OpenManage Integration for Microsoft System Center version 7.1.1 pour System Center Configuration Manager et System Center Virtual Machine Manager

Guide d'utilisation

DELL EMC

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

2019 - 04

Rév. A00

Table des matières

1

Introduction to OMIMSSC

OpenManage Integration for Microsoft System Center (OMIMSSC) provides integration into System Center suite of products. OMIMSSC enables full lifecycle management of Dell EMC PowerEdge servers by using integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC), and of Modular Systems (Dell EMC PowerEdge MX7000) by using OpenManage Enterprise Modular Edition.

OMIMSSC offers operating system deployment, Storage Spaces Direct cluster creation, hardware patching, firmware update, and device maintenance. Integrate OMIMSSC with Microsoft System Center Configuration Manager (SCCM) for managing devices in traditional data center, or integrate OMIMSSC with Microsoft System Center Virtual Machine Manager (SCVMM) for managing devices in virtual and cloud environments.

For information about SCCM and SCVMM, see the Microsoft documentation.

Nouveautés

Prend en charge le type HTTPS (Hypertext Transfer Protocol Secure) de la source de mise à jour.

2

Use cases of OMIMSSC

This chapter covers high-level details for discovering, deploying operating system, creating clusters, and maintaining Dell EMC devices using OMIMSSC.

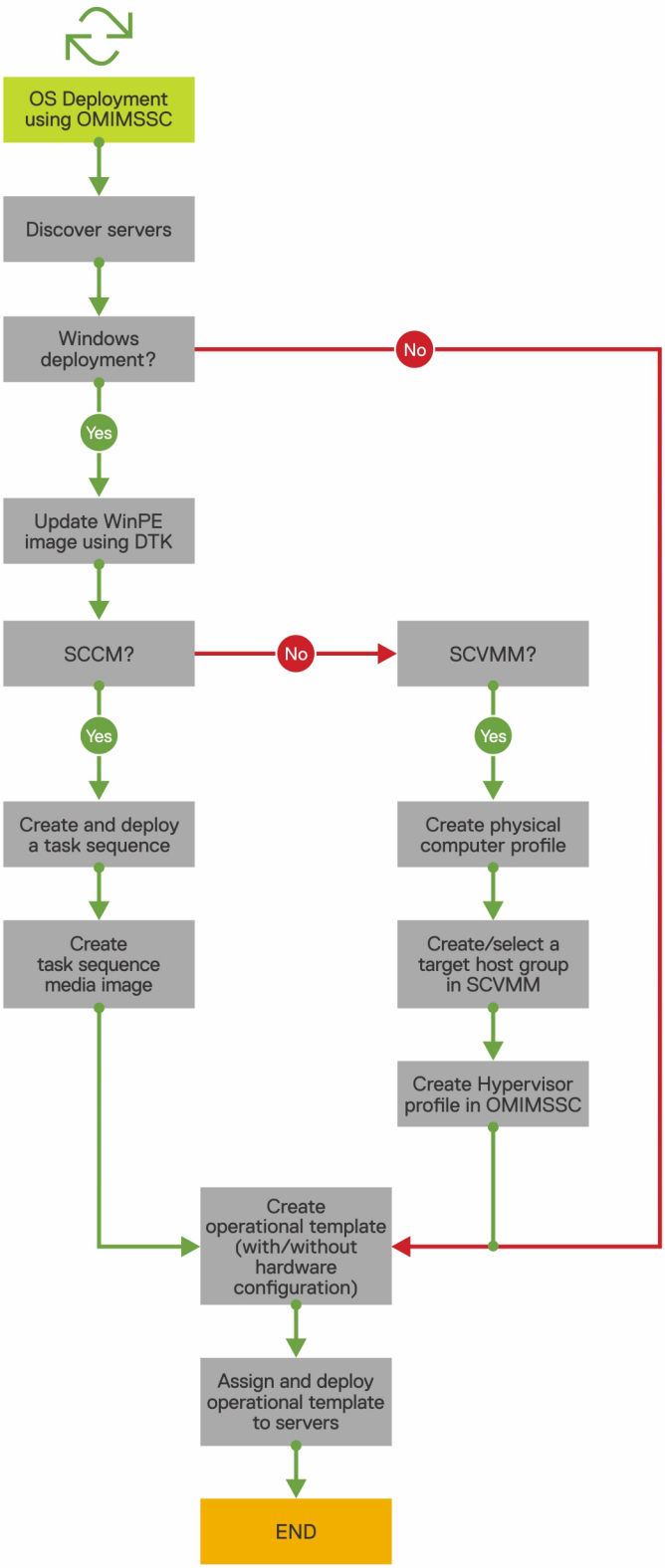
Cas d'utilisation pour les scénarios de déploiement

Utilisez OMIMSSC pour déployer un système d'exploitation Windows et non-Windows dans les environnements SCCM ou SCVMM à l'aide de Operational Template.

REMARQUE : Assurez-vous de mettre à niveau les versions de micrologiciel de périphérique vers les dernières versions disponibles sur ftp.dell.com ou downloads.dell.com avant le déploiement du système d'exploitation.

REMARQUE : Le déploiement de système d'exploitation non-Windows n'est pas pris en charge sur les serveurs de 11e génération.

Voici une représentation graphique de cas d'utilisation de déploiement de système d'exploitation dans OMIMSSC.



Deploying Windows OS using OMIMSSC console extension for SCCM

À propos de cette tâche

To deploy Windows OS through SCCM console using OMIMSSC, perform the following steps:

REMARQUE : Before deploying OS on a host server, ensure that in SCCM, the Client status of the server is No.

Étapes

1. Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot WIM image. For more information, see the WinPE update.
2. Import this .WIN image into the SCCM console, and create a boot image in SCCM. For more information, see the *Microsoft documentation*.
3. Create a task sequence in SCCM. For more information, see Creating task sequence.
4. Create a task sequence media image in SCCM. For more information, see the *Microsoft documentation*.

   REMARQUE : To enable unattended OS deployment when creating task sequence media, in Select the type of media, select Allow unattended operating system deployment check-box.
5. Découvrez le serveur de référence à l'aide de la page **Découverte**. Pour plus d'informations, reportez-vous à la section Découverte de serveurs par découverte manuelle.
6. Créez un Operational Template en capturant tous les détails du serveur découvert. Pour plus d'informations, reportez-vous à la section Création d'un modèle opérationnel à partir de serveurs de référence.
7. Attribuez un Operational Template sur un périphérique géré et vérifiez la conformité au modèle. Pour plus d'informations, reportez-vous à la section Attribution d'un modèle opérationnel et exécution de la conformité au modèle opérationnel.
8. Déployez un Operational Template pour rendre le modèle de périphérique conforme. Pour plus d'informations, reportez-vous à la section Déploiement d'un modèle opérationnel.
9. Affichez l'état de tâche du déploiement de système d'exploitation dans la page **Centre des tâches et des journaux**. Pour plus d'informations, reportez-vous à la section Lancement du Centre des tâches et des journaux.

Deploying hypervisor using OMIMSSC console extension for SCVMM

À propos de cette tâche

The different scenarios for hypervisor deployment are as follows:

Tableau 1. Hypervisor deployment scenarios

Condition	Action
If you require the latest factory drivers.	While creating a hypervisor profile, enable Lifecycle Controller (LC) driver injection.
If you want to retain the existing hardware configuration.	While creating the Operational Template, clear the check box for all the components that do not require any changes.

To deploy hypervisor through SCVMM console using OMIMSSC, perform the following steps:

Étapes

1. Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot ISO image. For more information, see the WinPE update.
2. Create a physical computer profile, and a host group in SCVMM. For more information, see the SCVMM documentation.

3 Create a hypervisor profile in the OMIMSSC console extension for SCVMM. For more information, see Creating a hypervisor profile.

4 Découvrez le serveur de référence à l'aide de la page **Découverte**. Pour plus d'informations, reportez-vous à la section Découverte de serveurs par découverte manuelle.

5 Créez un Operational Template en capturant tous les détails du serveur découvert. Pour plus d'informations, reportez-vous à la section Création d'un modèle opérationnel à partir de serveurs de référence.

6 Attribuez un Operational Template sur un périphérique géré et vérifiez la conformité au modèle. Pour plus d'informations, reportez-vous à la section Attribution d'un modèle opérationnel et exécution de la conformité au modèle opérationnel.

7 Déployez un Operational Template pour rendre le modèle de périphérique conforme. Pour plus d'informations, reportez-vous à la section Déploiement d'un modèle opérationnel.

8 Affichez l'état de tâche du déploiement de système d'exploitation dans la page **Centre des tâches et des journaux**. Pour plus d'informations, reportez-vous à la section Lancement du Centre des tâches et des journaux.

Redeploying Windows OS using OMIMSSC

À propos de cette tâche

To redeploy Windows OS on a server by using OMIMSSC console extension for SCCM or OMIMSSC console extension on SCVMM, perform the following steps:

Étapes

1 Delete the server from the Microsoft console. For more information, see Microsoft documentation.

2 Rediscover the server or synchronize OMIMSSC with the registered Microsoft console. The server is added as an unassigned server in OMIMSSC. For more information about discovery, see Discovering servers using manual discovery. For more information about synchronization, see Synchronizing with enrolled Microsoft console.

3 Créez un Operational Template en capturant tous les détails du serveur découvert. Pour plus d'informations, reportez-vous à la section Création d'un modèle opérationnel à partir de serveurs de référence.

4 Attribuez un Operational Template sur un périphérique géré et vérifiez la conformité au modèle. Pour plus d'informations, reportez-vous à la section Attribution d'un modèle opérationnel et exécution de la conformité au modèle opérationnel.

5 Déployez un Operational Template pour rendre le modèle de périphérique conforme. Pour plus d'informations, reportez-vous à la section Déploiement d'un modèle opérationnel.

6 Affichez l'état de tâche du déploiement de système d'exploitation dans la page **Centre des tâches et des journaux**. Pour plus d'informations, reportez-vous à la section Lancement du Centre des tâches et des journaux.

Déploiement de système d'exploitation non-Windows à l'aide d'extensions de console OMIMSSC

À propos de cette tâche

Pour déployer un système d'exploitation non-Windows à l'aide d'OMIMSSC, effectuez les étapes suivantes :

REMARQUE : Les étapes de déploiement d'un système d'exploitation non-Windows via OMIMSSC sont identiques dans les deux consoles Microsoft.

Étapes

1 Découvrez le serveur de référence à l'aide de la page **Découverte**. Pour plus d'informations, reportez-vous à la section Découverte de serveurs par découverte manuelle.

2 Créez un Operational Template en capturant tous les détails du serveur découvert. Pour plus d'informations, reportez-vous à la section Création d'un modèle opérationnel à partir de serveurs de référence.

3 Attribuez un Operational Template sur un périphérique géré et vérifiez la conformité au modèle. Pour plus d'informations, reportez-vous à la section Attribution d'un modèle opérationnel et exécution de la conformité au modèle opérationnel.

4 Déployez un Operational Template pour rendre le modèle de périphérique conforme. Pour plus d'informations, reportez-vous à la section Déploiement d'un modèle opérationnel.

REMARQUE :

Si la recherche DHCP échoue lors du déploiement, le délai d'expiration du serveur est atteint et ce dernier n'est pas déplacé vers la collection **Managed Lifecycle Controller Lifecycle Controller (ESXi)** dans SCCM.

Création de clusters d'Storage Spaces Direct à l'aide de Operational Template prédéfinis

Pour créer des clusters à l'aide d'OMIMSSC, effectuez les étapes suivantes :

1. Découvrez le serveur de référence à l'aide de la page **Découverte**. Pour plus d'informations, reportez-vous à la section Découverte de serveurs par découverte manuelle.
2. Modifiez le Operational Template prédéfini. Pour plus d'informations, reportez-vous à la section Modification d'un Operational Template.
3. Créez un commutateur logique. Pour plus d'informations, reportez-vous à la section Création d'un commutateur logique.
4. Créez un cluster d'Storage Spaces Direct. Pour plus d'informations, reportez-vous à la section Création de clusters d'Storage Spaces Direct.

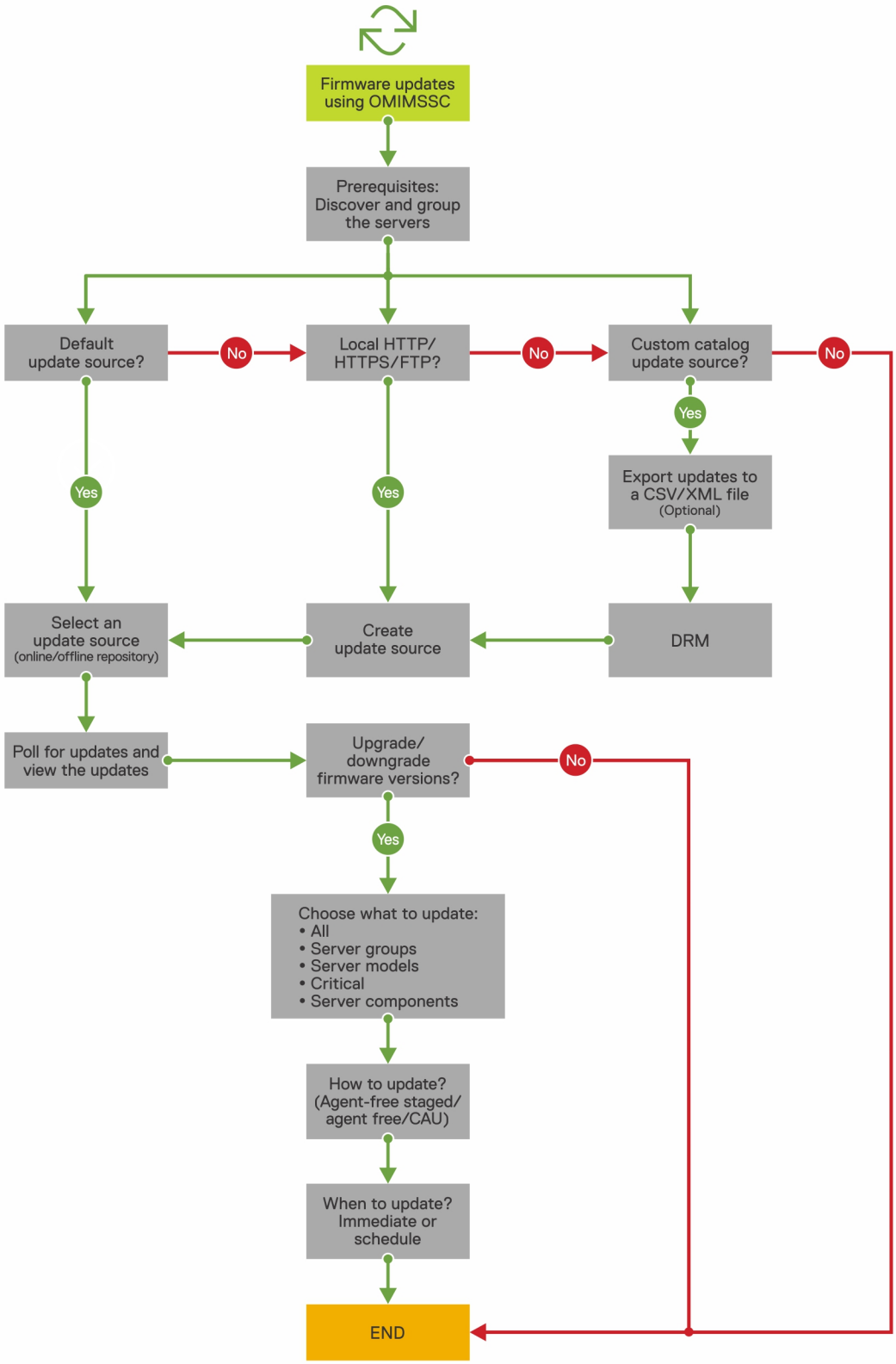
Cas d'utilisation pour le maintien des périphériques en condition opérationnelle

Maintenez les périphériques découverts en condition opérationnelle dans OMIMSSC.

Mise à jour du micrologiciel des serveurs et des périphériques MX7000

À propos de cette tâche

Voici une représentation graphique du workflow de mise à jour de micrologiciel.



Vous pouvez mettre à jour les périphériques sélectionnés à l'aide des sources de mise à jour suivantes :

- Source FTP en ligne ou locale
- Source HTTP en ligne ou locale
- Source HTTPS en ligne ou locale
- Source DRM (Dell Repository Manager) locale

Étapes

1 Créez ou sélectionnez une source de mise à jour par défaut. Pour plus d'informations sur la source de mise à jour, reportez-vous à la section Source de mise à jour.

> **REMARQUE : Assurez-vous de mettre à jour la source de mise à jour avec le dernier catalogue à l'aide de la fonction d'interrogation et de notification. Pour plus d'informations sur l'interrogation et la notification, reportez-vous à la section Interrogation et notification.**

Si vous effectuez une mise à jour des clusters d'Storage Spaces Direct, sélectionnez une source de mise à jour prédéfinie spécifique pour les clusters d'Storage Spaces Direct. Ces sources de mise à jour s'affichent uniquement dans la page **Centre de maintenance**.

Si vous effectuez une mise à jour de périphériques MX7000, sélectionnez une source de mise à jour prédéfinie spécifique pour les systèmes modulaires. Ces sources de mise à jour s'affichent uniquement dans la page **Centre de maintenance**.

2 Créez ou sélectionnez des groupes de mise à jour par défaut. Pour plus d'informations sur les groupes de mise à jour, reportez-vous à la section Groupes de mise à jour.

3 Découvrez ou synchronisez les périphériques avec une console Microsoft inscrite, et assurez-vous que l'inventaire des périphériques est à jour. Pour plus d'informations sur la découverte et la synchronisation, reportez-vous à la section Découverte de périphériques et synchronisation. Pour plus d'informations sur l'inventaire des serveurs, reportez-vous à la section Lancement de la vue Serveur.

4 Mettez à jour le périphérique en utilisant l'une des options suivantes :

- Sélectionnez les périphériques requis et cliquez sur **Exécuter la mise à jour**. Pour plus d'informations, reportez-vous à la section Mise à niveau ou rétrogradation des versions de micrologiciel à l'aide de la méthode d'exécution de mise à jour.

  > **REMARQUE : Pour rétrograder le micrologiciel de composants de périphérique, cochez la case Autoriser la rétrogradation. Si cette option n'est pas sélectionnée, aucune action n'est effectuée sur le composant qui requiert une rétrogradation de micrologiciel.**

- Sélectionnez le composant de mise à jour de micrologiciel dans Operational Template et déployez ce modèle. Pour plus d'informations sur Operational Template, reportez-vous à la section Operational Template.

Configuring replaced components

To match the firmware version, or the configuration settings of the replaced component to that of the old component, see Applying firmware and configuration settings.

Exportation et importation de profils de serveur

À propos de cette tâche

Exportez le profil de serveur au niveau d'une instance particulière, puis importez le profil pour rétablir le serveur :

Étapes

1 Créez une archive sécurisée. Pour plus d'informations sur la création d'une archive sécurisée, reportez-vous à la section Création d'une archive sécurisée.

2 Exportez un profil de serveur. Pour plus d'informations sur l'exportation d'un profil de serveur, reportez-vous à la section Exportation d'un profil de serveur.

3 Importez le profil de serveur sur le même serveur à partir duquel il a été exporté. Pour plus d'informations sur l'importation d'un profil de serveur, reportez-vous à la section Importation d'un profil de serveur.

> **REMARQUE : Vous pouvez importer le profil de serveur, y compris la configuration RAID, uniquement si la configuration RAID est exportée dans le profil.**

3

Views in OMIMSSC

View all the devices discovered in OMIMSSC in **Configuration and Deployment** page along with their hardware and firmware inventory information. Also, view all the jobs with status in **Jobs and Logs Center** page.

Sujets :

Lancement de la vue Serveur

La page **Vue Serveur** répertorie tous les serveurs non attribués et hôtes qui sont découverts dans OMIMSSC sous les onglets **Serveurs non attribués** et **Hôtes**.

