page 176
Dépannage OpenManage Mobile , page 178

Activation ou désactivation des notifications d'alerte pour OpenManage Mobile

Par défaut, OpenManage Enterprise est configuré pour envoyer des notifications d'alerte à l'application OpenManage Mobile. Cependant, les notifications d'alerte sont envoyées depuis OpenManage Enterprise uniquement lorsqu'un utilisateur d'OpenManage Mobile ajoute OpenManage Enterprise à l'application OpenManage Mobile.

REMARQUE : Les privilèges de l'administrateur sont requis pour l'activation ou la désactivation des notifications d'alerte pour OpenManage Mobile.

REMARQUE : Le serveur OpenManage Enterprise doit disposer d'un accès Internet (HTTPS) sortant pour qu'OpenManage Enterprise puisse envoyer des notifications d'alerte à OpenManage Mobile.

Pour activer ou désactiver les notifications d'alerte sur OpenManage Mobile depuis OpenManage Enterprise :

1. Cliquez sur **OpenManage Enterprise** > **Paramètres d'application** > **Mobiles**.
2. Cochez la case **Activer les notifications push**.
3. Cliquez sur **Appliquer**.

Tâches associées

Paramètres d'OpenManage Mobile , page 175

Information associée

Paramètres d'OpenManage Mobile , page 175
Suppression d'un abonné OpenManage Mobile , page 176

Activation ou désactivation des abonnés à OpenManage Mobile

Les cases de la colonne **Activé** dans la liste d'**Abonnés mobiles** vous permettent d'activer ou de désactiver la transmission des notifications d'alerte aux abonnés à OpenManage Mobile.

REMARQUE :

- Les privilèges de l'administrateur sont requis pour l'activation ou la désactivation d'abonnés OpenManage Mobile.
- Les abonnés OpenManage Mobile peuvent être désactivés automatiquement par OpenManage Enterprise si le service de notification push de leur prestataire de services mobiles indique que leur appareil est définitivement inaccessible.
- Même si des abonnés à OpenManage Mobile sont activés dans la liste d' **abonnés mobiles**, ils peuvent désactiver la réception des notifications d'alerte dans les paramètres d'application OpenManage Mobile.

Pour activer ou désactiver les notifications d'alerte des abonnés à OpenManage Mobile :

1. Cliquez sur **OpenManage Enterprise** > **Paramètres d'application** > **Mobiles**.
2. Pour les activer, cochez la case correspondante et cliquez sur **Activer**. Pour les désactiver, cochez la case et cliquez sur **Désactiver**. Vous pouvez sélectionner plusieurs abonnés simultanément.

Tâches associées

Paramètres d'OpenManage Mobile , page 175

Information associée

Paramètres d'OpenManage Mobile , page 175
Suppression d'un abonné OpenManage Mobile , page 176

Suppression d'un abonné OpenManage Mobile

Le fait de supprimer un abonné OpenManage Mobile entraîne la suppression de l'utilisateur de la liste des abonnés, ce qui empêche ce même utilisateur de recevoir des notifications d'alerte depuis la console OpenManage Enterprise. Cependant, l'utilisateur OpenManage Mobile peut être ultérieurement à nouveau abonné aux notifications d'alertes à partir de l'application OpenManage Mobile.

REMARQUE : Des privilèges de l'administrateur sont requis pour la suppression d'un abonné OpenManage Mobile.

Pour supprimer un abonné OpenManage Mobile :

1. Cliquez sur **OpenManage Enterprise** > **Paramètres d'application** > **Mobiles**.
2. Cochez la case correspondant au nom d'abonné, puis cliquez sur **Supprimer**.
3. Lorsque le programme vous invite à confirmer, cliquez sur **Oui**.

Tâches associées

Activation ou désactivation des notifications d'alerte pour OpenManage Mobile , page 175
Activation ou désactivation des abonnés à OpenManage Mobile , page 176
Suppression d'un abonné OpenManage Mobile , page 176
Affichage de l'état du service de notification d'alerte , page 177

Information associée

Paramètres d'OpenManage Mobile , page 175
Suppression d'un abonné OpenManage Mobile , page 176

Affichage de l'état du service de notification d'alerte

OpenManage Enterprise transfère des notifications d'alerte aux abonnés à OpenManage Mobile par l'intermédiaire du service de notification d'alertes correspondant de la plateforme du périphérique. Si l'abonné à OpenManage Mobile ne parvient pas à recevoir des notifications d'alerte, vous pouvez vérifier l' **état du service de notification** pour dépanner la livraison des notifications d'alerte.