À propos de cette tâche

Sous l'onglet **Serveurs non attribués**, affichez l'adresse IP iDRAC, le numéro de série, le modèle, la génération, la vitesse du processeur, la mémoire du serveur, l'état de conformité au modèle pour le Operational Template attribué, le numéro de série du système modulaire s'il s'agit d'un serveur modulaire et les informations de compatibilité matérielle. Si vous pointez sur la colonne **Compatibilité matérielle**, vous pouvez afficher les versions du BIOS, d'iDRAC, de LC et des packs de pilotes du périphérique. Pour plus d'informations sur la compatibilité matérielle, reportez-vous à la section À propos de la mise à jour de micrologiciel.

Sous l'onglet **Hôtes**, affichez le nom d'hôte, l'adresse IP iDRAC, le numéro de série, le modèle, la génération, la vitesse du processeur, la mémoire du serveur, le numéro de service du système modulaire s'il s'agit d'un serveur modulaire, le nom de domaine complet (FQDN) du cluster si le serveur fait partie d'un cluster, l'état de conformité au modèle pour le Operational Template attribué et les informations de compatibilité matérielle. Si vous pointez sur la colonne **Compatibilité matérielle**, vous pouvez afficher les versions du BIOS, d'iDRAC, de LC et des packs de pilotes du périphérique. Pour plus d'informations sur la compatibilité matérielle, reportez-vous à la section À propos de la mise à jour de micrologiciel.

Vous pouvez exécuter les tâches suivantes dans la page **Vue Serveur** :

- Découverte des serveurs
- Affichez des informations mises à jour en actualisant la page.
- Supprimez des serveurs d'OMIMSSC.
- Synchronisez avec la console Microsoft.
- Résolution des erreurs de synchronisation.
- Attribuez un Operational Template et exécutez la conformité au Operational Template.
- Déployer un Operational Template
- Corrélez les serveurs avec le groupe de clusters et le système modulaire auquel le serveur appartient.
- Lancement de la console iDRAC

Pour afficher les serveurs :

Étapes

1 Dans l'extension de console OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**.

2 Pour afficher les serveurs sans système d'exploitation, cliquez sur l'onglet **Serveurs non attribués**.

3 Pour afficher les serveurs hôtes, cliquez sur l'onglet **Hôtes**.

   a Pour afficher les groupes d'hôtes dans un format imbriqué tels que regroupés dans SCCM ou SCVMM, cliquez sur le menu déroulant **Sélectionner les hôtes de console**.

   Le menu déroulant **Sélectionner les hôtes de console** répertorie tous les groupes d'hôtes présents dans SCCM, avec un nom de groupe interne. Si vous sélectionnez le nom de groupe interne, tous les hôtes qui sont découverts et gérés dans SCCM et OMIMSSC s'affichent.

Étapes suivantes

Après avoir découvert les serveurs, tenez compte des éléments suivants :

- La colonne **Modèle opérationnel** s'affiche en tant que **Non attribué**, une fois que les serveurs ont été découverts. Afin de mettre à jour le micrologiciel et déployer le système d'exploitation sur ces serveurs, attribuez et déployez des Operational Template. Pour plus d'informations, reportez-vous à la section Gestion des Operational Template.
- Les serveurs découverts sont ajoutés aux groupes prédéfinis dans OMIMSSC. Vous pouvez créer des groupes de mise à jour personnalisée en fonction d'exigences fonctionnelles. Pour plus d'informations, reportez-vous à la section À propos des groupes de mise à jour.
- Lorsque vous vous connectez à OMIMSSC en tant qu'administrateur délégué, vous pouvez afficher tous les serveurs non attribués et hôtes qui ne sont pas propres à cet utilisateur. Par conséquent, assurez-vous de disposer des privilèges nécessaires avant d'effectuer des opérations sur les serveurs.
- S'il existe plusieurs consoles Microsoft inscrites dans OMIMSSC, les serveurs hôtes sont spécifiques de la console Microsoft où ils sont gérés. Les serveurs non attribués sont communs à toutes les consoles.

Launching Modular Systems view

The **Modular Systems View** page lists all the Modular Systems that are discovered in OMIMSSC.

À propos de cette tâche

View the CMC IP address, service tag, model, firmware version, template compliance status of Modular System for an assigned Operational Template, number of servers, Input/Output (I/O) Modules, and storage devices present on that Modular System. Configure the hardware and update Modular System firmware, by deploying the Operational Template.

You can perform the following tasks on **Modular Systems View** page:

- Discover Modular Systems using manual discovery
- Delete Modular System
- To view latest inventory information, refresh the page.
- Assign Operational Template for Modular System
- Deploy Operational Template for Modular System
- View I/O modules
- Launching I/O modules

To view Modular System discovered in OMIMSSC:

Étapes

1 In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**.

   All the Modular Systems discovered model names are displayed.

2 To view a specific Modular System, click a model name under **Modular Systems View**.

   All the Modular Systems of that model are displayed with their service tag.

3 To view all devices present in that Modular System, click service tag.

   All the servers, Input Output modules, and storage devices along with their details are displayed.

   REMARQUE : Only after a deep discovery of a Modular System, all devices in the Modular System and their information are displayed.

- By default the **Servers** tab is displayed.

  All the servers that are discovered in this Modular System are displayed.
- To view all the Input Output Modules present in a Modular System, click **I/O Modules** tab.
- To view all the storage devices present in the Modular System, click **Storage Devices** tab.

Étapes suivantes

After discovering Modular Systems, consider the following points:

- The **Operational Template** column is displayed as **Not Assigned**, after the Modular Systems are discovered. To update firmware and deploy operating system on these Modular Systems, assign and deploy Operational Templates. For more information, see Managing Operational Templates.
- View the count of Input/Output, storage devices, and servers present in Modular Systems after a shallow discovery. Perform a deep discovery, to view more details about the components in a Modular System.

Launching OpenManage Enterprise Modular console

À propos de cette tâche

To launch OpenManage Enterprise Modular console, perform the following steps:

Étapes

1 In OMIMSSC, expand **Configuration and Deployment**, and click **Modular Systems**.

2 Click **Device IP** of the Modular System.

Input/Output Modules

All the network Input/Output Modules along with their IP address, service tag, Input/Output type, model, firmware version and slot information are displayed.

À propos de cette tâche

Launch I/O Modules console from Input/Output Modules page.

To view information about Input/Output Modules, perform the following steps:

Étapes

1 In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**. Expand the **Modular Systems View**, and click service tag.

   All service tag of that model are displayed.

2 To view the Input/Output module, click **I/O Modules** tab.

Launching Input Output Modules console

À propos de cette tâche

Pour lancer la console du module d'entrée/sortie, effectuez les étapes suivantes :

Étapes

1 Dans OMIMSSC, développez **Configuration et déploiement**, cliquez sur **Vue Systèmes modulaires**. Développez le modèle au niveau des périphériques individuels.

   Tous les périphériques sous ce modèle s'affichent.

2 Cliquez sur **Modules d'E/S**.

3 Cliquez sur l'**adresse IP** du périphérique.

Launching Cluster View

The **Cluster View** page lists all the clusters discovered in OMIMSSC. View cluster's Fully Qualified Name (FQDN), service tag, and number of servers present in that cluster. Also, create a logical switch for clusters, and then create Storage Spaces Direct clusters using the predefined Operational Template.

À propos de cette tâche

You can perform the following tasks on **Cluster View** page:

- Creating logical switch (only for SC2016 VMM users)
- Creating Storage Spaces Direct clusters (only for SC2016 VMM users)
- Launching iDRAC console
- To view latest clusters discovered, refresh the page

To view cluster groups discovered in OMIMSSC:

Étapes

1 In OMIMSSC, click **Configuration and Deployment**, and then click **Cluster View**.

All the different types of clusters are grouped and listed.

2 To view information about specific type of clusters, expand the cluster type.

All the clusters of this type are listed on the left pane.

3 To view servers present in a cluster, click a cluster name.

Launching iDRAC console

À propos de cette tâche

To launch iDRAC console, perform the following step:

Étape

Dans OMIMSSC, développez **Configuration et déploiement** et sélectionnez l'une des options suivantes :

- Cliquez sur **Vue Serveur**. En fonction du serveur (s'il s'agit d'un hôte ou d'un serveur non attribué), cliquez sur l'onglet **Serveurs non attribués** ou **Hôtes**, puis cliquez sur l'adresse **IP iDRAC** du serveur.

  L'onglet **Serveurs non attribués** s'affiche par défaut.

  Pour afficher l'onglet Hôtes, cliquez sur **Hôtes**.
- Cliquez sur **Vue Cluster**. Développez le type de cluster et développez le groupe de cluster au niveau du serveur.

  L'onglet **Serveur** s'affiche.

Lancement du Centre de maintenance

La page **Centre de maintenance** répertorie tous les périphériques découverts dans les groupes et les ressources qui sont requis pour la maintenance des périphériques dans OMIMSSC. Dans la page **Centre de maintenance**, affichez l'inventaire de micrologiciel du périphérique, gérez les périphériques en conservant leur micrologiciel à jour en fonction des recommandations, rétablissez le serveur à un état antérieur s'il est tombé en panne, appliquez à un composant remplacé la configuration de l'ancien composant et exportez les journaux de serveur pour résoudre des problèmes. Dans la page **Paramètres de mise à jour**, affichez toutes les sources de mise à jour, l'interrogation et les notifications pour les dernières mises à jour de la source de mise à jour par défaut, les groupes de mise à jour des périphériques qui nécessitent une gestion similaire et toutes les archives sécurisées requises pour les configurations de serveur.

À propos de cette tâche

REMARQUE : Par défaut, OMIMSSC est fourni avec un fichier de catalogue qui affiche une version antérieure du rapport de comparaison pour la source de mise à jour FTP, HTTP et HTTPS prédéfinie. Par conséquent, vous devez télécharger le dernier catalogue afin d'afficher le dernier rapport de comparaison. Pour télécharger le catalogue le plus récent, modifiez et enregistrez les sources de mise à jour FTP, HTTP et HTTPS.

Vous pouvez effectuer les tâches suivantes sur la page **Centre de maintenance** :

- Créer une source de mise à jour
- Définir la fréquence d'interrogation
- Sélectionnez des groupes de mise à jour prédéfinis ou créez des groupes de mise à jour personnalisée.
- Afficher et actualiser l'inventaire de micrologiciel
- Mettre à niveau et rétrograder les versions de micrologiciel à l'aide de la méthode d'exécution de mise à jour
- Créer des archives sécurisées
- Exporter des profils de serveur
- Importer des profils de serveur
- Exportation de l'inventaire

Pour afficher la page **Centre de maintenance** :

Étape

Dans OMIMSSC, cliquez sur **Centre de maintenance**.

La page **Centre de maintenance** s'affiche.

Launching Jobs and Logs Center

View information about jobs initiated in OMIMSSC along with status of job's progress, and its subtask. Also, you can filter and view jobs of a particular job category.

À propos de cette tâche

You can view jobs that are initiated from OMIMSSC, in OMIMSSC Admin Portal and OMIMSSC console extension.

- OMIMSSC Admin portal—displays jobs that are initiated from all OMIMSSC consoles and users
- OMIMSSC console—displays jobs specific to a user and a console

Job names are either generated by the system or provided by users, and the subtasks are named after the IP address or hostname of the managed systems. Expand the subtask to view the activity logs for that job. Jobs are classified under four groups:

- **Running**—displays all the jobs that are currently running and in-progress state.
- **History**—displays all the jobs run in the past with its job status.
- **Scheduled**—displays all the jobs that are scheduled for a future date and time. Also, you can cancel these scheduled jobs.
- **Generic Logs**—displays OMIMSSC Appliance-specific, common log messages that are not specific to a task, and other activities. Every job is displayed with a user name and a console FQDN from where it was initiated.
  - **Appliance Log Messages**—displays all OMIMSSC Appliance-specific log messages such as restarting OMIMSSC Appliance. You can view this category of messages only from OMIMSSC Admin Portal.
  - **Generic Log Messages**—displays log messages that are common across different job categories that are listed in **Running**, **History**, and **Scheduled** tabs. These logs are specific to a console and a user.

    For example, if a firmware update job is in-progress for a group of servers, the tab displays log messages that belong to creating the Server Update Utility (SUU) repository for that job.

The various states of a job that is defined in OMIMSSC are as follows:

- **Canceled**—job is manually canceled, or after OMIMSSC Appliance restarts.
- **Successful**—job is completed successfully.
- **Failed**—job is not successful.
- **In Progress**—job is running.
- **Scheduled**—job has been scheduled for a future date and time.

  REMARQUE : If multiple jobs are submitted simultaneously to the same device, the jobs fail. Hence, ensure that you schedule jobs for same device at different times.
- **Waiting**—job is in a queue.
- **Recurring Schedule**—job is scheduled at regular intervals.

Étapes

1 In OMIMSSC, click **Jobs and Log Center**.

2 To view a specific category of jobs, such as **Scheduled**, **History**, or **Generic**, click the required tab.

Expand a job to view all the devices included in that job. Expand further to view the log messages for that job.

REMARQUE : All the job-related generic log messages are listed under the Generic tab and not under the Running or History tab.

3 (Optional) Apply filters to view different groups of jobs and status of job in **Status** column.

4

Managing profiles

Profiles contain all the data that is required for performing any operations in OMIMSSC.

Sujets :

About credential profile

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of the user. Each credential profile contains a user name and password for a single user account.

OMIMSSC uses credential profiles to connect to the managed systems' iDRAC. Also, you can use credential profiles to access the FTP site, resources available in Windows shares, and to work with different features of iDRAC.

You can create four types of credential profiles:

- Device Credential Profile—used to log in to iDRAC or CMC. Also, you can use this profile to discover a server, resolve synchronization issues, and deploy operating system. This profile is specific to a console. You can use and manage this profile only in a console where it is created.
- Windows Credential Profile—used for accessing share folders in Windows operating system
- FTP Credential Profile—used for accessing an FTP site
- Proxy Server Credentials—used for providing proxy credentials for accessing any FTP sites for updates.

> **REMARQUE : All profiles other than device profile are shared resources. You can use and manage these profiles from any of the enrolled consoles.**

Predefined credential profile

SYSTEM DEFAULT FTP account is a predefined credential profile available in OMIMSSC. The predefined credential profile is of type FTP, having **User Name**, and **Password** as **anonymous**. Use this profile to access `ftp.dell.com`

Creating credential profile

À propos de cette tâche

When creating a credential profile, consider the following points:

- During auto discovery, if a default credential profile is not available for iDRAC, and then the default iDRAC credentials is used. The default iDRAC user name is `root`, and password is `calvin`.
- To get information about the modular systems, the modular server is accessed with default CMC profile. The default CMC profile user name is `root` and password is `calvin`.
- (Only for SCVMM users) When a device type credential profile is created, an associated **RunAsAccount** is created in **SCVMM** to manage the device, and the name of the **RunAsAccount** is `Dell_CredentialProfileName`.
- Ensure that you do not edit, or delete the **RunAsAccount** in SCVMM.

Étapes

1 In OMIMSSC, perform any of the following steps to create a **Credential Profile**:
   - In OMIMSSC dashboard, click **Create Credential Profile**.
   - In the navigation pane, click **Profiles** > **Credential Profile**, and then click **Create**.
2 In **Credential Type**, select the credential profile type that you want to use.
3 Provide a profile name and description.

   REMARQUE : Default Profile for option is applicable only for a Device type credential profile.
4 In **Credentials**, provide the user name and password.
   - If you are creating a **Device Credential Profile**, select to make this profile as the default profile to log in to iDRAC or CMC by selecting the **Default Profile for** option. Select **None**, if you choose not to set the profile as a default profile.
   - If you are creating a **Windows Credential Profile**, provide the domain details in **Domain**.

     REMARQUE : Provide the domain name with Top Level Domain (TLD) details while creating the credential profile for console enrollment.

     For example, if the domain name is `mydomain`, and the TLD is `com`, provide the domain name in credential profile as: mydomain.com.
   - If you are creating a **Proxy Server Credentials**, provide the proxy server URL `http://hostname:port` or `http://IPaddress:port` format in **Proxy Server URL**.
5 To create the profile, click **Finish**.

Modifying credential profile

À propos de cette tâche

Consider the following before modifying a credential profile:

- After creating, you cannot modify the type of a credential profile. However, you can modify other fields.
- You cannot modify a credential profile, if it is in use.

REMARQUE : The steps to modify any type of credential profile are the same.

Étapes

1 Select the credential profile that you want to modify, click **Edit**, and update the profile.
2 To save the changes made, click **Save**.

Étape suivante

To view the changes made, refresh the **Credential Profile** page.

Suppression d'un profil de référence

À propos de cette tâche

Tenez compte des points suivants lorsque vous supprimez un profil de référence :

- Lorsqu'un profil de référence de type périphérique est supprimé, le **Compte d'identification** associé dans SCVMM est également supprimé.
- Lorsque vous supprimez le compte **RunAsAccount** dans SCVMM, le profil de référence correspondant n'est pas disponible dans OMIMSSC.
- Pour supprimer un profil de référence utilisé dans la découverte des serveurs, supprimez le serveur découvert, puis le profil de référence.
- Pour supprimer un profil de référence de type de périphérique utilisé pour le déploiement, supprimez les serveurs déployés dans l'environnement SCVMM, puis le profil de référence.

- Vous ne pouvez pas supprimer un profil de référence s'il est utilisé dans une source de mise à jour.

REMARQUE : Les étapes sont les mêmes quel que soit le type de profil de référence que vous supprimez.

Étape

Sélectionnez le profil de référence à supprimer, puis cliquez sur **Supprimer**.

Étape suivante

Pour afficher les modifications apportées, actualisez la page **Profil de référence**.

About hypervisor profile (for SCVMM users)

A hypervisor profile contains a customized WinPE ISO (WinPE ISO is used for hypervisor deployment), host group, and host profile taken from SCVMM, and LC drivers for injection. Only OMIMSSC console extension for SCVMM users, can create and manage hypervisor profiles.

Creating hypervisor profile

Create a hypervisor profile and use the profile to deploy hypervisors.

Prérequis

- Update the WinPE ISO image, and have access to the share folder where the image is saved. For information about updating the WinPE image, see WinPE update.
- Create a host group, and host profile or physical computer profile, in SCVMM. For information about creating host groups in SCVMM, see Microsoft documentation.

Étapes

1 In OMIMSSC, perform any one of the following tasks:
   - In the OMIMSSC dashboard, click **Create Hypervisor Profiles**.
   - In the left navigation pane, click **Profiles and Templates**, **Hypervisor Profile**, and then click **Create**.

   The **Hypervisor Profile Wizard** is displayed.
2 In the **Welcome** page click **Next**.
3 In **Hypervisor Profile**, provide a name and description of the profile, and then click **Next**.
4 In the **SCVMM Information** page,
   a For **SCVMM Host Group Destination**, select an SCVMM host group from the drop-down menu to add the host into this group.
   b From **SCVMM Host Profile/Physical Computer Profile**, select a host profile or physical computer profile from SCVMM that includes configuration information to be applied on servers.

      In SCVMM, select one of the following disk partition methods in a **Physical Computer Profile**:
      - When booting to UEFI mode, select **GUID Partition Table (GPT)** option.
      - When booting to BIOS mode, select **Master Board Record (MBR)** option.
5 In **WinPE Boot Image Source**, provide the following details, and click **Next**.
   a For **Network WinPE ISO Name**, provide the share folder path having the updated WinPE file name. For updating WinPE file, see WinPE update.
   b For **Credential Profile**, select the credentials having access to share folder having the WinPE file.
   c (Optional) To create a windows credential profile, click **Create New**. For information about creating credential profile, see Creating credential profile.
6 (Optional) To enable LC driver injection, perform the following steps:

   REMARQUE : Ensure that you select Enable Dell Lifecycle Controller Drivers Injection check-box, because the latest operating system driver packs for NIC cards are available in the latest operating system drivers.

   a Select the operating system that you want to deploy so that the relevant drivers are selected.

b Select **Enable LC Drivers Injection**.
c Select the hypervisor version **Hypervisor Version**.

7 In **Summary**, click **Finish**.

Étape suivante
To view the changes made, refresh the **Hypervisor profile** page.

Modifying hypervisor profile

À propos de cette tâche
Consider the following when you are modifying a hypervisor profile:

- You can modify host profile, host group, and drivers from Lifecycle Controller.
- You can modify the WinPE ISO name. However, you cannot modify the ISO image.

Étapes
1 Select the profile that you want to modify and click **Edit**.
2 Provide the details, and click **Finish**.

Étape suivante
To view the changes made, refresh the **Hypervisor profile** page.

Deleting hypervisor profile

Étape
Select the hypervisor profile that you want to delete, and click **Delete**.

Étape suivante
To view the changes made, refresh the **Hypervisor profile** page.

5

Discovering devices and synchronizing servers with MSSC console

Discovery is the process of adding supported modular systems and PowerEdge bare-metal servers or host servers or nodes in to OMIMSSC.

Synchronization with MSSC console is the process of adding host servers from registered Microsoft console (SCCM or SCVMM) in to OMIMSSC. Hence, using any one of the processes, you can add devices in to OMIMSSC . Only after discovering the devices, you can manage them in OMIMSSC.

Sujets :

About reference server configuration

A server configuration with a preferred boot sequence, BIOS, RAID settings, hardware configuration, firmware update attributes, and operating system parameters that is ideally suited for an organization is called reference server configuration.

Discover a reference server and capture the reference server settings in an Operational Template, and replicate it across different servers with same hardware configuration.

About reference Modular System configuration

A Modular System configuration with a preferred network configuration, user account, security, and alerts that is ideally suited for an organization is called reference Modular System configuration or reference chassis.

Discover a reference Modular System and capture the reference Modular System settings in an Operational Template, and replicate it across different Modular Systems of the same models.

Discovering devices in OMIMSSC

Discover MX7000 Modular Systems, hosts, and unassigned servers in OMIMSSC. Information about discovered devices is saved in OMIMSSC Appliance.

Using the following methods, you can discover Dell EMC servers using their iDRAC IP address:

REMARQUE : The discovered device is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS that are required to work with OMIMSSC. For information about supported versions, see *OpenManage Integration for Microsoft System Center Release Notes.*

Discover Modular Systems with device IP address using Discovering modular systems using manual discovery method.

Device discovery in OMIMSSC console extension for SCCM

Discover devices in OMIMSSC console extension for SCCM. After discovering a server, the server is added to a predefined group in OMIMSSC, and one of the following SCCM predefined groups or collections—**All Dell Lifecycle Controller Servers collection** and **Import Dell Server collection** that are created under the **Device Collections**.

If the discovered server is not present in SCCM, or if there are no predefined groups or collections in SCCM, the predefined collections are created and the discovered server is and then added to the respective group.

Device discovery in OMIMSSC console extension for SCVMM

Discover Modular Systems, hyper-V hosts, and unassigned servers in OMIMSSC console extension for SCVMM. After discovery, the devices are added to respective predefined update groups.

System requirements for managed systems

Managed systems are the devices that are managed using OMIMSSC. The system requirements for discovering servers using OMIMSSC console extensions are as follows:

- OMIMSSC console extension for SCCM supports modular, monolithic, and tower server models on 11th and later generations of servers.
- OMIMSSC console extension for SCVMM supports modular and monolithic server models on 11th and later generations of servers.
- For source configuration and destination configuration, use same type of disks—only Solid-state Drive (SSD), SAS, or only Serial ATA (SATA) drives.
- For successful hardware profile RAID cloning, for destination system disks, use same or greater size and number of disks as present in the source.
- RAID sliced virtual disks are not supported.
- iDRAC with shared LOM is not supported.
- RAID configured on external controller is not supported.
- Enable Collect System Inventory on Restart (CSIOR) in managed systems. For more information, see iDRAC documentation.

Discovering servers using auto discovery

To automatically discover servers, connect servers to the network and power on the servers. OMIMSSC auto discovers the unassigned servers by using the remote enablement feature of iDRAC. OMIMSSC works as a provisioning server and uses iDRAC reference to auto discover servers.

1 In OMIMSSC, create a device type credential profile by providing the iDRAC credentials and make it as default for servers. For information about creating a credential profile, see Creating a credential profile.

2 Disable the existing Administrator account in iDRAC settings in the managed device.

REMARQUE : It is recommended that you have a guest user account with operator privileges to log in to iDRAC in case auto discovery fails.

3 Enable the auto discovery feature in managed device's iDRAC settings. For more information, see iDRAC documentation.

4 In managed device's, iDRAC Settings, provide OMIMSSC Appliance IP in **provision server IP**, and then restart the server.

Discovering servers using manual discovery

To manually discover PowerEdge servers by using an IP address or an IP range. To discover servers, provide the iDRAC IP address and the device type credentials of a server. When you are discovering servers by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of a server.

Prérequis

Ensure that a default credential profile is available.

Étapes

1 Dans la console OMIMSSC, effectuez l'une des opérations suivantes :
   - Dans le tableau de bord, cliquez sur **Découvrir des serveurs**.
   - Dans le volet de navigation, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Serveur**, puis cliquez sur **Découvrir**.

2 In the **Discover** page, select the required option:
   - **Discover Using an IP Address**—to discover a server using an IP address.
   - **Discover Using an IP Range**—to discover all servers within an IP range.

3 Select the device type credential profile, or click **Create New** to create a device type credential profile.

   The selected profile is applied to all the servers.

4 In **iDRAC IP address**, provide the IP address of the server that you want to discover.

5 In **Discover Using an IP Address or IP Address Range**, do any of the following:
   - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
   - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.

6 Provide a unique job name, description for the job, and click **Finish**.

   Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

   The **Jobs and Logs Center** page is displayed. Expand the discovery job to view the progress of the job in **Running** tab.

After discovering a server, the server is added to **Hosts** tab, or **Unassigned** tab in the **Server View** page of **Configuration and Deployment** section.

- When you discover a server with an operating system that is deployed on it, and the server is already present in SCCM or SCVMM console, and then the server is listed as a host server under the **Hosts** tab.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, and then the server is listed as an unassigned server under the **Unassigned** tab in all the OMIMSSC console extensions, in case of multiple Microsoft consoles enrolled to single OMIMSSC Appliance.

After discovering a server, the server is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS to work with OMIMSSC. To view the firmware versions of the server components, hover the hover over the **Hardware Compatibility** column against the server row. For information about the supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.

A license is consumed for each discovered server. The **Licensed Nodes** count in **License Center** page decreases as the number of servers are discovered.

REMARQUE : To work with the servers discovered in the prior versions of OMIMSSC Appliance, rediscover the servers.

REMARQUE : When you log in to OMIMSSC as a delegated admin, you can view all the host servers and unassigned servers that are not specific to the logged in user. Hence, you cannot perform any operations on such servers. Make sure that you have the required privileges before performing any operations on such servers.

Discovering MX7000 by using manual discovery

To manually discover PowerEdge MX7000 Modular System by using an IP address or an IP range, provide a Modular System's IP address and device type credentials of the Modular System. When you are discovering Modular Systems by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of the Modular Systems.

Prérequis

Ensure that the default credential profile of a Modular System you want to discover is available.

À propos de cette tâche

To discover Modular Systems, perform the following steps:

Étapes

1. In OMIMSSC, click **Configuration and Deployment**, click **Modular Systems View**, and then click **Discover**.
2. In the **Discover** page, select the required option:
   - **Discover Using an IP Address**—to discover a Modular System using an IP address.
   - **Discover Using an IP Range**—to discover all Modular Systems within an IP range.
3. Select the device type credential profile, or click **Create New** to create a device type credential profile.

   The selected profile is applied to all the servers.
4. In **IP address**, provide the IP address of the Modular System that you want to discover.
5. In **Discover Using an IP Address or IP Address Range**, do one of the following:
   - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
   - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.
6. In **Modular Systems Discovery Methods**, select one of the following:
   - **Shallow discovery**—discovers Modular Systems and also number of servers in the Modular System.
   - **Deep discovery**—discovers Modular Systems and devices present in the Modular System such as Input Output Modules (IOM) and storage devices.

     REMARQUE : To deep discover MX7000 and its components, ensure that PowerEdge MX7000 and all its components are enabled with IPv4 address.
7. Provide a unique job name, and click **Finish**.

   Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

   To view the progress of the job in the **Running** tab, expand the discovery job in **Jobs and Logs Center**.

Synchronization of OMIMSSC console extension with enrolled SCCM

You can synchronize all servers (hosts and unassigned) from enrolled SCCM to OMIMSSC. Also, you get the latest firmware inventory information about the servers after synchronization.

Before synchronizing OMIMSSC and the enrolled SCCM console, ensure that the following requirements are met:

- Have details of default iDRAC credential profile for servers.
- Update the **Dell Default Collection** before synchronizing OMIMSSC with SCCM. However, if an unassigned server is discovered in SCCM, it is added to **Import Dell server collection**. To add this server in **Dell Default Collection**, add the server's iDRAC IP address in the **OOB** page.
- Ensure that there are no duplicate entries of devices in SCCM.

After synchronizing OMIMSSC with SCCM, if the device is not present in SCCM, and then the **All Dell Lifecycle Controller Servers** collection and the **Import Dell server** collection under **Device Collections** is created and the server is added to that respective group.

Synchronization of OMIMSSC console extension with enrolled SCVMM

You can synchronize all hyper-V hosts, hyper-V host clusters, modular hyper-V hosts, and unassigned servers from SCVMM consoles with OMIMSSC console extension for SCVMM. Also, you get the latest firmware inventory information about the servers after synchronization.

Consider the following before synchronizing OMIMSSC with SCVMM:

- Have details of default iDRAC credential profile for servers.
- If the host server's Baseboard Management Controller (BMC) is not configured with the iDRAC IP address, and then you cannot synchronize the host server with OMIMSSC. Hence, configure BMC in SCVMM (for more information, see MSDN article at `technet.microsoft.com`), and then synchronize OMIMSSC with SCVMM.
- SCVMM supports numerous hosts in the environment, due to which synchronization is a long running task.

Synchronizing with enrolled Microsoft console

À propos de cette tâche

To add servers managed in Microsoft console to OMIMSSC, perform the following step:

Étape

Dans OMIMSSC, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Serveur**, puis cliquez sur **Synchroniser avec OMIMSSC** pour synchroniser tous les hôtes qui sont répertoriés dans la console MSSC inscrite avec l'appliance OMIMSSC.

Resolving synchronization errors

The servers that are not synchronized with OMIMSSC are listed with their iDRAC IP address and host name.

À propos de cette tâche

REMARQUE : All servers that are not synchronized due to issues such as invalid credentials, or the iDRAC IP address, or connectivity, or other issues; ensure that you resolve the issues first, and then synchronize.

REMARQUE : During resynchronization, host servers that are deleted from the enrolled MSSC environment are moved to the Unassigned Servers tab in the OMIMSSC console extensions. If a server is decommissioned, and then remove that server from the list of unassigned servers.

To resynchronize servers with credential profile issues:

Étapes

1. In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Resolve Sync Errors**.
2. Select the servers for resynchronization, and select the credential profile, or to create a credential profile click **Create New**.
3. Provide a job name, and if necessary select the **Go to the Job List** option to view the job status automatically once the job is submitted.
4. Click **Finish** to submit the job.

Viewing System Lockdown Mode

The System Lockdown Mode setting is available in iDRAC for 14th generation of servers and later. The setting when turned on locks the system configuration including firmware updates. After the System Lockdown mode is enabled, users cannot change any configuration settings. This setting is intended to protect the system from unintentional changes. To perform any operations on the managed servers, ensure that you disable the setting on it's iDRAC console. In OMIMSSC console, the System Lockdown mode status is represented with a lock image before the iDRAC IP address of the server.

- A lock image is displayed along with the servers's iDRAC IP if the setting is enabled on that system.

- An unlocked image is displayed along with the servers's iDRAC IP if the setting is disabled on that system.

REMARQUE : Before launching the OMIMSSC console extensions, verify the iDRAC System Lockdown Mode setting on the managed servers.

For more information about iDRAC System Lockdown Mode, see iDRAC documentation available at **dell.com/support**.

Deleting servers from OMIMSSC

À propos de cette tâche

To delete a server, perform the following steps:

Consider the following points before deleting a server:

- After you delete a server, the consumed license is relinquished.
- You can delete a server that is listed in OMIMSSC based on the following criteria:
  - An unassigned server that is listed in the **Unassigned servers** tab.
  - If you delete a host server that is provisioned in enrolled SCCM or SCVMM and present in OMIMSSC under the **Hosts** tab, first delete the server in SCCM or SCVMM, and then delete the server from OMIMSSC.

Étapes

1 In the OMIMSSC console, click **Configuration and deployment**, and then click **Server View**:
   - To delete unassigned servers—in the **Unassigned Servers** tab, select the server, and click **Delete**.
   - To delete host servers—in the **Host Servers** tab, select the server, and click **Delete**.

2 In the confirmation dialog box, click **Yes**.

Deleting Modular Systems from OMIMSSC

À propos de cette tâche

To delete a Modular System, perform the following steps:

Étapes

1 In OMIMSSC console, click **Configuration and deployment**, and then click **Modular Systems View**.

2 Select the Modular Systems, and click **Delete**.

6

Preparing for operating system deployment

Before deploying Windows operating system on the managed servers, update the WinPE image, create a task sequence, LC boot media file, and task sequence media bootable ISO file. The steps vary for SCCM and SCVMM console users. Refer the bellow section for more details. For deploying non-windows operating system remember the points mentioned in Preparing for non-Windows OS deployment section.

Sujets :

À propos de l'image WinPE

L'image WinPE (environnement de préinstallation Windows) est utilisée pour déployer le système d'exploitation. Utilisez une image WinPE mise à jour pour déployer le système d'exploitation, car l'image WinPE disponible à partir de SCCM ou SCVMM peut ne pas contenir les pilotes les plus récents. Pour créer une image WinPE contenant tous les pilotes requis, mettez à jour l'image à l'aide de DTK. Assurez-vous que les packs de pilotes correspondant au système d'exploitation sont installés dans Lifecycle Controller.

REMARQUE : Ne renommez pas le fichier boot.wim.

Fourniture d'un fichier WIM pour SCCM

Copiez le fichier **boot.wim** à partir de l'emplacement suivant **\\shareip\sms_sitecode\OSD\boot\x64\boot.wim**, puis collez-le dans un dossier de partage accessible par OMIMSSC.

Par exemple, l'emplacement du chemin partagé : **\\shareip\sharefolder\boot.wim**

Fourniture d'un fichier WIM pour SCVMM

1. Installez le rôle WDS (Windows Deployment Server) sur un serveur, puis ajoutez le serveur PXE à SCVMM.

   Pour en savoir plus sur l'ajout du rôle WDS sur un serveur, et sur l'ajout d'un serveur PXE à SCVMM, consultez la documentation de Microsoft.
2. Copiez le fichier **boot.wim** depuis le serveur PXE présent à l'emplacement suivant **C:\RemoteInstall\DCMgr\Boot\Windows\Images**, puis collez-le dans un dossier de partage accessible par OMIMSSC.

   Par exemple, l'emplacement du chemin partagé : **\\shareip\sharefolder\boot.wim**

Extraction des pilotes DTK

Un fichier DTK contient les versions de micrologiciel nécessaires qui sont requises pour les serveurs sur lesquels vous déployez les systèmes d'exploitation.

À propos de cette tâche

REMARQUE : Lors de l'utilisation de la dernière version du fichier DTK pour la création d'une image ISO WinPE, utilisez le Dell EMC OpenManage Deployment Toolkit for Windows. Le fichier Dell EMC OpenManage Deployment Toolkit for Windows contient les versions de micrologiciel nécessaires qui sont requises pour les systèmes sur lesquels vous effectuez le déploiement des systèmes d'exploitation. Utilisez la version la plus récente du fichier, et n'utilisez pas le fichier Dell EMC OpenManage Deployment Toolkit Windows Driver Cabinet pour la mise à jour WinPE.

Étapes

1 Double-cliquez sur le fichier exécutable DTK.

2 Pour décompresser les pilotes DTK, sélectionnez un dossier.

Par exemple, **C:\DTK501**.

3 Copiez le dossier DTK décompressé dans un dossier de partage.

Par exemple, **\\Shareip\sharefolder\DTK\DTK501**.

REMARQUE : Si vous effectuez une mise à niveau de SCVMM SP1 vers SCVMM R2, effectuez une mise à niveau vers Windows PowerShell 4.0 et créez une image ISO WinPE.

Mise à jour d'une image WinPE

À propos de cette tâche

Un nom de tâche unique est attribué à chaque tâche de mise à jour WinPE.

Étapes

1 Dans OMIMSSC, sélectionnez **Mise à jour WinPE**.

La page **Mise à jour WinPE** s'affiche.

2 Dans **Source de l'image**, pour **Chemin de l'image WinPE personnalisée**, entrez le chemin de l'image WinPE, ainsi que le nom du fichier contenant l'image.

Par exemple, **\\Shareip\sharefolder\WIM\boot.wim**.

3 Sous **Chemin DTK**, pour **Chemin des pilotes DTK**, indiquez l'emplacement des pilotes du toolkit de déploiement Dell EMC.

Par exemple, **\\Shareip\sharefolder\DTK\DTK501**.

4 Sous **Fichier de sortie**, pour **Nom du fichier ISO ou WIM**, entrez un nom pour le fichier en même temps que le type de fichier qui va être généré après la mise à jour de l'image WinPE.

Entrez l'un des types de fichiers de sortie :

- Fichier WIM pour SCCM
- Fichier ISO pour SCVMM

5 Sous **Profil de référence**, pour **Profil de référence**, entrez les informations d'identification qui ont accès au dossier de partage où l'image WinPE est enregistrée.

6 (Facultatif) Pour afficher la liste des tâches, sélectionnez **Accéder à la liste des tâches**.

Un nom de tâche unique est attribué à chaque mise à jour WinPE.

7 Cliquez sur **Update** (Mettre à jour).

L'image WinPE avec le nom du fichier fourni à l'étape précédente est créée sous **\\Shareip\sharefolder\WIM**.

Preparing for operating system deployment on SCCM console

Before deploying operating system on managed servers discovered using OMIMSSC in SCCM console, create a Dell EMC specific or a custom task sequence, an LC boot media file, and task sequence media bootable ISO file.

Task sequence-SCCM

Task sequence is a series of commands that is used to deploy operating system on the managed system using SCCM.

Before creating Operational Template, Dell EMC recommends that you complete the following prerequisites.

- In Configuration Manager, ensure that the system is discovered and present under **Assets and Compliance** > **Device Collections** > **All Dell Lifecycle Controller Servers**. For more information, see Discover servers.
- Install the latest BIOS version on the system.
- Install the latest version of Lifecycle Controller on the system.
- Install the latest version of iDRAC firmware on the system.

REMARQUE : Always launch the Configuration Manager console with administrator privileges.

Types of task sequence

You can create a task sequence in two ways:

- Create a Dell-specific task sequence using OMIMSSC Deployment template.
- Create a custom task sequence.

The task sequence goes to the next task sequence step irrespective of the success or failure of the command.

Création d'une séquence de tâches propre à Dell

À propos de cette tâche

Pour créer une séquence de tâches propre à Dell à l'aide de l'option **Modèle de déploiement de serveur OMIMSSC** :

Étapes

1 Lancez Configuration Manager.

La console Configuration Manager s'affiche.

2 Dans le volet de gauche, sélectionnez **Bibliothèque logicielle** > **Aperçu Systèmes d'exploitation** > **Séquence de tâches**.

3 Cliquez avec le bouton droit de la souris sur **Séquences de tâches**, puis cliquez sur **Déploiement de serveur OMIMSSC** > **Créer un modèle de déploiement de serveur OMIMSSC**.

L'**Assistant Séquence de tâches de déploiement de serveur OMIMSSC** s'affiche.

4 Saisissez le nom de la séquence de tâches dans le champ **Nom de la séquence de tâches**.

5 Dans la liste déroulante, sélectionnez l'image de démarrage à utiliser.

REMARQUE : Nous vous recommandons d'utiliser l'image d'amorçage personnalisée Dell que vous avez créée.

6 Dans **Installation du système d'exploitation**, sélectionnez le type d'installation pour le système d'exploitation. Les options disponibles sont les suivantes :

- **Utilisation d'une image WIM du système d'exploitation**
- **Installation du système d'exploitation par script**

7 Sélectionnez un package de système d'exploitation dans le menu déroulant **Package de système d'exploitation à utiliser**.