Pour afficher la condition du service de notification d'alerte, cliquez sur **Paramètres de l'application** > **Mobiles**.

Tâches associées

Affichage de l'état du service de notification d'alerte , page 177

Information associée

Paramètres d'OpenManage Mobile , page 175
Suppression d'un abonné OpenManage Mobile , page 176
Affichage de l'état du service de notification d'alerte , page 177

État du service de notification

Le tableau suivant fournit des informations sur l'**État du service de notification** affiché à la page **Paramètres de l'application** > **Mobile**.

Tableau 29. État du service de notification

Icône d'état	Description de l'état
	Le service est en cours d'exécution et fonctionne normalement. **REMARQUE :** Cet état du service reflète uniquement les communications réussies avec le service de notification de la plate-forme. Si le périphérique de l'abonné n'est pas connecté à Internet ou à un service de données cellulaires, les notifications ne seront délivrées qu'une fois la connexion restaurée.
	Le service a rencontré une erreur lors de la livraison d'un message qui peut être de nature temporaire. Si le problème persiste, suivez les procédures de dépannage ou contactez le support technique.
	Le service a rencontré une erreur lors de la livraison d'un message. Suivez les procédures de dépannage ou contactez le support technique, au besoin.

Affichage d'informations sur les abonnés d'OpenManage Mobile

Suite à l'ajout réussi d'OpenManage Enterprise par un utilisateur OpenManage Mobile, l'utilisateur est ajouté au tableau d'**abonnés mobiles** dans OpenManage Enterprise. Pour afficher des informations à propos des abonnés mobiles, dans OpenManage Enterprise, cliquez sur **Paramètres d'application** > **Mobiles**.

Vous pouvez également exporter les informations à propos des abonnés mobiles vers un fichier .CSV en utilisant la liste déroulante **Exporter**.

Informations sur les abonnés OpenManage Mobile

Le tableau suivant fournit des informations sur le tableau **Abonnés mobiles** affiché à la page **Paramètres d'application** > **Mobiles**.

Tableau 30. Informations sur les abonnés OpenManage Mobile

Champ	Description
ACTIVÉ	Cochez ou décochez la case, puis cliquez sur **Activer** ou **Désactiver** respectivement pour activer ou désactiver les notifications d'alerte pour un abonné à OpenManage Mobile.
ÉTAT	Affiche la condition de l'abonné, indiquant si la console OpenManage Enterprise est en mesure ou non d'envoyer des notifications d'alerte au service de transfert des alertes.
MESSAGE DE CONDITION	Description de l'état du message d'état.
NOM D'UTILISATEUR	Nom de l'utilisateur d'OpenManage Mobile.
ID DE PÉRIFÉRIQUE	Identificateur unique du périphérique mobile.
DESCRIPTION	Description du périphérique mobile.
FILTRE	Les filtres sont des critères que l'abonné a configuré pour la notification des alertes.
DERNIÈRE ERREUR	Date et heure de la dernière erreur lors de l'envoi d'une notification d'alerte à l'utilisateur d'OpenManage Mobile.
DERNIER PUSH	Date et heure d'envoi réussi de la dernière notification d'alerte d'OpenManage Enterprise au service de transfert des alertes.
DERNIÈRE CONNEXION	Date et heure du dernier accès de l'utilisateur à la console OpenManage Enterprise via OpenManage Mobile.
ENREGISTREMENT	Date et heure auxquelles l'utilisateur a ajouté la console OpenManage Enterprise dans OpenManage Mobile.

Dépannage OpenManage Mobile

Si OpenManage Enterprise est incapable de s'enregistrer auprès du service de transfert de messages ou de transmettre des notifications, les résolutions suivantes sont disponibles :

Tableau 31. Dépannage OpenManage Mobile

Problème	Raison	Résolution
OpenManage Enterprise ne parvient pas à se connecter au service de transfert de messages Dell. [Code 1001/1002]	La connectivité Internet sortante (HTTPS) est perdue.	À l'aide d'un navigateur Web, vérifiez si une connectivité Internet sortante est disponible. Si la connexion est indisponible, exécutez les tâches de dépannage réseau suivantes : • Vérifiez si les câbles réseau sont connectés. • Vérifiez l'adresse IP et les paramètres du serveur DNS. • Vérifiez si le pare-feu est configuré pour autoriser le trafic sortant. • Vérifiez si le réseau de votre fournisseur d'accès Internet fonctionne normalement.
	Paramètres de proxy sont incorrects.	Définir l'hôte proxy, le port, le nom d'utilisateur et le mot de passe comme requis.
	Le service de transfert de messages est temporairement indisponible.	Attendez que le service redevienne disponible.