8 Si vous disposez d'un package contenant **unattend.xml**, sélectionnez-le dans le menu **Package avec les informations unattend.xml**. Sinon, cliquez sur **<ne pas sélectionner maintenant>**.

9 Cliquez sur **Créer**.

La fenêtre **Séquence de tâches créée** apparaît et affiche le nom de la séquence de tâches que vous avez créée.

10 Cliquez sur **Close** (fermer) dans la zone de message de confirmation qui s'affiche.

Création d'une séquence de tâches personnalisée

1 Lancez Configuration Manager.

La console Configuration Manager s'affiche.

2 Dans le volet de gauche, sélectionnez **Bibliothèque logicielle** > **Aperçu** > **Systèmes d'exploitation** > **Séquences de tâches**.

3 Cliquez-droite sur **Séquences de tâches**, puis cliquez sur **Créer une séquence de tâches**.

L'**Assistant Création d'une séquence de tâches** s'affiche.

4 Sélectionnez **Créer une nouvelle séquence de tâches personnalisée**, puis cliquez sur **Suivant**.

5 Entrez le nom de la séquence de tâches, dans la zone de texte **Nom de la séquence de tâches** .

6 Recherchez l'image d'amorçage Dell que vous avez créée, puis cliquez sur **Suivant**.

L'écran **Confirmer les paramètres** s'affiche.

7 Examinez les paramètres, puis cliquez sur **Suivant**.

8 Cliquez sur **Fermer** dans la zone de message de confirmation qui s'affiche.

Editing a task sequence

À propos de cette tâche

REMARQUE : While editing task sequence on SCCM 2016, the missing objects references messages does not list Setup windows and ConfigMgr package. Add the package and then save the task sequence.

Étapes

1 Launch the Configuration Manager.

The Configuration Manager screen is displayed.

2 In the left pane, select **Software Library** > **Operating Systems** > **Task Sequence**.

3 Right-click the task sequence that you want to edit and click **Edit**.

The **Task Sequence Editor** window is displayed.

4 Click **Add** > **Dell Deployment** > **Apply Drivers from Dell Lifecycle Controller.**

The custom action for your Dell server deployment is loaded. You can now make changes to the task sequence.

REMARQUE : When editing a task sequence for the first time, the error message, Setup Windows and Configuration Manager is displayed. To resolve the error, create and select the Configurations Manager Client Upgrade package. For more information about creating packages, see the Configuration Manager documentation at technet.microsoft.com.

Définition d'un emplacement de partage par défaut pour le support de démarrage Lifecycle Controller

À propos de cette tâche

Pour définir un emplacement de partage par défaut pour le support de démarrage Lifecycle Controller :

Étapes

1 Dans **Configuration Manager**, sélectionnez **Administration** > **Configuration du site Sites**

2 Cliquez avec le bouton droit de la souris sur **<nom du serveur de site>** et sélectionnez **Configurer les composants du site**, puis sélectionnez **Gestion hors bande**.

La fenêtre **Propriétés de composant de gestion hors bande** apparaît.

3 Cliquez sur l'onglet **Lifecycle Controller**.

4 Sous **Emplacement de partage par défaut pour le support de démarrage Lifecycle Controller personnalisé**, cliquez sur **Modifier** pour modifier l'emplacement de partage par défaut du support de démarrage Lifecycle Controller personnalisé.

5 Dans la fenêtre **Modifier les informations de partage**, saisissez un nouveau nom de partage et un nouveau chemin de partage.

6 Cliquez sur **OK**.

Création d'un support de séquence de tâches (ISO de démarrage)

1 Dans Configuration Manager, sous **Bibliothèque de logiciels**, cliquez avec le bouton droit de la souris sur **Séquences de tâches** et sélectionnez **Créer un support de séquence de tâches**.

> **REMARQUE : Veillez à gérer et à mettre à jour l'image de démarrage au sein de tous les points de distribution avant de démarrer cet Assistant.**

> **REMARQUE : OMIMSSC ne prend pas en charge la méthode Supports autonomes pour créer des supports de séquence de tâches.**

2 À partir de l'**Assistant de support de séquence de tâches**, sélectionnez **Support amorçable**, sélectionnez l'option **Autoriser le déploiement du système d'exploitation sans assistance**, puis cliquez sur **Suivant**.

3 Sélectionnez **Ensemble de CD/DVD**, cliquez sur **Parcourir** et sélectionnez l'emplacement où vous souhaitez enregistrer l'image ISO.

4 Cliquez sur **Suivant**.

5 Décochez la case **Protéger le support à l'aide d'un mot de passe**, puis cliquez sur **Suivant**.

6 Naviguez et sélectionnez **Image d'amorçage du déploiement de Dell PowerEdge Server**.

> **REMARQUE : Utilisez l'image d'amorçage créée à l'aide de DTK uniquement.**

7 Sélectionnez le point de distribution dans le menu déroulant et cochez la case **Afficher les points de distribution des sites enfants**.

8 Cliquez sur **Suivant**.

L'écran **Résumé** affiche les informations concernant le support de la séquence de tâches.

9 Cliquez sur **Suivant**.

La barre de progression s'affiche.

10 Une fois l'image créée, fermez l'Assistant.

Preparing for non-Windows operating system deployment

Ensure that you remember the following points for deploying non-windows operating systems on managed systems:

- ISO file is available in either Network File System Version (NFS) or Common Internet File System (CIFS) share with read and write access.
- Confirm that virtual drive is available on the managed system.
- After deploying ESXi operating system, the server is moved to **Managed Lifecycle Controller (ESXi)** collection in SCCM.
- After deploying any type of non-windows operating system, the servers are moved to **Default Non-Windows Host Update Group**.
- It is recommended that the network adapter is connected to the network port in the server on which the operating system is being deployed.

7

Managing Operational Templates

Operational Templates contain complete device configuration and are used for deploying operating system and update firmware for PowerEdge servers and Modular Systems within Microsoft environment.

Operational Templates capture the complete configurations from a reference server, or reference Modular System. Then you can modify the hardware configurations, set firmware update attributes, and operating system parameters (only for servers) in an Operational Template if required and deploy this template across devices. Also, you can check the compliance status against an assigned Operational Template and view the compliance report in a summary page.

For information about reference server and reference Modular System, see About reference server configuration and About reference Modular System configuration.

The following table lists all the features that Operational Template supports:

Tableau 2. Functionality of OMIMSSC

Component	Configuration and deployment	Firmware update	View inventory	Operational Template compliance status
BIOS	Yes	Yes	Yes	Yes
iDRAC	Yes	Yes	Yes	Yes
NIC/CNA	Yes	Yes	Yes	Yes
RAID	Yes	Yes	Yes	Yes
FC	Yes	No	Yes	Yes
Windows	Yes	—	No	—
RHEL	Yes	—	No	—
ESXI	Yes	—	No	—
Management Module	Yes	Yes	Yes	Yes
PSU	No	No	No	No
Storage	No	No	No	No
Input/Output	No	No	No	No
Network Input/Output	No	No	No	No

Sujets :

- Predefined Operational Templates
- Creating Operational Template from reference servers
- Creating Operational Template from reference Modular Systems
- Viewing Operational Template
- Modifying Operational Template
- Deleting Operational Template
- Assigning Operational Template and running Operational Template compliance for servers

- Déploiement d'un Operational Template sur des serveurs
- Assigning Operational Template for Modular Systems
- Deploying Operational Template for Modular System
- Unassigning Operational Template

Predefined Operational Templates

Predefined templates have all the configurations that are required to create Storage Spaces Direct clusters or Windows Server Software-Defined (WSSD). OMIMSSC supports creating clusters on R740XD and R640 Storage Spaces Direct Ready Node models along with their specific network adapters.

Tableau 3. List of predefined Operational Templates

Operational Template name	Description
R740XD_Mellanox_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having Mellanox card.
R740XD_QLogic_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having QLogic card.
R640_Mellanox_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having Mellanox card.
R640_QLogic_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having QLogic card.

Consider the following points before deploying an Operational Template:

- The predefined templates are available only for management systems running SC2016 VMM.
- The predefined Storage Spaces Direct template shows NIC card in slot 1. However, while deploying the Operational Template the NIC configuration is applied on the right slot. And if there are multiple NIC cards on the device, all the NIC cards are configured with the same configuration that is specified in the Operational Template.

Creating Operational Template from reference servers

Prérequis

Avant de créer un Operational Template, assurez-vous que vous effectuez les tâches suivantes :

- Découvrez un serveur de référence à l'aide de la fonction **Découverte**. Pour en savoir plus sur la découverte des serveurs, reportez-vous à la section Découverte de serveurs par découverte manuelle.
- Pour les utilisateurs SCCM :
  - Créez une séquence de tâches. Pour plus d'informations, reportez-vous à la section Création d'une séquence de tâches.
  - Pour le déploiement d'un système non-Windows, vous devez disposer d'un profil de référence de type de périphérique. Pour plus d'informations, reportez-vous à la section Création d'un profil de référence.
- Pour les utilisateurs SCVMM :
  - Créez un profil d'hyperviseur. Pour plus d'informations sur la création d'un profil d'hyperviseur, reportez-vous à la section Création d'un profil d'hyperviseur.
  - Pour les déploiements Windows, vous devez disposer d'un profil de référence de type de périphérique. Pour plus d'informations, reportez-vous à la section Création d'un profil de référence.
- Si vous n'utilisez pas la source de mise à jour par défaut, créez une source de mise à jour. Pour plus d'informations, reportez-vous à la section Création d'une source de mise à jour.

À propos de cette tâche

You can create an Operational Template by capturing the configuration of the reference server. After capturing the configuration, you can directly save the template, or edit the attributes for update source, hardware configuration, and Windows component as per your requirement. Now you can save the template, which can be used on PowerEdge homogeneous servers.

Étapes

1 Dans OMIMSSC, effectuez l'une des opérations suivantes pour ouvrir un Operational Template :

- Dans le tableau de bord OMIMSSC, cliquez sur **Créer un modèle opérationnel**.
- Dans le volet de navigation, cliquez sur **ProfilsModèle opérationnel** et cliquez sur **Créer**.

L'Assistant **Modèle opérationnel** s'affiche.

2 Entrez le nom et la description du modèle.

3 Sélectionnez le type de périphérique, entrez l'adresse IP du périphérique de référence, puis cliquez sur **Suivant**.

REMARQUE : Vous pouvez capturer la configuration du serveur de référence à l'aide d'iDRAC 2.0 et versions supérieures.

4 Dans **Composants de périphérique**, cliquez sur un composant pour afficher les attributs disponibles et leurs valeurs.

Les composants sont les suivants :

- Mise à jour du micrologiciel
- Composants matériels (RAID, carte NIC et BIOS).

REMARQUE : Dans le composant iDRAC intégré 1, vous trouverez ci-dessous les privilèges et leurs valeurs pour l'attribut Privilège d'administrateur utilisateur.

Tableau 4. Tableau des valeurs de privilège

Valeur	Droits
1	Ouverture de session
2	Configuration
4	Configurer des utilisateurs
8	Journaux
16	Contrôle du système
32	Accéder à la console virtuelle
64	Accéder à Média Virtuel
128	Opérations système
256	Débogage
499	Privilèges d'opérateur

- Système d'exploitation : sélectionnez Windows, ESXi ou RHEL.

5 Utilisez la barre de défilement horizontal pour localiser un composant. Sélectionnez le composant, développez un groupe, puis modifiez ses valeurs d'attribut. Utilisez la barre de défilement vertical pour modifier un groupe et les attributs d'un composant.

6 Cochez la case en regard de chaque composant, car les configurations des composants sélectionnés sont appliquées sur le périphérique géré lorsque le Operational Template est appliqué. Cependant, toutes les configurations du périphérique de référence sont capturées et enregistrées dans le modèle.

REMARQUE : Indépendamment de la sélection des cases en regard de chaque composant, toutes les configurations sont capturées dans le modèle.

Dans le composant **Système d'exploitation**, suivez les étapes décrites dans l'une ou l'autre des options suivantes, selon vos besoins :

- Pour le déploiement de système d'exploitation Windows dans SCCM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour SCCM.
- Pour le déploiement de système d'exploitation Windows dans SCVMM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour SCVMM.
- OMIMSSC

- Pour le déploiement de système d'exploitation non-Windows, reportez-vous à la section Composant non-Windows pour les extensions de console OMIMSSC.

7 Pour enregistrer le profil, cliquez sur **Terminer**.

Windows OS component for OMIMSSC console extension for SCCM

À propos de cette tâche

While creating or editing Operational Template for server, perform the following steps for windows component:

Étapes

1 Sélectionnez une séquence de tâches et une méthode de déploiement.

REMARQUE : Seules les séquences de tâches déployées sur les collections sont répertoriées dans le menu déroulant.

Pour en savoir plus sur la séquence de tâches, reportez-vous à la section Séquence de tâches.

2 Sélectionnez l'une des options suivantes pour la **méthode de déploiement** :

- **Démarrer sur l'image ISO du réseau** : redémarre l'image ISO spécifiée.
- **Activer ISO sur la carte vFlash et redémarrer** : télécharge l'image ISO sur la carte vFlash et redémarre le système.
- **Redémarrer sur vFlash** : redémarre sur la carte vFlash. Assurez-vous que l'image ISO est présente sur la carte vFlash.

REMARQUE : Pour utiliser l'option Redémarrer sur vFlash, le nom d'étiquette de la partition créée sur vFlash doit être ISOIMG.

3 (Facultatif) Pour utiliser l'image présente dans le partage réseau, sélectionnez l'option **Utiliser l'image ISO réseau comme image de secours**.

4 Saisissez un fichier image de support d'amorçage.

5 Sélectionnez les pilotes nécessaires pour le système d'exploitation.

Windows component for OMIMSSC console extension for SCVMM

À propos de cette tâche

While creating or editing Operational Template for server, perform the following steps for windows component:

Étape

Sélectionnez **Profil d'hyperviseur**, **Profil de référence** et **Adresse IP de serveur à partir de**.

REMARQUE : Nom d'hôte et Carte NIC de gestion de serveur sont toujours des valeurs de pool.

Si vous sélectionnez **Adresse IP de serveur à partir de** en tant que **Statique**, assurez-vous que vous avez configuré le réseau logique dans SCVMM, et que les champs suivants sont des valeurs de pool :

- **Réseau logique de console**
- **Sous-réseau IP**
- **Adresse IP statique**

Non-Windows component for OMIMSSC console extensions

À propos de cette tâche

While creating or editing Operational Template for server, perform the following steps for non-windows component:

Étape

Sélectionnez un système d'exploitation non-Windows, la version du système d'exploitation, le type de dossiers de partage, le nom du fichier ISO, l'emplacement du fichier ISO et le mot de passe pour le compte root du système d'exploitation.

(Facultatif) Sélectionnez un profil de référence de type Windows pour l'accès au partage CIFS.

Nom d'hôte est une valeur de pool et si vous désactivez l'option DHCP, les champs suivants sont des valeurs de pool :

- **Adresse IP**
- **Masque de sous-réseau**
- **Passerelle par défaut**
- **DNS principal**
- **DNS secondaire**

REMARQUE : Les types de partages NFS (Network File System) et CIFS (Common Internet File System) sont pris en charge pour le déploiement de système d'exploitation non-Windows.

Creating Operational Template from reference Modular Systems

Prérequis

Avant de créer un Operational Template, assurez-vous que vous effectuez les tâches suivantes :

- Découvrez un système modulaire à l'aide de la fonction **Découverte**. Pour en savoir plus sur la découverte des systèmes modulaires, reportez-vous à la section Découverte des systèmes modulaires par découverte manuelle.
- Si vous n'utilisez pas la source de mise à jour par défaut, créez une source de mise à jour. Pour plus d'informations, reportez-vous à la section Création d'une source de mise à jour.

À propos de cette tâche

You can create an Operational Template by capturing the configuration of the reference Modular Systems. After capturing the configuration, you can directly save the template, or edit the attributes for update source and hardware configuration as per your requirement. Now you can save the template, that can be used to configure other Modular Systems of the same model.

REMARQUE : If you want to configure Active Directory (AD) users on other MX7000 devices ensure that you create an Operational Template from an MX7000 Modular System where all the AD users are configured.

REMARQUE : User account's passwords are not captured in Operational Template, from reference Modular System for security reasons. Edit the Operational Template to add a new user account and password, and then apply the Operational Template on the managed Modular Systems. Else, you can apply the Operational Template without any changes to user accounts, and the same passwords that are used in the reference Modular System are applied on the managed Modular System.

Étapes

1 Dans OMIMSSC, effectuez l'une des opérations suivantes pour ouvrir un Operational Template :

- Dans le tableau de bord OMIMSSC, cliquez sur **Créer un modèle opérationnel**.
- Dans le volet de navigation, cliquez sur **ProfilsModèle opérationnel** et cliquez sur **Créer**.

L'Assistant **Modèle opérationnel** s'affiche.

2 Entrez le nom et la description du modèle.

3 Dans **Composants de périphérique**, cliquez sur un composant pour afficher les attributs disponibles et leurs valeurs.

The components are as follows:

- Mise à jour du micrologiciel
- Management Module Embedded

REMARQUE : Ensure that the Web Server attribute is enabled. If this component is not enabled, and then the MX7000 Modular Systems cannot be accessed through OMIMSSC after deploying the Operational Template.

REMARQUE : For SNMP Configuration and Syslog Configuration, ensure that you select all four configurations available in each attribute, to apply them on managed devices.

4 Utilisez la barre de défilement horizontal pour localiser un composant. Sélectionnez le composant, développez un groupe, puis modifiez ses valeurs d'attribut. Utilisez la barre de défilement vertical pour modifier un groupe et les attributs d'un composant.

5 Cochez la case en regard de chaque composant, car les configurations des composants sélectionnés sont appliquées sur le périphérique géré lorsque le Operational Template est appliqué. Cependant, toutes les configurations du périphérique de référence sont capturées et enregistrées dans le modèle.

6 Pour enregistrer le profil, cliquez sur **Terminer**.

Viewing Operational Template

To view Operational Templates created:

In OMIMSSC console, click **Profiles and Templates**, and then click **Operational Template**. All the templates that are created are listed here.

Modifying Operational Template

À propos de cette tâche

You can modify the update source, hardware configurations, and operating system of an operational template.

Consider the following before modifying an Operational Template:

- The values of few attributes depend on the values of other attributes. When you change attribute values manually, ensure that you also change the interdependent attributes. If these interdependent values are not changed appropriately, and then applying the hardware configurations may fail. Hence, Dell EMC recommends that you do not edit these configurations that are captured in an Operational Template.
- The step to modify predefined Operational Templates and custom created Operational Templates are the same.
- (For SCCM users and servers only) When editing a task sequence on SCCM 2016, the **missing objects references** messages do not list the **Setup windows and ConfigMgr** package. Hence, you must add the package and then save the task sequence.
- (For SCVMM users and servers only) All the Storage Spaces Direct specific attributes are read-only attributes in the predefined Storage Spaces Direct template. However, you can edit the name of the template, operating system components, and hardware configurations.

REMARQUE : The steps to modify any Operational Template are the same.

Étapes

1 Select the template that you want to modify and click **Edit**.

The Operational Template page is displayed.

2 (Optional) Edit the name and description of the template, and then click **Next**.

3 To view the available attributes and their values in **Device Components**, click a component.

4 Modify the values of the available attributes.

REMARQUE : Select the check box against each component since only the selected component's configurations are applied on the managed system, when the Operational Template is applied.

REMARQUE : When editing Operational Template, few Advanced Host Controller Interface (AHCI) component attributes that are read-only are listed as editable. However, when these read-only attributes are set and the Operational Template is deployed, there are no changes that are made to the device.

- For MX7000 Modular Systems:
  - Configurations are applied only if all the attributes for a group are selected. Hence, ensure that you select all the attributes in a group, even if you want to change one of the attributes in the group.
  - To add a new user through an Operational Template, select all the attributes of existing users that were exported when capturing the Operational Template, select the recently added user groups, and save the Operational Template.
  - To provide the time zone values, see Appendix.

5 For the operating system component, perform either of the following tasks depending on your requirement:

- Pour le déploiement de système d'exploitation Windows dans SCCM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour SCCM.

- Pour le déploiement de système d'exploitation Windows dans SCVMM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour SCVMM.
- OMIMSSC
- Pour le déploiement de système d'exploitation non-Windows, reportez-vous à la section Composant non-Windows pour les extensions de console OMIMSSC.

6 To save the profile, click **Finish**.

Deleting Operational Template

To delete an Operational Template, perform the following steps:

À propos de cette tâche

Before deleting an Operational Template, ensure that:

- The selected Operational Template is not associated with any server or Modular System. If it is associated with a device, and then, unassign the template and then delete the template.
- No jobs that are associated with Operational Template are running.
- You have not selected a predefined Operational Template, since you cannot delete a predefined template.
- The steps to delete any type of Operational Template are the same.

Étape

Select the templates that you want to delete and click **Delete**. To confirm, click **Yes** .

Assigning Operational Template and running Operational Template compliance for servers

Assign an Operational Template to a server, and run the Operational Template compliance. Only after assigning an Operational Template to a server, you can view its Operational Template compliance status. You can compare a server's configuration with an Operational Template by assigning the template to a server. Once you assign an Operational Template, the compliance job runs and the Operational Template status is displayed on completion.

À propos de cette tâche

To assign an Operational Template, perform the following steps:

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**. Sélectionnez les serveurs requis et cliquez sur **Attribuer un modèle opérationnel et exécuter la conformité**.

La page **Attribuer un Operational Template et exécuter la conformité** s'affiche.

2 Sélectionnez le modèle dans le menu déroulant **Operational Template**, entrez un nom de tâche, puis cliquez sur **Attribuer**.

La liste déroulante Operational Template répertorie les modèles du même type que celui des périphériques sélectionnés dans l'étape précédente.

Si le périphérique est conforme au modèle, une case de couleur **verte** cochée s'affiche.

Si le Operational Template n'est pas appliqué avec succès sur le périphérique ou si le composant matériel dans Operational Template n'est pas sélectionné, une case avec un symbole d'**information** s'affiche.

Si le périphérique n'est pas conforme au modèle, un symbole d'**avertissement** s'affiche. Uniquement dans le cas où le périphérique n'est pas conforme au Operational Template attribué, vous pouvez afficher un rapport récapitulatif en cliquant sur le lien du nom de modèle. La page **Operational Template - Rapport récapitulatif** affiche un rapport récapitulatif des différences qui existent entre le modèle et le périphérique.

Pour afficher un rapport détaillé, effectuez les étapes suivantes :

a Cliquez sur **Afficher la conformité détaillée**. Ici, les composants dont les valeurs d'attribut diffèrent de celles du modèle attribué s'affichent. Les couleurs indiquent les différents états de la conformité au Operational Template.

- Symbole d'avertissement de couleur jaune : non-conformité. Indique que la configuration du périphérique ne correspond pas aux valeurs du modèle.
- Case de couleur rouge : indique que le composant n'est pas présent sur le périphérique.

Déploiement d'un Operational Template sur des serveurs

Prérequis

Pour déployer un système d'exploitation sur des serveurs gérés, assurez-vous que vous disposez de l'article KB 4093492 ou une version supérieure installée sur votre système de gestion et sur l'image de système d'exploitation qui est utilisée pour le déploiement.

À propos de cette tâche

Vous pouvez déployer un système d'exploitation Windows et non-Windows (ESXi et RHEL) en déployant le Operational Template attribué aux serveurs.

REMARQUE : Téléchargez et installez les pilotes appropriés depuis le site Dell.com/support si un point d'exclamation jaune s'affiche sous Gestionnaire de périphériques après le déploiement du système d'exploitation Windows 2016 sur les serveurs de 12e génération.

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**. Sélectionnez les serveurs sur lesquels vous souhaitez déployer un modèle, puis cliquez sur **Déployer Operational Template**.

La page **Déployer** Operational Template s'affiche.

2 (Facultatif) Pour exporter tous les attributs qui sont marqués comme valeurs de pool dans le modèle sélectionné vers un fichier CSV, cliquez sur **Exporter les attributs de pool**. Sinon, passez à l'étape 4.

REMARQUE : Avant d'exporter les valeurs de pool, ajoutez l'adresse IP de l'appliance OMIMSSC dans laquelle l'extension de console OMIMSSC est installée au site intranet local. Pour plus d'informations sur l'ajout de l'adresse IP dans le navigateur IE, consultez la section *Browser settings* (Paramètres du navigateur) du document *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide* (Guide d'installation de Dell EMC OpenManage Integration for Microsoft System Center version 7.1 pour System Center Configuration Manager et System Center Virtual Machine Manager).

3 Si vous avez exporté les valeurs de pool, entrez les valeurs de tous les attributs qui sont marqués comme valeurs de pool dans le fichier CSV et enregistrez le fichier. Dans **Pool de valeurs d'attribut**, sélectionnez ce fichier pour l'importer.

Le format d'un fichier CSV est attribute-value-pool.csv.

REMARQUE : Assurez-vous de sélectionner un fichier CSV qui a tous les attributs corrects et l'adresse IP iDRAC, sinon les informations d'identification iDRAC ne sont pas modifiées en raison du modèle, étant donné que la tâche n'est pas suivie par OMIMSSC après la modification de l'adresse IP iDRAC ou des informations d'identification iDRAC et qu'elle est marquée comme étant en échec bien que la tâche puisse être réussie dans iDRAC.

4 Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Déployer**.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Assigning Operational Template for Modular Systems

Assign an Operational Template to a Modular System and run the Operational Template compliance. This operation compares the configuration of a Modular System and an Operational Template by assigning the selected template to a Modular System. After you assign an Operational Template, the compliance job runs and the compliance status is displayed on completion.

À propos de cette tâche

To assign an Operational Template for Modular Systems, perform the following steps:

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement** et cliquez sur **Vue Systèmes modulaires**. Sélectionnez le système modulaire requis et cliquez sur **Attribuer un Modèle opérationnel**.

La page **Attribuer Operational Template** s'affiche.

2 Sélectionnez le modèle dans le menu déroulant **Operational Template**, entrez un nom de tâche, puis cliquez sur **Attribuer**.

Si le périphérique est conforme au modèle, une case de couleur **verte** cochée s'affiche.

Si le Operational Template n'est pas appliqué avec succès sur le périphérique ou si le composant matériel dans Operational Template n'est pas sélectionné, une case avec un symbole d'**information** s'affiche.

REMARQUE : The Operational Template compliance status excludes any changes that are made to user attributes.

Si le périphérique n'est pas conforme au modèle, un symbole d'**avertissement** s'affiche. Uniquement dans le cas où le périphérique n'est pas conforme au Operational Template attribué, vous pouvez afficher un rapport récapitulatif en cliquant sur le lien du nom de modèle. La page **Operational Template - Rapport récapitulatif** affiche un rapport récapitulatif des différences qui existent entre le modèle et le périphérique.

Pour afficher un rapport détaillé, effectuez les étapes suivantes :

a Cliquez sur **Afficher la conformité détaillée**. Ici, les composants dont les valeurs d'attribut diffèrent de celles du modèle attribué s'affichent. Les couleurs indiquent les différents états de la conformité au Operational Template.

- Symbole d'avertissement de couleur jaune : non-conformité. Indique que la configuration du périphérique ne correspond pas aux valeurs du modèle.
- Case de couleur rouge : indique que le composant n'est pas présent sur le périphérique.

Deploying Operational Template for Modular System

À propos de cette tâche

You can configure Modular System components, and update the Modular System firmware versions by deploying the assigned Operational Template.

REMARQUE : In a Multi-Chassis Management (MCM), if lead chassis is configured with Propagation to member chassis, and then configuring and updating lead chassis and member chassis from OMIMSSC will override the changes done through propagation.

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement** et cliquez sur **Vue Systèmes modulaires**. Sélectionnez le système modulaire sur lequel vous avez attribué le modèle, puis cliquez sur **Déployer un Operational Template**.

La page **Déployer un Operational Template** s'affiche.

2 (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.

3 Si vous avez exporté les valeurs de pool, entrez les valeurs de tous les attributs qui sont marqués comme valeurs de pool dans le fichier CSV et enregistrez le fichier. Dans **Pool de valeurs d'attribut**, sélectionnez ce fichier pour l'importer.

Le format d'un fichier CSV est attribute-value-pool.csv.

REMARQUE : Ensure that you select a .CSV file which has all proper attributes and the CMC IP or CMC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the CMC IP or CMC credentials changes.

4 Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Déployer**.

REMARQUE : There are no supported system-specific pool value attributes for Modular System. Hence, there are no pool values to be exported.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Unassigning Operational Template

1 In OMIMSSC, perform any one of the following tasks:

- Click **Configuration and Deployment**, and click **Server View**.

- Click **Configuration and Deployment**, and click **Modular System View**.

Select the required devices and click **Assign Operational Template and Run Compliance**.

The **Assign Operational Template and Run Compliance** page is displayed.

2 Select **Unassign** from **Operational Template** drop-down menu, and click **Assign**.
Operational Template is unassigned to selected devices.

8

Firmware update in OMIMSSC

Maintain Dell EMC devices up-to-date by upgrading to the latest firmware to use security, issue fixes, and enhancements, using OMIMSSC. Update the firmware of devices using Dell EMC update repositories.

Updating firmware is supported only on hardware compatible devices. For using the features available in OMIMSSC on the managed devices, the managed devices must have the minimum required firmware versions of iDRAC, Lifecycle Controller (LC), and BIOS. Devices having the required firmware versions are hardware compatible.

Sujets :

About update groups

Update groups are a group of devices that require similar update management. There are two types of update groups that are supported in OMIMSSC:

- Predefined update groups—You cannot manually create, modify, or delete the predefined update groups.
- Custom update groups—You can create modify and delete devices in these groups.

REMARQUE : All server groups that exist in SCVMM are listed in OMIMSSC. However, the list of servers in OMIMSSC is not user-specific. Therefore, ensure that you have access to perform any operations on those devices.

Predefined update groups

After discovering a device, the discovered device is added to one of the following predefined groups.

- **Default host groups**—this group consists of servers that are deployed with Windows operating system or are synchronized with a registered Microsoft console.
- **Default unassigned groups**—this group consists of unassigned or bare-metal servers discovered.
- **Default non-windows host groups**—this group consists of servers that are deployed with non-windows operating systems.
- **Chassis update groups**—this group consists of modular servers and chassis or Modular Systems. 12th generation of servers and later are discovered along with their chassis information. By default, a group is created with the following name format, **Chassis-Service-tag-of-Chassis-Group**. For example, `Chassis-GJDC4BS-Group`. If a modular server is deleted from a cluster update group, and then the server is added to the chassis update group along with its CMC information. Even if there are no modular servers in the corresponding chassis update group, since all modular servers in the chassis are in a cluster update group, the chassis update group continues to exist, but displays only the CMC information.
- **Cluster update groups**—this group consists of **Windows Server Failover clusters**. If a 12th generation and later modular server is part of cluster, and then the CMC information is also added in the inventory in the **Maintenance Center** page.

Custom update groups

Create custom update groups of type **Generic update groups** by adding the discovered devices into groups that require similar management. However, you can add a device into a custom update group only from **Default unassigned update groups** and **Default host update groups**. To add the servers in custom update group, search for the required device using their service tag. After you add a device into a custom update group, the device is removed from the predefined update group and is available, only in the custom update group.

Viewing update groups

To view update groups:

1 In **OMIMSSC**, click **Maintenance Center** and then click **Maintenance Settings**.

2 In **Maintenance Settings**, click **Update Groups**.

All the custom groups created are displayed with name, group type, and number of servers in the group.

Création de groupes mise à jour personnalisée

1 Dans la console OMIMSSC, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.

2 Dans **Paramètres de maintenance**, cliquez sur **Groupes de mise à jour**, puis cliquez sur **Créer**.

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

3 Indiquez un nom de groupe et une description, puis sélectionnez le type de groupe de mise à jour à créer.

Les groupes de mise à jour personnalisée peuvent avoir des serveurs uniquement des types de groupes de mise à jour suivants :

- Groupe de mise à jour générique : contient les serveurs des groupes de mise à jour non attribués par défaut et des groupes de mise à jour d'hôte par défaut.
- Groupe de mise à jour d'hôte : contient les serveurs des groupes de mise à jour d'hôte par défaut.

En outre, vous pouvez avoir une combinaison de serveurs des deux types de groupes de serveurs.

4 Pour ajouter des serveurs au groupe de mise à jour, recherchez les serveurs à l'aide de leur numéro de série, et pour ajouter des serveurs dans la table **Serveurs inclus dans le groupe de mise à jour**, cliquez sur la flèche droite.

5 Pour créer le groupe de mise à jour personnalisée, cliquez sur **Enregistrer**.

Modification des groupes de mise à jour personnalisée

À propos de cette tâche

Tenez compte des aspects suivants lorsque vous modifiez un groupe de mise à jour personnalisé :

- Vous ne pouvez pas modifier le type d'un groupe de mise à jour après avoir créé un groupe.
- Pour transférer des serveurs d'un groupe de mise à jour personnalisé vers un autre, vous pouvez :
  - a Retirer le serveur d'un groupe de mise à jour personnalisé existant. Il est alors automatiquement ajouté au groupe de mise à jour prédéfini.
  - b Modifier le groupe personnalisé pour y ajouter le serveur, puis rechercher ce dernier en utilisant le numéro de service.

Étapes

1 Dans **OMIMSSC**, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.

2 Dans **Paramètres de maintenance**, cliquez sur **Groupes de mise à jour**, sélectionnez le groupe de mise à jour, puis cliquez sur **Modifier** pour modifier le groupe de mise à jour.

Suppression de groupes mise à jour personnalisée

À propos de cette tâche

Tenez compte des points suivants lorsque vous supprimez un groupe de mise à jour personnalisée dans les cas suivants :

- Vous ne pouvez pas supprimer un groupe de mise à jour auquel est associée une tâche planifiée, en cours ou en attente. Par conséquent, supprimez les tâches planifiées qui sont associées à un groupe de mise à jour personnalisée avant de supprimer le groupe de serveurs.
- Vous pouvez supprimer un groupe de mise à jour même si des serveurs sont présents dans ce groupe de mise à jour. Cependant, après avoir supprimé un tel groupe de mise à jour, les serveurs sont déplacés vers leurs groupes de mise à jour prédéfinis respectifs.
- Si un périphérique qui est présent dans un groupe de mise à jour personnalisée est supprimé de MSSC, et que vous synchronisez OMIMSSC avec la console MSSC inscrite, le périphérique est supprimé du groupe de mise à jour personnalisée et est déplacé dans le groupe prédéfini approprié.

Étapes

1 Dans **OMIMSSC**, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.

2 Dans **Paramètres de maintenance**, cliquez sur **Groupes de mise à jour**, sélectionnez le groupe de mise à jour, puis cliquez sur **Supprimer** pour supprimer le groupe mise à jour.

À propos des sources de mise à jour

Les sources de mise à jour contiennent une référence aux fichiers de catalogue qui contiennent les mises à jour Dell EMC (BIOS, packs de pilotes tels que les composants de gestion, cartes réseau) et le fichier exécutable autonome appelé DUP (Dell Update Packages, packages de mise à jour Dell).

Vous pouvez créer une source de mise à jour ou un référentiel, et le définir en tant que source de mise à jour par défaut pour générer un rapport de comparaison, et recevoir des alertes lorsque de nouveaux fichiers de catalogue sont disponibles dans le référentiel.

À l'aide d'OMIMSSC, vous pouvez maintenir le micrologiciel des périphériques à jour à l'aide de sources de mise à jour en ligne ou hors ligne.

Les sources de mise à jour en ligne sont des référentiels qui sont gérés par Dell EMC.

Les sources de mise à jour hors ligne sont des référentiels locaux et utilisés lorsqu'il n'existe aucune connexion Internet.

Il est recommandé de créer des référentiels personnalisés et de placer le partage réseau dans l'intranet local de l'appliance OMIMSSC. Cela permet d'économiser la bande passante Internet et également de fournir un référentiel interne sécurisé.

Mettez à jour le micrologiciel à l'aide des sources de mise à jour suivantes :

- **Référentiel DRM** : référentiel hors ligne. Exportez les informations d'inventaire des périphériques découverts à partir de l'appliance OMIMSSC pour préparer un référentiel dans DRM. Pour en savoir plus sur l'intégration avec DRM et la création d'une source de mise à jour via DRM, reportez-vous à la section Intégration avec DRM. Après la création d'un référentiel dans DRM, dans OMIMSSC, sélectionnez la source de mise à jour qui est créée via DRM, et les périphériques appropriés, et exécutez une mise à jour sur les périphériques. Pour en savoir plus sur DRM, consultez les documents relatifs à *Dell Repository Manager* à l'adresse **dell.com\support**.
- **FTP, HTTP ou HTTPS** : peut être un référentiel en ligne ou hors ligne. Mettez à jour les composants spécifiques des appareils par rapport à la dernière mise à jour fournie sur le site FTP, HTTP ou HTTPS. Dell EMC prépare un référentiel tous les deux mois et publie les mises à jour suivantes via les catalogues PDK :
  - BIOS et micrologiciel du serveur
  - Packs de pilotes de système d'exploitation certifiés par Dell EMC : pour le déploiement du système d'exploitation

    REMARQUE : Si vous sélectionnez une source de mise à jour en ligne, lors du déploiement du Operational Template, les dernières versions de micrologiciel sont téléchargées et appliquées sur les périphériques gérés. Par conséquent, les versions de micrologiciel peuvent varier entre le périphérique de référence et le périphérique déployé.
- **Inventaire de micrologiciel de référence et comparaison** : peut être converti en un référentiel hors ligne via DRM. Créez un fichier d'inventaire de référence qui contient l'inventaire de micrologiciel des périphériques sélectionnés. Le fichier d'inventaire de référence peut contenir des informations d'inventaire d'un périphérique du même type ou du même modèle, ou peut avoir plusieurs périphériques

de différents types ou modèles. Vous pouvez comparer les informations d'inventaire des périphériques présents dans OMIMSSC par rapport au fichier d'inventaire de référence enregistré. Pour transmettre le fichier exporté à DRM et créer un référentiel, consultez les documents relatifs à *Dell Repository Manager* disponibles à l'adresse **dell.com\support**.

Source de mise à jour prédéfinie et par défaut

OMIMSSC inclut trois sources de mise à jour prédéfinies qui sont disponibles après une nouvelle installation ou une mise à niveau. **CATALOGUE FTP EN LIGNE DELL** est une source de mise à jour prédéfinie de type FTP, **CATALOGUE HTTP EN LIGNE DELL** est une source de mise à jour prédéfinie de type HTTP et **CATALOGUE HTTPS EN LIGNE DELL** est une source de mise à jour par défaut prédéfinie de type HTTPS. Cependant, vous pouvez créer une autre source de mise à jour et la marquer comme une source de mise à jour par défaut.

REMARQUE : Si vous utilisez un serveur proxy pour accéder au référentiel, modifiez la source de mise à jour pour ajouter les détails du serveur proxy et enregistrez les modifications.

Sources de mise à jour prédéfinie et par défaut pour les clusters d'Storage Spaces Direct

OMIMSSC prend en charge la mise à jour des clusters d'Storage Spaces Direct via des sources de mise à jour prédéfinies spécifiques. Ces sources de mise à jour font référence aux fichiers de catalogue qui contiennent les versions de micrologiciel les plus récentes et recommandées des composants pour les clusters d'Storage Spaces Direct. Elles sont répertoriées uniquement sur la page **Centre de maintenance**.

CATALOGUE FTP EN LIGNE DELL S2D est une source de mise à jour prédéfinie de type FTP, qui fait partie de **CATALOGUE FTP EN LIGNE DELL**.

CATALOGUE HTTP EN LIGNE DELL S2D est une source de mise à jour prédéfinie de type HTTP, qui fait partie de **CATALOGUE HTTP EN LIGNE DELL**.

CATALOGUE HTTPS EN LIGNE DELL S2D est une source de mise à jour prédéfinie par défaut de type HTTPS, qui fait partie de **CATALOGUE HTTPS EN LIGNE DELL**.