Tableau 31. Dépannage OpenManage Mobile (suite)

Problème	Raison	Résolution
Le service de transfert de messages ne parvient pas à se connecter au service de notification de la plateforme du périphérique. [Code 100-105, 200-202, 211-212]	Le service du fournisseur de plateforme est temporairement indisponible pour le service de transfert de messages.	Attendez que le service redevienne disponible.
Le jeton de communications du périphérique n'est plus enregistré auprès du service du fournisseur de plateforme. [Code 203]	L'application OpenManage Mobile a été mise à jour, restaurée, ou désinstallée, ou le système d'exploitation du périphérique a été mis à niveau ou restauré.	Réinstallez OpenManage Mobile sur le périphérique ou suivez les procédures de dépannage de OpenManage Mobile du *Guide d'utilisation d'OpenManage Mobile* et reconnectez le périphérique à OpenManage Enterprise. Si le périphérique n'est plus connecté à OpenManage Enterprise, supprimez l'abonné.
L'enregistrement d'OpenManage Enterprise est rejeté par le service de transfert de messages. [Code 154]	Une version obsolète de OpenManage Enterprise est en cours d'utilisation.	Effectuez une mise à niveau vers une version plus récente d'OpenManage Enterprise.

Tâches associées

Paramètres d'OpenManage Mobile , page 175

Information associée

Paramètres d'OpenManage Mobile , page 175

21

Autres références et descriptions de champ

Des définitions de certains champs s'affichant souvent dans l'interface graphique utilisateur d'OpenManage Enterprise sont répertoriées et expliquées dans ce chapitre. De plus, d'autres informations utiles sont également fournies ici pour référence.

Sujets :

Référence de planification

- **Mettre à jour maintenant** : la version du micrologiciel est mise à jour et associée à la version disponible sur le catalogue associé. Pour que la mise à jour soit effective au prochain redémarrage du périphérique, sélectionnez la case à cocher **Préparer pour le prochain redémarrage du serveur**.
- **Programmer plus tard** : sélectionnez cette option pour préciser la date et l'heure où la version du micrologiciel doit être mise à jour.

Définitions de champs de ligne de base du micrologiciel

- **CONFORMITÉ** : état d'intégrité de la configuration de base du micrologiciel. Même si un périphérique associé à une ligne de base du micrologiciel est dans un état d'intégrité critique, l'intégrité de la ligne de base est également définie comme critique. C'est ce qu'on appelle l'état d'intégrité cumulé, qui équivaut à l'état de la ligne de base présentant un haut degré de gravité. Pour plus d'informations sur l'état d'intégrité globale, voir le livre blanc *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (Gestion de l'état d'intégrité globale avec l'iDrac sur les serveurs PowerEdge de Dell EMC à partir de la 14ème génération) disponible sur le Dell TechCenter.
- **NOM** : nom de la ligne de base du micrologiciel. Cliquez ici pour afficher le rapport de conformité de la ligne de base sur la page **Rapport de conformité.** Pour plus d'informations sur la création d'une ligne de base de micrologiciel, voir Création d'une ligne de base de firmware/pilote , page 81.
- **Catalogue** : catalogue du micrologiciel auquel appartient la ligne de base du micrologiciel. Voir Gestion des catalogues de firmwares et de pilotes , page 78.
- **HEURE DE LA DERNIÈRE EXÉCUTION** : heure à laquelle le rapport de conformité de la ligne de base a été exécuté pour la dernière fois. Voir Vérification de la conformité d'un firmware et d'un pilote de périphérique , page 82.

Définitions de champs de tâche de planification

- **Exécuter maintenant** permet de commencer la tâche immédiatement.
- **Exécuter ultérieurement** permet de spécifier une date et une heure ultérieures.

- **Exécuter selon la planification** pour exécuter de manière répétée selon une fréquence sélectionnée. Sélectionnez **Tous les jours**, puis sélectionnez la fréquence appropriée.

REMARQUE : par défaut, l'horloge du planificateur de tâches est réinitialisée à 00:00 tous les jours. Le format cron ne prend pas en compte l'heure de création de la tâche lors du calcul de la fréquence de la tâche. Par exemple, si une tâche débute à 10:00 et doit s'exécuter une fois toutes les 10 heures, l'exécution suivante débutera à 20:00. Cependant, l'heure suivante n'est pas 06:00 le jour suivant mais 00:00. Cela est dû au fait que l'horloge du planificateur est réinitialisée à 00:00 tous les jours.