Sources de mise à jour prédéfinie et par défaut pour les systèmes modulaires

OMIMSSC prend en charge la mise à jour des systèmes modulaires via des sources de mise à jour prédéfinies spécifiques. Ces sources de mise à jour font référence aux fichiers de catalogue qui contiennent les versions de micrologiciel les plus récentes et recommandées des composants pour les systèmes modulaires. Elles sont répertoriées uniquement sur la page **Centre de maintenance**.

CATALOGUE MX7000 FTP EN LIGNE DELL est une source de mise à jour prédéfinie de type FTP, qui fait partie de **CATALOGUE FTP EN LIGNE DELL**.

CATALOGUE MX7000 HTTP EN LIGNE DELL est une source de mise à jour prédéfinie de type HTTP, qui fait partie de **CATALOGUE HTTP EN LIGNE DELL**.

CATALOGUE MX7000 HTTPS EN LIGNE DELL est une source de mise à jour prédéfinie par défaut de type HTTPS, qui fait partie de **CATALOGUE HTTPS EN LIGNE DELL**.

Validation des données à l'aide d'un test de connexion

Utilisez **Tester la connexion** pour vérifier que l'emplacement de la source de mise à jour est accessible en utilisant les informations d'identification mentionnées lors de la création de la source de mise à jour. Vous êtes autorisé à créer une source de mise à jour uniquement une fois la connexion réussie.

Setting up local FTP

To set up local FTP:

1 Create a folder structure in your local FTP that is an exact replica of the online FTP, **ftp.dell.com**.
2 Download the **catalog.gz** file from online FTP and unzip the files.
3 Open the **catalog.xml** file and change the **baseLocation** to your local FTP URL, and compress the file with **.gz** extension.
For example, change the **baseLocation** from `ftp.dell.com` to **ftp.yourdomain.com**.
4 Place the catalog file and the DUP files in your local FTP folder replicating the same structure as in **ftp.dell.com**.

Configuration de HTTP local

À propos de cette tâche
Pour configurer le HTTP local :
Étapes
1 Créez une structure de dossiers dans votre HTTP local qui est une réplique exacte de **downloads.dell.com**.
2 Téléchargez le fichier **catalog.gz** à partir du HTTP en ligne depuis l'emplacement **http://downloads.dell.com/catalog/catalog.xml.gz** et extrayez les fichiers.
3 Extrayez le fichier **catalog.xml** et remplacez l'entrée **baseLocation** par votre URL HTTP locale, puis compressez le fichier avec l'extension **.gz**.
Par exemple, modifiez l'entrée **baseLocation** downloads.dell.com par un nom d'hôte ou une adresse IP, telle que **hostname.com**.
4 Placez le fichier de catalogue avec le fichier de catalogue modifié, et les fichiers DUP dans votre dossier HTTP local en utilisant la même structure que dans **downloads.dell.com**.

Configuration du HTTPS local

À propos de cette tâche
Pour configurer le HTTPS local :
Étapes
1 Créez une structure de dossiers dans votre HTTPS local qui est une réplique exacte de **downloads.dell.com**.
2 Téléchargez le fichier **catalog.gz** à partir du HTTPS en ligne depuis l'emplacement **https://downloads.dell.com/catalog/catalog.xml.gz** et extrayez les fichiers.
3 Extrayez le fichier **catalog.xml** et remplacez l'entrée **baseLocation** par votre URL HTTPS locale, puis compressez le fichier avec l'extension **.gz**.
Par exemple, modifiez l'entrée **baseLocation** downloads.dell.com par un nom d'hôte ou une adresse IP, telle que **hostname.com**.
4 Placez le fichier de catalogue avec le fichier de catalogue modifié et les fichiers DUP dans votre dossier HTTPS local en utilisant la même structure que dans **downloads.dell.com**.

Affichage de la source de mise à jour

1 Dans **OMIMSSC**, cliquez sur **Centre de maintenance**.

2 Dans **Centre de maintenance**, cliquez sur **Paramètres de maintenance**, puis sur **Source de mise à jour**.

Toutes les sources de mise à jour créées s'affichent en même temps que leur description, le type de source, l'emplacement et le nom du profil de référence.

Création d'une source de mise à jour

Prérequis

- Selon le type de la source de mise à jour, assurez-vous qu'un profil de référence Windows ou FTP est disponible.
- Assurez-vous que vous installez et configurez DRM avec des rôles d'administrateur, si vous créez une source de mise à jour DRM.

Étapes

1 Dans la console OMIMSSC, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.

2 Dans la page **Source de mise à jour**, cliquez sur **Créer** et indiquez un nom et une description pour la source de mise à jour.

3 Sélectionnez l'un des types suivants de sources de mise à jour à partir du menu déroulant **Type de source** :

- Sources FTP : sélectionnez cette option pour créer une source de mise à jour FTP en ligne ou locale.

  REMARQUE : Si vous créez une source FTP, indiquez vos références FTP, ainsi que les références de proxy si le site FTP est accessible avec références de proxy.

- Sources HTTP : sélectionnez cette option pour créer une source de mise à jour HTTP en ligne ou locale.

  REMARQUE : Si vous créez une source de mise à jour de type HTTP, fournissez le chemin complet du catalogue avec son nom et vos références de proxy pour accéder à la source de mise à jour.

- Sources HTTPS : sélectionnez cette option pour créer une source de mise à jour HTTPS en ligne.

  REMARQUE : Si vous créez une source de mise à jour de type HTTPS, fournissez le chemin complet du catalogue avec son nom et vos informations d'identification de proxy pour accéder à la source de mise à jour.

  Référentiel DRM : sélectionnez cette option pour créer une source de mise à jour de référentiel locale. Assurez-vous que vous avez installé DRM.

  REMARQUE : Si vous créez une source DRM, indiquez vos informations d'identification Windows et assurez-vous que l'emplacement partagé Windows est accessible. Dans le champ d'emplacement, indiquez le chemin complet du fichier de catalogue avec le nom du fichier.

- Fichiers de sortie d'inventaire : sélectionnez cette option pour afficher l'inventaire de micrologiciel par rapport à la configuration de serveur de référence.

  REMARQUE : Vous pouvez afficher un rapport de comparaison en utilisant Fichiers de sortie d'inventaire comme source de mise à jour. Les informations d'inventaire du serveur de référence sont comparées à tous les autres serveurs qui sont découverts dans OMIMSSC.

4 Dans **Emplacement**, indiquez l'URL de la source de mise à jour d'une source FTP, HTTP ou HTTPS et l'emplacement partagé Windows pour DRM.

REMARQUE : Le site FTP local doit répliquer le FTP en ligne.

REMARQUE : Le site HTTP local doit répliquer le HTTP en ligne.

REMARQUE : L'indication de HTTP ou HTTPS dans l'URL pour une source FTP n'est pas obligatoire.

5 Pour accéder à la source de mise à jour, sélectionnez le profil de référence requis dans **Informations d'identification**.

6 Dans **Informations d'identification de proxy**, sélectionnez les informations d'identification de proxy appropriées si un proxy est requis pour accéder à la source FTP ou HTTP.

7 (Facultatif) Pour désigner la source de mise à jour créée comme source de mise à jour par défaut, sélectionnez **Désigner comme source par défaut**.

8 Pour vérifier que l'emplacement de la source de mise à jour est accessible à l'aide des informations d'identification mentionnées, cliquez sur **Tester la connexion**, puis cliquez sur **Enregistrer**.

REMARQUE : Vous pouvez créer la source de mise à jour uniquement si la connexion test a réussi.

Modification de la source de mise à jour

À propos de cette tâche

Tenez compte des points suivants avant de modifier une source de mise à jour :

- Pour modifier la source de mise à jour **CATALOGUE S2D FTP EN LIGNE DELL**, **CATALOGUE S2D HTTP EN LIGNE DELL** ou **CATALOGUE S2D HTTPS EN LIGNE DELL**, modifiez la source de mise à jour prédéfinie respective et enregistrez les modifications. Cette mise à jour est reflétée dans la source de mise à jour **CATALOGUE S2D FTP EN LIGNE DELL**, **CATALOGUE S2D HTTP EN LIGNE DELL** ou **CATALOGUE S2D HTTPS EN LIGNE DELL**.
- Vous ne pouvez pas modifier le type d'une source de mise à jour, ni son emplacement, une fois que cette source de mise à jour a été créée.
- Vous pouvez modifier une source de mise à jour, même si la source de mise à jour est en cours d'utilisation par une tâche en cours ou une tâche planifiée, ou si elle est utilisée dans un modèle de déploiement. Un message d'avertissement s'affiche pendant la modification de la source de mise à jour en cours d'utilisation. Cliquez sur **Confirmer** pour accéder aux modifications.
- Lorsqu'un fichier de catalogue est mis à jour dans la source de mise à jour, le fichier de catalogue mis en cache localement n'est pas mis à jour automatiquement. Pour mettre à jour le fichier de catalogue enregistré dans la mémoire cache, modifiez la source de mise à jour ou supprimez et recréez la source de mise à jour.

Étape

Sélectionnez la source de mise à jour à modifier, cliquez sur **Modifier** et mettez à jour la source selon vos besoins.

Deleting update source

À propos de cette tâche

Consider the following points before, deleting an update source:

- You cannot delete a predefined update source.
- You cannot delete an update source if it is used in an in-progress, or a scheduled job.
- You cannot delete an update source if it is a default update source.

Étape

Select the update source that you want to delete, and click **Delete**.

Integration with Dell EMC Repository Manager(DRM)

OMIMSSC is integrated with DRM to create custom update sources in OMIMSSC. The integration is available from DRM version 2.2 onwards. Provide the discovered device information from OMIMSSC Appliance to DRM, and using the available inventory information, you can create a custom repository in DRM and set it as an update source in OMIMSSC for performing firmware updates and creating clusters on managed devices. For more information about creating a repository in DRM, see *Dell EMC Repository Manager* documents available at Dell.com/support/home.

Integrating DRM with OMIMSSC

À propos de cette tâche

REMARQUE : Consider factors such as testing on test environment, security updates, application recommendations, Dell EMC advisories, to prepare the required updates.

REMARQUE : To view the latest inventory information about discovered devices, after upgrading OMIMSSC, reintegrate DRM with OMIMSSC Appliance.

Étapes

1 Launch the **Dell Repository Manager Data Center** version.

2 Click **My Repositories**, click **New**, and then click **Dell OpenManage Essentials (OME) inventory**.

3 Enter the **URL (Rest API)** in the following format: `https:// IP address of appliance/genericconsolerepository/` and then click **Next**.

4 Provide the user name and password of OMIMSSC Appliance, click **OK**. To confirm your selection, click **OK**.

Étape suivante

After integrating DRM with OMIMSSC, see *Obtain firmware catalog for Storage Spaces Direct Ready Nodes Using Dell Repository Manager* section from *Dell EMC Microsoft Storage Spaces Direct Ready Node Operations Guide for managing and monitoring Ready Node life cycle* at dell.com/support

Setting polling frequency

Configure polling and notifications, to receive alerts when there is a new catalog file available at the update source, that is selected as default. OMIMSSC Appliance saves a local cache of the update source. The color of the notification bell changes to orange color when there is a new catalog file available at the update source. To replace the locally cached catalog available in OMIMSSC Appliance, click the bell icon. After replacing the old catalog file with the latest catalog file, the bell color changes to green.

À propos de cette tâche

To set the polling frequency:

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, puis cliquez sur **Interrogation et notification**.

2 Select how frequently the polling should happen:

- **Never**—this option is selected by default. Select to never receive any updates.
- **Once a week**—select to receive updates about new catalogs available at update source on a weekly basis.
- **Once every 2 weeks**—select to receive updates about new catalogs available at update source once every two weeks.
- **Once a month**—select to receive updates about new catalogs available at update source on a monthly basis.

Affichage et actualisation de l'inventaire de périphérique

Affichez le rapport de comparaison pour les périphériques par rapport à une source de mise à jour dans la page **Centre de maintenance**. Lors de la sélection d'une source de mise à jour, un rapport s'affiche comparant le micrologiciel existant au micrologiciel présent dans la source de mise à jour sélectionnée. Le rapport est généré dynamiquement lors de la modification de la source de mise à jour. L'inventaire du serveur est comparé avec la source de mise à jour, et des actions recommandées sont répertoriées. Cette activité prend beaucoup de temps en fonction du nombre de périphériques et de composants de périphérique présents. Vous ne pouvez pas effectuer d'autres tâches au cours de ce processus. L'actualisation de l'inventaire actualise l'ensemble de l'inventaire du périphérique, même si vous sélectionnez un seul composant de ce périphérique.

À propos de cette tâche

Parfois, l'inventaire du périphérique est mis à jour, mais la page n'affiche pas l'inventaire le plus récent. Par conséquent, vous devez utiliser l'option d'actualisation pour afficher les dernières informations d'inventaire des périphériques découverts.

REMARQUE : Après la mise à niveau vers la dernière version d'OMIMSSC, si la connexion à ftp.dell.com ou downloads.dell.com échoue, la source de mise à jour FTP en ligne Dell par défaut, HTTP Dell ou HTTPS Dell ne peut pas télécharger le fichier de catalogue. Par conséquent, le rapport de comparaison n'est pas disponible. Pour afficher un rapport de comparaison pour la source de mise à jour par défaut, modifiez la source de mise à jour FTP en ligne Dell par défaut, HTTP Dell ou HTTPS Dell (fournissez les informations d'identification du proxy si nécessaire), puis effectuez la même sélection dans le menu déroulant Sélectionner une source de mise à jour. Pour plus d'informations sur la modification d'une source de mise à jour, reportez-vous à la section Modification de la source de mise à jour.

REMARQUE : Une copie locale du fichier de catalogue est située dans OMIMSSC lorsque le produit est fourni. Par conséquent, le dernier rapport de comparaison n'est pas disponible. Pour afficher les résultats du dernier rapport de comparaison, mettez à jour le fichier de catalogue. Pour mettre à jour le fichier de catalogue, modifiez la source de mise à jour et enregistrez-la, ou supprimez et recréez une source de mise à jour.

REMARQUE : Dans SCCM, même après avoir actualisé les informations d'inventaire, les détails de serveur tels que la version du pack de pilotes et les pilotes disponibles pour le système d'exploitation, ne sont pas mis à jour dans la page des propriétés Contrôleurs Dell Out of Band (OOB). Pour mettre à jour les propriétés OOB, synchronisez OMIMSSC avec la console SCCM inscrite.

REMARQUE : Lorsque vous effectuez une mise à niveau d'OMIMSSC, les informations concernant les serveurs qui sont découverts dans les versions antérieures ne s'affichent pas. Pour obtenir les dernières informations sur les serveurs et corriger le rapport de comparaison, effectuez une nouvelle découverte des serveurs.

Pour actualiser et afficher l'inventaire de micrologiciel des périphériques détectés :

Étapes

1 Dans **OMIMSSC**, cliquez sur **Centre de maintenance**.

La page **Centre de maintenance** s'affiche avec un rapport de comparaison pour tous les périphériques qui sont découverts dans OMIMSSC par rapport à la source de mise à jour sélectionnée.

2 (Facultatif) Pour consulter un rapport de comparaison uniquement pour un groupe spécifique de périphériques, sélectionnez uniquement les périphériques requis.

3 (Facultatif) Pour consulter un rapport de comparaison pour une autre source de mise à jour, modifiez la source de mise à jour en sélectionnant une source de mise à jour dans le menu déroulant **Sélectionner une source de mise à jour**.

4 Pour afficher les informations de micrologiciel concernant les composants de périphérique, telles que la version en cours, la version de référence et les actions de mise à jour qui sont recommandées par Dell EMC, développez le groupe de serveurs sous **Groupe de périphériques/serveurs** jusqu'au niveau des serveurs, puis jusqu'au niveau des composants. En outre, affichez le nombre de mises à jour recommandées pour les périphériques. Passez le curseur sur l'icône des mises à jour disponibles pour voir les détails correspondants des mises à jour, tels que le nombre de mises à jour critiques et les mises à jour recommandées.

La couleur du voyant de l'icône des mises à jour disponibles est basée sur l'importance globale des mises à jour et les catégories de mise à jour critique sont les suivantes :

- La couleur est rouge, même s'il n'existe qu'une seule mise à jour critique dans le serveur ou le groupe de serveurs.
- La couleur est jaune s'il n'y a aucune mise à jour critique.
- La couleur est verte si les versions de micrologiciel sont à jour.

Une fois le rapport de comparaison rempli, les actions de mise à jour suivantes sont suggérées :

- Rétrograder : une version antérieure est disponible, et vous pouvez rétrograder le micrologiciel existant vers cette version.
- Aucune action requise : le micrologiciel existant est identique à celui de la source de mise à jour.
- Aucune mise à jour disponible : aucune mise à jour n'est disponible pour ce composant.

  REMARQUE : Aucune mise à jour n'est disponible pour les composants de bloc d'alimentation (PSU) MX7000 des systèmes modulaires MX7000 et des serveurs dans les catalogues en ligne. Dans le cas où vous souhaitez mettre à jour le composant PSU du système modulaire Mx7000, reportez-vous à *Mise à jour du composant de bloc d'alimentation pour les périphériques Dell EMC PowerEdge MX7000*. Pour la mise à jour du composant PSU des serveurs, contactez le support Dell EMC.

- Mise à niveau - Facultative : les mises à jour sont facultatives. Elles comportent de nouvelles fonctions ou toute mise à niveau de configuration spécifique.
- Mise à niveau - Urgente : les mises à jour sont critiques et permettent de résoudre les problèmes de sécurité, de performances ou de réparation dans les composants tels que le BIOS, etc.
- Mise à niveau - Recommandée : les mises à jour sont des corrections de problèmes, ou n'importe quelle amélioration de fonction pour les composants. En outre, des correctifs de compatibilité avec d'autres mises à jour de micrologiciel sont inclus.

Tenez compte des points suivants pour les informations relatives aux cartes NIC pour les serveurs de 11e génération :

- Après l'application de filtres en fonction d'une **nature de mise à jour Urgente**, un rapport répertoriant uniquement les composants avec des mises à jour urgentes s'affiche. Si ce rapport est exporté, les composants avec une action de rétrogradation qui ont également une mise à jour critique sont également exportés.

- Lorsqu'il existe plusieurs interfaces réseau disponibles dans une seule carte NIC, il n'y a qu'une seule entrée pour toutes les interfaces de la liste **Informations sur les composants**. Une fois les mises à jour de micrologiciel appliquées, toutes les cartes NIC sont mises à niveau.
- Lorsqu'une carte NIC est ajoutée, ainsi que les cartes existantes, la carte NIC qui vient d'être ajoutée est répertoriée en tant qu'instance supplémentaire dans la liste **Informations sur les composants**. Une fois les mises à jour de micrologiciel appliquées, toutes les cartes NIC sont mises à niveau.

Applying filters

Apply filters to view selected information in the comparison report.

À propos de cette tâche

Filter the comparison report based on available server components. OMIMSSC supports three categories of filters:

- **Nature Of Update**—select to filter and view only the selected type of updates on servers.
- **Component Type** —select to filter and view only the selected components on servers.
- **Server Model** —select to filter and view only the selected server models.

REMARQUE : You cannot export and import server profiles if the filters are applied.

To apply the filters:

Étape

In OMIMSSC, click **Maintenance Center**, click the filters drop-down menu, and then select the filters.

Removing filters

À propos de cette tâche

To remove filters:

Étape

In OMIMSSC, click **Maintenance Center**, and then click **Clear Filters**, or clear the selected check boxes.

Mise à niveau et rétrogradation des versions de micrologiciel à l'aide de la méthode d'exécution de mise à jour

Prérequis

Avant d'appliquer des mises à jour sur des périphériques, assurez-vous que les conditions suivantes sont remplies :

- Une source de mise à jour est disponible.

  REMARQUE : Sélectionnez une source de mise à jour d'Storage Spaces Direct ou des sources de mise à jour Mx7000 pour l'application des mises à jour de micrologiciel sur les clusters d'Storage Spaces Direct ou les systèmes modulaires MX7000, étant donné que ces sources de mise à jour voient une référence modifiée au catalogue qui contient les versions de micrologiciel recommandées des composants pour les clusters d'Storage Spaces Direct et les systèmes modulaires.
- La file d'attente des tâches de l'iDRAC ou du module de gestion est vidée avant d'appliquer les mises à jour sur les périphériques gérés.

À propos de cette tâche

Appliquez les mises à jour sur les groupes de périphériques sélectionnés qui sont compatibles avec OMIMSSC. Il est possible d'appliquer les mises à jour immédiatement ou de les planifier. Les tâches qui sont créées pour les mises à jour de micrologiciel sont répertoriées dans la page **Centre des tâches et des journaux**.

Tenez compte des éléments suivants avant de procéder à la mise à niveau ou la rétrogradation du micrologiciel :

- Lorsque vous lancez cette tâche, celle-ci prend beaucoup de temps en fonction du nombre de périphériques et de composants de périphérique présents.
- Vous pouvez appliquer les mises à jour de micrologiciel sur un seul composant d'un périphérique, ou à tout l'environnement.

- S'il n'existe aucune mise à jour ou rétrogradation applicable pour un périphérique, l'exécution d'une mise à jour de micrologiciel sur les périphériques n'entraîne aucune action sur les périphériques.
- Pour plus d'informations sur la mise à jour du châssis, consultez la section *Updating CMC firmware* (Mise à jour du micrologiciel CMC) du document *Dell PowerEdge M1000e Chassis Management Controller User's Guide* (Guide d'utilisation du micrologiciel Dell PowerEdge M1000e Chassis Management Controller).
  - Pour plus d'informations sur la mise à jour du micrologiciel du châssis dans VRTX, consultez la section *Updating firmware* (*Mise à jour du micrologiciel) du document Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide (Guide d'utilisation de Dell Chassis Management Controller pour Dell PowerEdge VRTX).*
  - Pour plus d'informations sur la mise à jour du micrologiciel du châssis dans FX2, consultez la section *Updating firmware (Mise à jour du micrologiciel)* du document *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide (Guide d'utilisation de Dell Chassis Management Controller pour Dell PowerEdge X2)*.

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, sélectionnez les serveurs ou les groupes de systèmes modulaires, ainsi qu'une source de mise à jour, puis cliquez sur **Exécuter la mise à jour**.

2 Dans la zone **Détails de la mise à jour**, entrez le nom et la description de la tâche de mise à jour de micrologiciel.

3 Pour activer la rétrogradation des versions de micrologiciel, cochez la case **Autoriser la rétrogradation**.

Si cette option n'est pas sélectionnée, il n'y a aucune action sur le composant qui nécessite une rétrogradation de micrologiciel.

4 Sous **Planifier la mise à jour**, sélectionnez l'une des options suivantes :

- **Exécuter maintenant** : cette option permet d'appliquer les mises à jour immédiatement.
- Sélectionnez une date et une heure pour planifier une mise à jour de micrologiciel à l'avenir.

5 Sélectionnez l'une des méthodes suivantes, puis cliquez sur **Terminer**.

- **Mises à jour planifiées sans agent** : les mises à jour applicables sans un redémarrage du système sont appliquées immédiatement, et les mises à jour qui nécessitent un redémarrage sont appliquées lors du redémarrage du système. Pour vérifier si toutes les mises à jour sont appliquées, actualisez l'inventaire. La tâche de mise à jour échoue entièrement, même en cas d'échec de l'opération sur un seul périphérique.

  REMARQUE : OMIMSSC prend en charge les mises à jour planifiées sans agent uniquement pour les systèmes modulaires Mx7000.

- **Mises à jour sans agent** : les mises à jour sont appliquées et le système redémarre immédiatement.

REMARQUE : Mise à jour CAU (Cluster-Aware) : automatise le processus de mise à jour en utilisant les fonctions CAU de Windows dans les groupes de mise à jour de cluster afin de maintenir la disponibilité du serveur. Les mises à jour sont transmises au coordinateur des mises à jour de cluster qui est présent sur le même système où le serveur SCVMM est installé. Le processus de mise à jour est automatisé afin de maintenir la disponibilité du serveur. La tâche de mise à jour est soumise à la fonction CAU (Cluster-Aware-Update) de Microsoft, quelle que soit la sélection effectuée dans le menu déroulant Méthode de mise à jour. Pour plus d'informations, reportez-vous à la section Mises à jour via CAU.

REMARQUE : Après avoir envoyé une tâche de mise à jour de micrologiciel à iDRAC, OMIMSSC interagit avec iDRAC pour déterminer l'état de la tâche et l'affiche dans la page Tâches et journaux du portail d'administration OMIMSSC. S'il n'y a pas de réponse d'iDRAC sur l'état de la tâche pendant une longue durée, l'état de la tâche est marqué comme étant en échec.

Updates using CAU

Updates on servers (that are part of cluster) happen through cluster update coordinator which is present on the same system where SCVMM server is installed. The updates are not staged and are applied immediately. Using Cluster Aware Update (CAU), you can minimize any disruption or server downtime enabling continuous availability of the workload. Hence, there is no impact to the service provided by the cluster group. For more information about CAU, see Cluster-Aware Updating Overview section at `technet.microsoft.com`.

Before applying the updates on cluster update groups, verify the following:

- Ensure that the enrolled user has administrator privileges for updating clusters through CAU feature.
- Connectivity to selected update source.
- Availability of failover clusters.

- Ensure that Windows Server 2012 or Windows Server 2012 R2 or Windows 2016 operating system is installed on all failover cluster nodes to support the CAU feature.
- Configuration of automatic updates is not enabled to automatically install updates on any failover cluster node.
- Enable firewall rule that enables remote shutdown on each node in the failover cluster.
- Cluster group should have minimum of two nodes.
- Check for cluster update readiness and ensure that there are no major errors and warnings in the Cluster Readiness report for applying the CAU method. For more information about CAU, see Requirements and Best Practices for Cluster—aware Updating section at Technet.microsoft.com.

REMARQUE :

For information about applying the updates, see Upgrading and downgrading firmware versions using run update method .

9

Creating clusters using Operational Template

This chapter covers information about creating the Storage Spaces Direct clusters.

Creating logical switch for Storage Spaces Direct clusters

À propos de cette tâche

Create logical switch from OMIMSSC in SCVMM.

REMARQUE : The IP address that is entered in Configuration for Management section overrides the IP address that is entered in operating system component of Storage Spaces Direct predefined Operational Template.

Étapes

1 In OMIMSSC, expand **Configuration and Deployment**, click **Cluster View**, and then click **Create logical switch for Cluster**.

2 Provide a name for the logical switch, and select the host group present in SCVMM for associating the logical switch.

3 Provide the following details, and click **Create**.

   a In **Configuration for Management**, provide the **Subnet**, **Start IP**, **End IP**, **DNS Server**, **DNS Suffix**, and **Gateway** details.

   REMARQUE : Provide the subnet information in Classless InterDomain Routing (CIDR) notation.

   b In **Configuration for Storage**, provide the **VLAN**, **Subnet**, **Start IP**, and **End IP** details.

4 Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Créer**.

   Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Étapes suivantes

To verify that the logical switch is created successfully, check for the logical switch name in the drop-down menu listed in **Create Cluster** page.

To view the details of the logical switch, perform the following steps in SCVMM:

1 To view the logical switch name, click **Fabric**, and in **Networking**, click **Logical Switches**.

2 To view the logical switch's Uplink Port Profile (UPP), click **Fabric**, and in **Networking**, click **Logical Switches**.

3 To view the logical switch's network, click **Fabric**, and in **Networking**, click **Logical Networks**.

Création de clusters d'Storage Spaces Direct

Prérequis

- Assurez-vous que vous créez un réseau logique à l'aide de la fonction **Configurer le réseau pour les clusters**.
- Assurez-vous que vous utilisez SC2016 VMM.
- Assurez-vous que vous utilisez Windows Server 2016 Datacenter Edition.
- Assurez-vous que les configurations des serveurs gérés correspondent aux exigences en matière de versions de pilote et de micrologiciel de solution d'Storage Spaces Direct. Pour plus d'informations, consultez la documentation *Dell EMC Storage Spaces Direct Ready Nodes PowerEdge R740XD and PowerEdge R640 Support Matrix*.
- Pour plus d'informations sur l'infrastructure et la gestion des Storage Spaces Direct, consultez la documentation *Dell EMC Microsoft Storage Spaces Direct Ready Node Deployment Guide for scalable hyper-converged infrastructure with R740xd and R640 Storage Spaces Direct Ready Nodes* (Guide de déploiement des nœuds Ready d'espaces de stockage direct Dell EMC Microsoft pour une infrastructure hyperconvergée évolutive avec les nœuds Ready d'espaces de stockage direct R740xd et R640).

À propos de cette tâche

Tenez compte des points suivants avant de créer des clusters d'Storage Spaces Direct :

- Vous pouvez créer un cluster d'Storage Spaces Direct dans OMIMSSC en indiquant une adresse IP statique uniquement.
- La taille du disque virtuel s'affiche comme étant égale à zéro dans le modèle opérationnel prédéfini des Storage Spaces Direct. Mais, après avoir appliqué le modèle opérationnel prédéfini des Storage Spaces Direct, le lecteur est créé uniquement avec une taille égale à la taille complète du support de stockage physique M.2. Pour plus d'informations sur l'espace de lecteur virtuel, consultez le Guide d'utilisation d'iDRAC disponible à l'adresse **dell.com/support**.

Pour créer un cluster d'Storage Spaces Direct, effectuez les étapes suivantes :

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Cluster**.

La page **Vue Cluster** s'affiche.

2 Indiquez un nom de cluster et sélectionnez le Operational Template prédéfini pour la création des clusters d'Storage Spaces Direct.

- Les serveurs non attribués qui appartiennent uniquement à un modèle de serveur et une carte NIC spécifiques s'affichent en fonction du Operational Template que vous sélectionnez dans le menu déroulant **Operational Template**.

3 Pour ajouter des serveurs à un cluster, sélectionnez les serveurs en utilisant la case à cocher.

4 Pour ajouter des valeurs de pool spécifiques du système, cliquez sur **Exporter un pool de valeurs d'attribut**.

Modifiez et enregistrez le fichier afin de pouvoir indiquer les valeurs de pool spécifiques du système.

5 (Facultatif) Si vous devez définir les valeurs spécifiques d'un système, dans **Pool de valeurs d'attribut**, cliquez sur **Parcourir** et sélectionnez le fichier CSV modifié.

6 Entrez un nom de tâche unique, puis cliquez sur **Créer**.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Étapes suivantes

Pour vérifier si les clusters ont été créés avec succès :

1 Vérifiez l'état de réussite de la tâche de création de cluster.

2 Affichez le cluster dans la page **Vue Cluster**.

3 Affichez le cluster dans SCVMM.

10

Managing devices in OMIMSSC

Maintain servers and Modular Systems up-to-date by scheduling jobs for upgrading firmware for server and Modular Systems components. Manage servers by recovering servers to an earlier state by exporting its earlier configuration, applying the configurations of the old component on replaced component, and exporting LC logs for troubleshooting.

Sujets :

Server recovery

Save a server's configurations in protection vault by exporting a server's configurations to a profile and importing the profile on same server to reinstate it to an earlier state.

Protection vault

Protection vault is a secure location where you can save server profiles. Export server profile from a server or a group of servers and import them to same server or group of servers. You can save this server profile on a shared location in the network by creating an external vault or on a vFlash Secure Digital (SD) card by creating an internal vault. You can associate a server or a group of servers with only one protection vault. However, you can associate one protection vault with many servers or group of servers. You can save a server profile on only one protection vault. However, you can save any number of server profiles on a single protection vault.

Creating protection vault

Prérequis

Ensure that vault location is accessible.

Étapes

1 In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.

2 In **Maintenance Center**, click **Protection Vault**, and then click **Create**.

3 Select a type of protection vault you want to use and provide the details.

- If you are creating a protection vault of type **Network Share**, provide a location to save the profiles, credentials to access this location and a passphrase to secure the profile.

  REMARQUE : **This type of protection vault provides support file sharing of type Common Internet File System (CIFS).**

- If you are creating a protection vault of type **vFlash**, provide the passphrase to secure the profile.

Modifying protection vault

À propos de cette tâche

You cannot modify the name, description, type of protection vault, and passphrase.

Étapes

1 In **OMIMSSC**, click **Maintenance Center** > **Maintenance Settings** > **Protection Vault**.

2 To modify the vault, select the vault and click **Edit**.

Deleting protection vault

À propos de cette tâche

You cannot delete a protection vault in the following circumstances:

- The protection vault is associated with a server or a group of servers.

  To delete such a protection vault, delete the server or group of servers, and then delete the protection vault.
- There is a scheduled job associated with the protection vault. However, to delete such a protection vault, delete the scheduled job, and then delete the protection vault.

Étapes

1 In **OMIMSSC**, click **Maintenance Center** > **Maintenance Settings** > **Protection Vault**.

2 Select the vault to delete and click **Delete**.

Exporting server profiles

Export a server profile including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and the configuration of those components. OMIMSSC Appliance creates a file containing all the configurations, which you can save on a vFlash SD card or network share. Select a protection vault of your choice to save this file. You can export the configuration profiles of a server or a group of servers immediately or schedule it for later. Also, you can select a relevant recurrence option as to how frequently the server profiles have to be exported.

Prérequis

Disable the **F1/F2 Prompt on Error** option in **BIOS Settings**.

À propos de cette tâche

Consider the following before exporting server profiles:

- At an instance, you can schedule only one export configuration job for a group of servers.
- You cannot perform any other activity on that server or group of servers whose configuration profiles are being exported.
- Ensure that the **Automatic Backup** job in iDRAC is not scheduled at the same time.
- You cannot export server profiles if the filters are applied. To export server profiles, clear all the applied filters.
- To export server profiles, ensure that you have the iDRAC Enterprise license.
- Before exporting server profile, ensure that the IP address of the server is not changed. If the server IP has changed due to any other operation, then rediscover this server in OMIMSSC, and then schedule the export server profile job.

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez les serveurs dont vous souhaitez exporter les profils, puis cliquez sur **Exporter** dans le menu déroulant **Profil de périphérique**.

La page **Exporter le profil du serveur** s'affiche.

2 In the **Export Server Profile** page, provide the job details, and then select a protection vault.

For more information about protection vaults, see Creation of protection vault.

In **Schedule Export Server Profile** select one of the following:

- **Run Now**—export the server configuration immediately of the selected servers, or group of servers.
- Schedule—provide a schedule to export the server configuration of the selected group of servers.
  - **Never**—select to export the server profile only once during the scheduled time.
  - **Once a week**—select to export the server profile on a weekly basis.

- **Once every 2 weeks**—select to export the server profile once every two weeks.
- **Once every 4 weeks**—select to export the server profile once every four weeks.

Importing server profile

You can import a server profile that was previously exported for that same server, or group of servers. Importing server profile is useful in restoring the configuration and firmware of a server to a state stored in the profile.

À propos de cette tâche

You can import server profiles in two ways:

- Quick import server profile—allows you to automatically import the latest exported server profile for that server. You need not select individual server profiles for each of the servers for this operation.
- Custom import server profile—allows you to import server profiles for each of the individually selected servers. For example, if exporting server profile is scheduled, and the server profile is exported every day, this feature allows you to select a specific server profile that is imported from the list of server profiles available in the protection vault of that server.

Import server profile notes:

- You can import a server profile from a list of exported server profiles for that server only. You cannot import the same server profiles for different servers or server groups. If you try to import server profile of another server or server group, the import server profile job fails.
- If a server profile image is not available for a particular server or group of servers, and an import server profile job is attempted for that particular server or group of servers, the import server profile job fails for those particular servers that do that have server profile. A log message is added in the Activity logs with the details of the failure.
- After exporting a server profile, if any component is removed from the server, and then an import profile job is started, all the components information are restored except the missing component information is skipped. This information is not available in the activity log of OMIMSSC. To know more about the missing components, see iDRAC's **LifeCycle Log**.
- You cannot import a server profile after applying the filters. To import server profiles, clear all the applied filters.
- To import server profiles, you must have the iDRAC Enterprise license.

Étapes

1 Dans OMIMSSC, sous **Centre de maintenance**, sélectionnez les serveurs dont vous souhaitez importer les profils, puis cliquez sur **Importer** dans le menu déroulant **Profil de périphérique**.

La section **Importer le profil de serveur** s'affiche.

2 Provide the details, select the **Import Server Profile Type** you want.

> **REMARQUE : A server profile is exported along with the existing RAID configuration. However, you can import the server profile including or excluding the RAID configuration on the server or group of servers. Preserve Data is selected by default and preserves the existing RAID configuration in the server. Clear the check box if you want to apply the RAID settings stored in the server profile.**

3 To import the server profile, click **Finish**.

Applying firmware and configuration settings on replaced component

The part replacement feature automatically updates a replaced server component to the required firmware version or the configuration of the old component, or both. The update occurs automatically when you reboot the server after replacing the component.

À propos de cette tâche

To set the configurations for part replacement:

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, sélectionnez les serveurs ou un groupe de serveurs, puis cliquez sur **Remplacement de pièce**.

REMARQUE : Le nom d'option devient Configurer un remplacement de pièce lorsque vous placez le pointeur sur Remplacement de pièce.

La fenêtre **Configuration du remplacement de pièce** s'affiche.

2 You can set **CSIOR**, **Part Firmware Update**, and **Part Configuration Update**, to any of the following options, and then click **Finish**:

- Collect System Inventory On Restart (CSIOR)—collects all the component information on every system restart.
  - **Enabled**—the software and hardware inventory information of the server components are automatically updated during every system restart.
  - **Disabled**—the software and hardware inventory information of the server components are not updated.
  - **Do not change the value on the server**—the existing server configuration is retained.
- Part firmware update—restores, or upgrades, or downgrades the component firmware version based on the selection made.
  - **Disabled**—the part firmware update is disabled and the same is applied on the replaced component.
  - **Allow version upgrade only**—the upgraded firmware versions are applied on the replaced component, if the firmware version of the new component is earlier than the existing version.
  - **Match firmware of replaced part**—the firmware version on the new component is matched to the firmware version of the original component.
  - **Do not change the value on the server**—the existing configuration of the component is retained.
- Part configuration update—restores or upgrades the component configuration based on the selection made.
  - **Disabled**—the part configuration update is disabled and the saved configuration of the old component is not applied on the replaced component.
  - **Apply always**—the part configuration update is enabled and the saved configuration of the old component is applied on the replaced component.
  - **Apply only if firmware matches**—the saved configuration of the old component is applied on the replaced component, only if their firmware versions match.
  - **Do not change the value on the server**—the existing configuration is retained.

Collecting LC logs for servers

À propos de cette tâche

LC logs provide records of past activities in a managed server. These log files are useful for server administrators since they provide detailed information about recommended actions and some other technical information that is useful for troubleshooting purpose.

The various types of information available in LC logs are alerts-related, configuration changes on the system hardware components, firmware changes due to an upgrade or downgrade, replaced parts, temperature warnings, detailed timestamps of when the activity has started, severity of the activity, and so on.

The exported LC log file is saved in a folder and the folder is named after the server's service tag. LC logs are saved in the format: `<YYYYMMDDHHMMSSSSS>.<file format>`. For example, 20160720103001O597.xml.gz is the LC file name, which includes the date and time of the file when it was created.

There are two options to collect LC logs:

- Complete LC logs—exports active and archived LC log files. They are large in size, and hence compressed to `.gz` format and exported to the specified location on a CIFS network share.
- Active LC logs—exports recent LC log files immediately or schedule a job to export the log files at regular intervals. View, search, and export these log files to OMIMSSC Appliance. In addition, you can save a backup of log files in a network share.

To collect LC logs, perform the following steps:

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez un serveur ou un groupe de serveurs, cliquez sur le menu déroulant **Journaux LC** et cliquez sur **Collecter les journaux LC**.

2 In **LC Log Collection**, select one of the following options, and click **Finish**:

- **Export Complete LC Logs (.gz)**—select to export complete LC logs to a CIFS network share by providing Windows credentials.

- **Export Active Logs (Run now)**—select to export the active logs immediately to OMIMSSC Appliance.
  - (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

    REMARQUE : Ensure that you update the firmware versions of iDRAC and LC before, exporting active LC logs for 11th generation of servers.
- **Schedule LC Log Collection**—select select to export the active logs at regular intervals.