Catégories d'alerte après réaffectation d'EEMI

Tableau des réaffectations d'EEMI

Tableau 32. Catégories d'alerte dans OpenManage Enterprise

Catégorie précédente	Sous-catégorie précédente	Nouvelle catégorie	Nouvelle sous-catégorie
Audit	Périphériques	Intégrité du système	Périphériques
Audit	Périphériques	Configuration	Périphériques
Audit	Périphériques	Configuration	Périphériques
Audit	Périphériques	Configuration	Périphériques
Audit	Périphériques	Configuration	Périphériques
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Application	Configuration	Application
Audit	Périphériques	Audit	Utilisateurs
Audit	Modèles	Configuration	Modèles
Audit	Modèles	Configuration	Modèles
Audit	Modèles	Configuration	Modèles
Audit	Modèles	Configuration	Modèles
Audit	Modèles	Configuration	Modèles
Configuration	Inventaire	Configuration	Tâche
Configuration	Inventaire	Configuration	Tâche
Configuration	Inventaire	Configuration	Tâche
Configuration	Inventaire	Configuration	Périphériques
Configuration	Inventaire	Configuration	Périphériques
Configuration	Inventaire	Configuration	Périphériques
Configuration	Micrologiciel	Configuration	Tâches
Configuration	Micrologiciel	Configuration	Tâches
Divers	Tâches	Configuration	Tâches
Divers	Tâches	Configuration	Tâches
Divers	Tâches	Configuration	Tâches
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique

Tableau 32. Catégories d'alerte dans OpenManage Enterprise (suite)

Catégorie précédente	Sous-catégorie précédente	Nouvelle catégorie	Nouvelle sous-catégorie
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique
Divers	Générique	Configuration	Générique
Divers	Périphériques	Configuration	Périphériques
Divers	Périphériques	Configuration	Périphériques
Audit	Sécurité	Configuration	Sécurité
Audit	Sécurité	Configuration	Sécurité
Audit	Sécurité	Configuration	Sécurité

Substitution de jeton dans les scripts distants et la stratégie d'alerte

OpenManage Enterprise prend en charge l'utilisation des jetons pour améliorer la rédaction de scripts distants et la création de stratégies d'alerte.

Tableau 33. Jetons pris en charge dans OpenManage Enterprise

Jetons	Description
`$IP`	Adresse IP de l'appareil
`$MSG`	Message
`$DATE`	Date
`$TIME`	Heure
`$SEVERITY`	Gravité
`$SERVICETAG`	Numéro de série
`$RESOLUTION`	Résolution recommandée
`$CATEGORY`	Nom des catégories d'alertes
`$ASSETTAG`	Numéro d'inventaire
`$MODEL`	Nom du modèle
`$HOSTNAME`	Nom de domaine complet ou nom d'hôte (en l'absence de nom de domaine complet)

Flux de débogage sur le terrain

Dans OpenManage Enterprise, vous pouvez autoriser le débogage de la console à l'aide de l'option Field Service Debug (débogage sur le terrain, FSD).

L'option FSD permet de réaliser les tâches suivantes :

- Autoriser l'activation et la copie des journaux de débogage
- Autoriser la copie des journaux en temps réel
- Autoriser la sauvegarde ou la restauration de le base de données sur la machine virtuelle.

Les rubriques référencées dans chaque tâche fournissent des instructions détaillées. Pour activer l'option FSD, procédez comme suit :

1. Débloquez la fonctionnalité FSD. Voir la section Déblocage de la fonction FSD , page 183.
2. Installez ou fournissez un fichier FSD DAT.ini signé. Voir la section Installation ou octroi d'un fichier FSD DAT.ini signé , page 183.
3. Faites appel aux fonctions FSD. Voir la section Appel FSD , page 184.
4. Désactivez l'option FSD. Voir la section Désactivation de l'option FSD , page 184.

Déblocage de la fonction FSD

Vous pouvez débloquer la fonction FSD par le biais de l'interface TUI.

1. Accédez au menu principal de l'interface TUI.
2. Dans l'interface TUI, pour utiliser l'option FSD, sélectionnez **Activer le mode Field Service Debug (FSD)**.
3. Pour générer une nouvelle demande de déblocage de FSD, sur l'écran **Fonctions FSD**, sélectionnez **Débloquer les fonctions FSD**
4. Pour déterminer la durée des fonctions de débogage demandées, sélectionnez une date de début et une date de fin.
5. Sur l'écran **Choisir les fonctions de débogage demandées**, sélectionnez une fonction de débogage à partir d'une liste de fonctions de débogage propre à la console. Dans le coin inférieur droit, sélectionnez **Générer**.

   REMARQUE : La fonction de débogage qui est actuellement prise en charge est `RootShell`.

6. Sur l'écran **Télécharger un fichier .DAT**, affichez les instructions de signature et l'adresse URL du partage dans lequel se trouve le fichier .DAT.ini.
7. Utilisez un client externe pour extraire le fichier .DAT.ini de l'adresse URL du partage indiqué à l'étape 6.

   REMARQUE : Le répertoire de partage téléchargé possède des privilèges d'accès en lecture seule et ne prend en charge qu'un seul fichier .DAT.ini à la fois.

8. Effectuez l'une des tâches suivantes, selon que vous soyez un utilisateur de Dell EMC externe ou interne :
   - Envoyez le fichier .DAT.ini à un contact Dell EMC pour qu'il le signe si vous êtes un utilisateur externe.
   - Téléchargez le fichier .DAT.ini dans une Fonction d'authentification de Field Service Debug (FSDAF) Dell et envoyez-le.
9. Attendez qu'un fichier .DAT.ini signé et approuvé par Dell EMC soit renvoyé.

Installation ou octroi d'un fichier FSD DAT.ini signé

Assurez-vous que vous avez bien reçu le fichier DAT.ini, signé et approuvé par Dell EMC.

REMARQUE : Une fois que Dell EMC approuve le fichier DAT.ini, vous devez charger le fichier vers la console qui a généré la commande de déblocage d'origine.

1. Pour charger un fichier DAT.ini signé, sur l'écran **Fonctions FSD**, sélectionnez **Installer/Octroyer un fichier DAT FSD signé**.

   REMARQUE : Le répertoire de partage par chargement a des privilèges d'écriture seule et ne prend en charge qu'un seul fichier DAT.ini à la fois. La limite de taille de fichier DAT.ini est de 4 Ko.

2. Sur l'écran **Charger un fichier DAT signé**, suivez les instructions concernant le chargement du fichier DAT.ini vers une URL de partage de fichiers donnée.
3. Utilisez un client externe pour charger le fichier DAT.ini vers un emplacement de partage.
4. Sur l'écran **Charger un fichier DAT signé**, sélectionnez **J'ai chargé le fichier DAT FSD**.

S'il n'y a pas d'erreurs pendant le chargement du fichier DAT.ini, un message confirmant la réussite de l'installation du certificat s'affiche. Pour continuer, cliquez sur **OK**.

Le chargement du fichier DAT.ini peut échouer pour l'une des raisons suivantes :

- Le répertoire de partage par chargement n'a pas suffisamment d'espace disque libre.
- Le fichier DAT.ini chargé ne correspond pas à la requête de fonction de débogage précédente.
- La signature fournie par Dell EMC pour le fichier DAT.ini n'est pas valide.

Appel FSD

Assurez-vous que le fichier DAT.ini a été signé, renvoyé par Dell EMC et téléchargé sur OpenManage Enterprise.

1. Pour faire appel à une fonctionnalité de débogage, accédez à l'écran **Fonctions FSD**, puis sélectionnez **Appeler les fonctionnalités FSD**.
2. Sur l'écran **Appeler les fonctionnalités de débogage demandées**, sélectionnez une fonctionnalité de débogage à partir d'une liste approuvée dans le fichier DAT.ini signé par Dell EMC. Dans le coin inférieur droit, cliquez sur **Appeler**.

   REMARQUE : La fonctionnalité de débogage actuellement prise en charge est `RootShell`.

Lorsque la commande `invoke` est exécutée, OpenManage Enterprise peut démarrer un processus SSH. Le client SSH externe peut s'associer à OpenManage Enterprise à des fins de débogage.

Désactivation de l'option FSD

Après avoir appelé une fonction de débogage sur une console, la fonction FSD continue de fonctionner jusqu'à ce que la console redémarre ou que la fonction de débogage soit arrêtée. Sinon, la durée déterminée entre la date de début et la date de fin est dépassée.

1. Pour arrêter les fonctions de débogage, sur l'écran **Fonctions FSD**, sélectionnez **Désactiver les fonctions de débogage**.
2. Sur l'écran **Désactiver les fonctions de débogage appelées**, sélectionnez une ou plusieurs fonction(s) de débogage à partir d'une liste de fonctions de débogage actuellement appelées. Dans le coin inférieur droit de l'écran, sélectionnez **Désactiver**.

Assurez-vous d'avoir arrêté tous les démons ou sessions SSH qui utilisent actuellement la fonction de débogage.

Définitions des champs de la section Gestion du catalogue

NOM DU CATALOGUE : nom du catalogue. Les catalogues intégrés ne peuvent pas être modifiés.

TÉLÉCHARGER : indique l'état du téléchargement de catalogues depuis le dossier de sa logithèque. Les états disponibles sont les suivants : Terminé, En cours d'exécution et Échec.

LOGITHÈQUE : types de logithèque comme dell.com, CIFS et NFS.

EMPLACEMENT DE LA LOGITHÈQUE : emplacement où les catalogues sont enregistrés. Par exemple, dell.com, CIFS et NFS. Indique également l'état de l'achèvement d'une tâche s'exécutant sur le catalogue.

FICHIER DU CATALOGUE : type de fichier du catalogue.

DATE DE CRÉATION : date à laquelle le fichier de catalogue a été créé.

Rapports de ligne de base de conformité du firmware et du pilote : appareils dont l'état de conformité est « Inconnu »

L'état de conformité des firmwares ou des pilotes des appareils de stockage, réseau et d'infrastructure hyperconvergée (HCI) suivants dans les rapports de conformité de la ligne de base des firmwares et des pilotes s'affiche comme « Inconnu », car le catalogue des firmwares/pilotes Dell ne prend pas en charge les mises à jour logicielles ou des firmwares de ces appareils.

Tableau 34. Rapports de ligne de base de conformité des firmwares/pilotes : périphériques faussement conformes

Catégorie de périphérique	Liste des périphériques
Stockage	• SC-Series • MD Series • Série ME

Tableau 34. Rapports de ligne de base de conformité des firmwares/pilotes : périphériques faussement conformes (suite)

Catégorie de périphérique	Liste des périphériques
Périphériques réseau dans les châssis FX2, VRTX et M1000e	• Commutateurs F10 • IOA (agrégateurs d'entrée/de sortie) • IOM (Modules d'entrée/de sortie)
Appliances hyperconvergées (HCI)	• VXRail • Série XC
Périphériques pouvant être mis à jour à l'aide de Dell Update Package (DUP) du périphérique individuel, mais non directement pris en charge par le catalogue Dell	• Moteur de structure MX9116n • Commutateur Ethernet MX5108n • PowerEdge MX5000s
Périphériques qui ne peuvent pas être mis à jour à l'aide du catalogue Dell ou du DUP individuel **REMARQUE :** Pour la mise à jour du firmware/pilote de ces périphériques, veuillez vous reporter au Guide d'installation du périphérique.	• Module d'extension de structure MX7116n • PowerEdge MX 25 GbE PTM

REMARQUE : Pour obtenir la liste complète des périphériques des séries SC, MD, ME et XC, reportez-vous à https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Convention de dénomination générique pour les serveurs Dell EMC PowerEdge

Pour couvrir une gamme de modèles de serveur, les serveurs PowerEdge sont désormais nommés à l'aide de la convention de dénomination générique et non de leur génération.

Cette rubrique explique comment identifier la génération d'un serveur PowerEdge nommé à l'aide de la convention de dénomination générique.

Exemple :

Le modèle de serveur R740 est un système à deux processeurs à rack de la 14e génération de serveurs dotés de processeurs Intel. Dans la documentation, pour faire référence à R740, la convention de dénomination générique serveur **YX4X** est utilisée, où :

- La lettre **Y** (alphabet) est utilisée pour désigner les formats des serveurs suivants :
  - **C** = Cloud : nœuds de serveurs modulaires pour les environnements à grande échelle
  - **F** = flexible : traîneaux hybrides basés sur rack pour les boîtiers FX2/FX2s basés sur rack
  - **M** ou **MX*** = modulaire : serveurs lames pour les boîtiers modulaires MX7000, M1000e et/ou VRTX
  - **R** = serveurs montables en rack
  - **T** = serveurs tour
- La lettre **X** (chiffre) indique la classe (nombre de processeurs) du serveur.
- Le chiffre **4** indique la génération du serveur.
- La lettre **X** (chiffre) indique la marque du processeur.

Tableau 35. Convention de dénomination des serveurs PowerEdge et exemples

Serveurs YX3X	Système YX4X
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540