  In **Schedule LC Log Collection**, select a date and time to export the log files.

  Select a radio button depending on how frequently the files have to be exported. The available options for scheduling frequency to determine how often you want to collect the LC logs are:

  - **Never**—this option is selected by default. Select to export the LC logs only once at the scheduled time.
  - **Daily**—select to export the LC logs daily at the scheduled time.
  - **Once a week**—select to export the LC logs on a weekly basis at the scheduled time.
  - **Once every 4 weeks**—select to export the LC logs in every four weeks at the scheduled time.
  - (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

    REMARQUE : Provide a share folder with sufficient storage space, since the exported files are large in size.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Viewing LC logs

View all the active LC logs, search for detailed description, and download the logs in CSV format.

Prérequis

Add OMIMSSC Appliance in **Local Intranet site** list as mentioned in *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

Étapes

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez un serveur ou un groupe de serveurs, cliquez sur le menu déroulant **Journaux LC** et cliquez sur **Afficher les journaux LC**.

2 All the servers in the selected group and the servers for which LC logs are collected are listed with their LC log files. Click a file name to view all the log entries in the LC log file specific to that server. For more information, see File description.

3 (Optional) Use the search box to search description in all the log files, and export the file in CSV format.

There are two ways to search message description in an LC file:

- Click a file name to open the LC log file and search for a description in the search box.
- Provide a description text in the search box, and then view all the LC files with these instances of text.

REMARQUE : If the LC log message description is long, the message is truncated to 80 characters.

REMARQUE : The time displayed against the LC log messages follows the iDRAC time zone.

File description

Use this page to view detailed information about recommended actions and some other technical information that are useful for tracking or alert purposes for a particular server.

To view the contents of a file, click a file name:

- You can search for particular message descriptions.

- You can either view the log files in the window or download the file to view additional log messages.
- You can view any comments provided by a user for an activity.

REMARQUE : When using the search option, only the search results are exported to CSV file.

REMARQUE : If the message is long, the message is truncated to 80 characters.

REMARQUE : Click Message ID to view more information about the message.

Exportation de l'inventaire

Exportez l'inventaire des serveurs sélectionnés ou d'un groupe de serveurs vers un fichier au format XML ou CSV. Vous pouvez enregistrer ces informations Windows dans un répertoire partagé ou sur un système de gestion. Utilisez ces informations d'inventaire pour créer un fichier d'inventaire de référence dans une source de mise à jour.

Prérequis

Assurez-vous de définir les paramètres du navigateur tel que mentionné dans la section *Browser settings* (Paramètres du navigateur) dans le document *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide* (Guide d'installation de Dell EMC OpenManage Integration for Microsoft System Center version 7.1 pour System Center Configuration Manager et System Center Virtual Machine Manager).

REMARQUE : Vous pouvez importer le fichier XML dans DRM et créer un référentiel en fonction du fichier d'inventaire.

À propos de cette tâche

REMARQUE : Bien que vous sélectionniez uniquement les informations des composants d'un serveur et les exportiez, toutes les informations d'inventaire du serveur sont exportées.

Étapes

1 Dans **OMIMSSC**, cliquez sur **Centre de maintenance**.

2 Sélectionnez les serveurs desquels vous souhaitez exporter l'inventaire, puis sélectionnez le format depuis le menu déroulant **Exporter l'inventaire**.

Le fichier est exporté au format CSV ou XML en fonction de la sélection. Le fichier se compose de détails tels que les groupes de serveurs, le numéro de série du serveur, le nom d'hôte ou l'adresse IP, le modèle de périphérique, le nom de composant, la version de micrologiciel en cours sur ce composant, la version de micrologiciel de la source de mise à jour et l'action de mise à jour sur ce composant.

Cancelling scheduled jobs

Prérequis

Ensure that the job is in **Scheduled** state.

Étapes

1 In OMIMSSC, do any of the following:

- In the navigation pane, click **Maintenance Center**, and then click **Manage Jobs**.
- In the navigation pane, click **Jobs and Log Center**, and then click **Scheduled** tab.

2 Select jobs that you want to cancel, click **Cancel**, and then to confirm, click **Yes**.

11

Configuration et déploiement

À propos de cette tâche
Découverte

Étapes

1 Dans la console OMIMSSC, effectuez l'une des opérations suivantes :
   - Dans le tableau de bord, cliquez sur **Découvrir des serveurs**.
   - Dans le volet de navigation, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Serveur**, puis cliquez sur **Découvrir**.
2 Cliquez sur **Découvrir**.

Étape suivante
Pour afficher les modifications apportées, actualisez la page **Profil de référence**.

Sujets :

Scénarios d'utilisation

1 Découvrez le serveur de référence à l'aide de la page **Découverte**. Pour plus d'informations, reportez-vous à la section Discovering servers using manual discovery.
2 Créez un Operational Template en capturant tous les détails du serveur découvert. Pour plus d'informations, reportez-vous à la section Creating Operational Template from reference servers.
3 Attribuez un Operational Template sur un périphérique géré et vérifiez la conformité au modèle. Pour plus d'informations, reportez-vous à la section Assigning Operational Template and running Operational Template compliance for servers.
4 Déployez un Operational Template pour rendre le modèle de périphérique conforme. Pour plus d'informations, reportez-vous à la section Déploiement d'un Operational Template sur des serveurs.

5 Affichez l'état de tâche du déploiement de système d'exploitation dans la page **Centre des tâches et des journaux**. Pour plus d'informations, reportez-vous à la section Launching Jobs and Logs Center.

Création de modèles opérationnels

Prérequis

Avant de créer un Operational Template, assurez-vous que vous effectuez les tâches suivantes :

- Découvrez un serveur de référence à l'aide de la fonction **Découverte**. Pour en savoir plus sur la découverte des serveurs, reportez-vous à la section Discovering servers using manual discovery.
- Découvrez un système modulaire à l'aide de la fonction **Découverte**. Pour en savoir plus sur la découverte des systèmes modulaires, reportez-vous à la section Discovering MX7000 by using manual discovery.
- Si vous n'utilisez pas la source de mise à jour par défaut, créez une source de mise à jour. Pour plus d'informations, reportez-vous à la section Création d'une source de mise à jour.
- Pour les utilisateurs SCCM :
  - Créez une séquence de tâches. Pour plus d'informations, reportez-vous à la section Types of task sequence.
  - Pour le déploiement d'un système non-Windows, vous devez disposer d'un profil de référence de type de périphérique. Pour plus d'informations, reportez-vous à la section Creating credential profile.
- Pour les utilisateurs SCVMM :
  - Créez un profil d'hyperviseur. Pour plus d'informations sur la création d'un profil d'hyperviseur, reportez-vous à la section Creating hypervisor profile.
  - Pour les déploiements Windows, vous devez disposer d'un profil de référence de type de périphérique. Pour plus d'informations, reportez-vous à la section Creating credential profile.

Étapes

1 Dans OMIMSSC, effectuez l'une des opérations suivantes pour ouvrir un Operational Template :
   - Dans le tableau de bord OMIMSSC, cliquez sur **Créer un modèle opérationnel**.
   - Dans le volet de navigation, cliquez sur **ProfilsModèle opérationnel** et cliquez sur **Créer**.

   L'Assistant **Modèle opérationnel** s'affiche.

2 Cliquez sur **Créer**.

   L'Assistant **Modèle opérationnel** s'affiche.

3 Entrez le nom et la description du modèle.

4 Sélectionnez le type de périphérique, entrez l'adresse IP du périphérique de référence, puis cliquez sur **Suivant**.

   REMARQUE : Vous pouvez capturer la configuration du serveur de référence à l'aide d'iDRAC 2.0 et versions supérieures.

5 Dans **Composants de périphérique**, cliquez sur un composant pour afficher les attributs disponibles et leurs valeurs.

   Les composants sont les suivants :
   - Mise à jour du micrologiciel
   - Composants matériels (RAID, carte NIC et BIOS).

REMARQUE : Dans le composant iDRAC intégré 1, vous trouverez ci-dessous les privilèges et leurs valeurs pour l'attribut Privilège d'administrateur utilisateur.

Tableau 5. Tableau des valeurs de privilège

Valeur	Droits
1	Ouverture de session
2	Configuration
4	Configurer des utilisateurs
8	Journaux
16	Contrôle du système
32	Accéder à la console virtuelle
64	Accéder à Média Virtuel
128	Opérations système
256	Débogage
499	Privilèges d'opérateur

- Système d'exploitation : sélectionnez Windows, ESXi ou RHEL.

6 Utilisez la barre de défilement horizontal pour localiser un composant. Sélectionnez le composant, développez un groupe, puis modifiez ses valeurs d'attribut. Utilisez la barre de défilement vertical pour modifier un groupe et les attributs d'un composant.

7 Cochez la case en regard de chaque composant, car les configurations des composants sélectionnés sont appliquées sur le périphérique géré lorsque le Operational Template est appliqué. Cependant, toutes les configurations du périphérique de référence sont capturées et enregistrées dans le modèle.

REMARQUE : Indépendamment de la sélection des cases en regard de chaque composant, toutes les configurations sont capturées dans le modèle.

Dans le composant **Système d'exploitation**, suivez les étapes décrites dans l'une ou l'autre des options suivantes, selon vos besoins :

- Pour le déploiement de système d'exploitation Windows dans SCCM, reportez-vous à la section Windows OS component for OMIMSSC console extension for SCCM.
- Pour le déploiement de système d'exploitation Windows dans SCVMM, reportez-vous à la section Windows component for OMIMSSC console extension for SCVMM.
- OMIMSSC
- Pour le déploiement de système d'exploitation non-Windows, reportez-vous à la section Non-Windows component for OMIMSSC console extensions.

8 Pour enregistrer le profil, cliquez sur **Terminer**.

Dossiers de programme d'installation

Les dossiers suivants sont créés après l'installation de l'extension de console :

- Log : ce dossier contient les informations de journal se rapportant à la console.

REMARQUE : Si les informations d'identification du compte d'administrateur de domaine et du compte d'administrateur local sont différentes, n'utilisez pas le compte d'administrateur de domaine pour vous connecter à SCCM ou SCVMM. Utilisez plutôt un autre compte d'utilisateur de domaine pour vous connecter à SCCM ou SCVMM.

Attribution de modèles opérationnels

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**. Sélectionnez les serveurs requis et cliquez sur **Attribuer un modèle opérationnel et exécuter la conformité**.

La page **Attribuer un Operational Template et exécuter la conformité** s'affiche.

2 Sélectionnez les serveurs requis et cliquez sur **Attribuer un modèle opérationnel et exécuter la conformité**.

3 Dans OMIMSSC, cliquez sur **Configuration et déploiement** et cliquez sur **Vue Systèmes modulaires**. Sélectionnez le système modulaire requis et cliquez sur **Attribuer un Modèle opérationnel**.

La page **Attribuer Operational Template** s'affiche.

4 Sélectionnez les systèmes modulaires, puis cliquez sur **Attribuer un modèle opérationnel et exécuter la conformité**.

La page **Attribuer un Operational Template** s'affiche.

5 Sélectionnez le modèle dans le menu déroulant **Operational Template**, entrez un nom de tâche, puis cliquez sur **Attribuer**.

La liste déroulante Operational Template répertorie les modèles du même type que celui des périphériques sélectionnés dans l'étape précédente.

Si le périphérique est conforme au modèle, une case de couleur **verte** cochée s'affiche.

Si le Operational Template n'est pas appliqué avec succès sur le périphérique ou si le composant matériel dans Operational Template n'est pas sélectionné, une case avec un symbole d'**information** s'affiche.

Si le périphérique n'est pas conforme au modèle, un symbole d'**avertissement** s'affiche. Uniquement dans le cas où le périphérique n'est pas conforme au Operational Template attribué, vous pouvez afficher un rapport récapitulatif en cliquant sur le lien du nom de modèle. La page **Operational Template - Rapport récapitulatif** affiche un rapport récapitulatif des différences qui existent entre le modèle et le périphérique.

Pour afficher un rapport détaillé, effectuez les étapes suivantes :

a Cliquez sur **Afficher la conformité détaillée**. Ici, les composants dont les valeurs d'attribut diffèrent de celles du modèle attribué s'affichent. Les couleurs indiquent les différents états de la conformité au Operational Template.

- Symbole d'avertissement de couleur jaune : non-conformité. Indique que la configuration du périphérique ne correspond pas aux valeurs du modèle.
- Case de couleur rouge : indique que le composant n'est pas présent sur le périphérique.

Déploiement de modèles opérationnels

À propos de cette tâche

REMARQUE : Assurez-vous que vous n'activez pas les attributs qui modifient les informations d'identification permettant de se connecter au périphérique après avoir déployé le Operational Template.

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**. Sélectionnez les serveurs sur lesquels vous avez appliqué le modèle, puis cliquez sur **Déployer un Operational Template**.

La page **Déployer un Operational Template** s'affiche.

2 Dans OMIMSSC, cliquez sur **Configuration et déploiement** et cliquez sur **Vue Systèmes modulaires**. Sélectionnez le système modulaire sur lequel vous avez attribué le modèle, puis cliquez sur **Déployer un Operational Template**.

La page **Déployer un Operational Template** s'affiche.

3 (Facultatif) Pour exporter tous les attributs qui sont marqués comme valeurs de pool dans le modèle sélectionné vers un fichier CSV, cliquez sur **Exporter les attributs de pool**. Sinon, passez à l'étape 4.

REMARQUE : Avant d'exporter les valeurs de pool, ajoutez l'adresse IP de l'appliance OMIMSSC dans laquelle l'extension de console OMIMSSC est installée au site intranet local. Pour plus d'informations sur l'ajout de l'adresse IP dans le navigateur IE, consultez la section *Browser settings* (Paramètres du navigateur) du document *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide* (Guide d'installation de Dell EMC OpenManage Integration for Microsoft System Center version 7.1 pour System Center Configuration Manager et System Center Virtual Machine Manager).

4 Si vous avez exporté les valeurs de pool, entrez les valeurs de tous les attributs qui sont marqués comme valeurs de pool dans le fichier CSV et enregistrez le fichier. Dans **Pool de valeurs d'attribut**, sélectionnez ce fichier pour l'importer.

Le format d'un fichier CSV est **attribute-value-pool.csv**.

REMARQUE : Assurez-vous de sélectionner un fichier CSV qui a tous les attributs corrects et l'adresse IP iDRAC, sinon les informations d'identification iDRAC ne sont pas modifiées en raison du modèle, étant donné que la tâche n'est pas suivie par OMIMSSC après la modification de l'adresse IP iDRAC ou des informations d'identification iDRAC et qu'elle est marquée comme étant en échec bien que la tâche puisse être réussie dans iDRAC.

5 Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Déployer**.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

Composant de système d'exploitation Windows pour l'extension de console OMIMSSC pour SCCM

1 Sélectionnez une séquence de tâches et une méthode de déploiement.

REMARQUE : Seules les séquences de tâches déployées sur les collections sont répertoriées dans le menu déroulant.

Pour en savoir plus sur la séquence de tâches, reportez-vous à la section Task sequence-SCCM.

2 Sélectionnez l'une des options suivantes pour la **méthode de déploiement** :

- **Démarrer sur l'image ISO du réseau** : redémarre l'image ISO spécifiée.
- **Activer ISO sur la carte vFlash et redémarrer** : télécharge l'image ISO sur la carte vFlash et redémarre le système.
- **Redémarrer sur vFlash** : redémarre sur la carte vFlash. Assurez-vous que l'image ISO est présente sur la carte vFlash.

REMARQUE : Pour utiliser l'option Redémarrer sur vFlash, le nom d'étiquette de la partition créée sur vFlash doit être ISOIMG.

3 (Facultatif) Pour utiliser l'image présente dans le partage réseau, sélectionnez l'option **Utiliser l'image ISO réseau comme image de secours**.

4 Saisissez un fichier image de support d'amorçage.

5 Sélectionnez les pilotes nécessaires pour le système d'exploitation.

Composant Windows pour l'extension de console OMIMSSC pour SCVMM

Sélectionnez **Profil d'hyperviseur**, **Profil de référence** et **Adresse IP de serveur à partir de**.

REMARQUE : Nom d'hôte et Carte NIC de gestion de serveur sont toujours des valeurs de pool.

Si vous sélectionnez **Adresse IP de serveur à partir de** en tant que **Statique**, assurez-vous que vous avez configuré le réseau logique dans SCVMM, et que les champs suivants sont des valeurs de pool :

- **Réseau logique de console**
- **Sous-réseau IP**
- **Adresse IP statique**

Composant non-Windows pour l'extension de console OMIMSSC pour SCCM/SCVMM

À propos de cette tâche

Étape

Sélectionnez un système d'exploitation non-Windows, la version du système d'exploitation, le type de dossiers de partage, le nom du fichier ISO, l'emplacement du fichier ISO et le mot de passe pour le compte root du système d'exploitation.

(Facultatif) Sélectionnez un profil de référence de type Windows pour l'accès au partage CIFS.

Nom d'hôte est une valeur de pool et si vous désactivez l'option DHCP, les champs suivants sont des valeurs de pool :

- **Adresse IP**
- **Masque de sous-réseau**
- **Passerelle par défaut**
- **DNS principal**
- **DNS secondaire**

REMARQUE : Les types de partages NFS (Network File System) et CIFS (Common Internet File System) sont pris en charge pour le déploiement de système d'exploitation non-Windows.

Découverte dans une console MSSC inscrite

Après la découverte, le serveur est ajouté à l'onglet **Hôtes** ou l'onglet **Non attribué**. Le serveur découvert est marqué comme conforme ou non conforme lorsqu'il contient les versions minimales du micrologiciel LC, de l'iDRAC et du BIOS requises pour utiliser OMIMSSC.

- Lorsque vous découvrez un serveur PowerEdge sur lequel un système d'exploitation est présent et déjà présent dans la console SCCM ou SCVMM, le serveur est répertorié comme serveur hôte sous l'onglet **Hôtes** dans la console OMIMSSC dans laquelle la tâche de détection est lancée.
  - Si l'hôte est un serveur modulaire, le numéro de série du système modulaire contenant le serveur s'affiche également.
  - Si l'hôte fait partie d'un cluster, le nom de domaine complet (FQDN) du cluster s'affiche.
- Lorsque vous découvrez un serveur Dell PowerEdge qui n'est pas répertorié dans SCCM ou SCVMM, le serveur est répertorié en tant que serveur non attribué sous l'onglet **Non attribué** dans toutes les consoles OMIMSSC non inscrites.
- Une licence est utilisée après la découverte d'un serveur. Le nombre de **nœuds de licence** diminue au fur et à mesure que les licences sont découvertes.

Importation du profil du serveur

1. Dans OMIMSSC, sous **Centre de maintenance**, sélectionnez les serveurs dont vous souhaitez importer les profils, puis cliquez sur **Importer** dans le menu déroulant **Profil de périphérique**.

   La section **Importer le profil de serveur** s'affiche.
2. Sélectionnez les serveurs dont vous souhaitez importer les profils, puis cliquez sur **Importer** dans le menu déroulant **Profil de périphérique**.

   La section **Importer le profil de serveur** s'affiche.

Exporter le profil du serveur

1. Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez les serveurs dont vous souhaitez exporter les profils, puis cliquez sur **Exporter** dans le menu déroulant **Profil de périphérique**.

   La page **Exporter le profil du serveur** s'affiche.
2. Sélectionnez les serveurs dont vous souhaitez exporter les profils, puis cliquez sur **Exporter** dans le menu déroulant **Profil de périphérique**.

   La page **Exporter le profil du serveur** s'affiche.

Affichage de journaux LC

1. Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez un serveur ou un groupe de serveurs, cliquez sur le menu déroulant **Journaux LC** et cliquez sur **Afficher les journaux LC**.
2. Sélectionnez les serveurs dont vous souhaitez afficher les journaux, cliquez sur le menu déroulant **Journaux LC**, puis cliquez sur **Afficher les journaux LC**.

Collecter les journaux LC

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**. Sélectionnez un serveur ou un groupe de serveurs, cliquez sur le menu déroulant **Journaux LC** et cliquez sur **Collecter les journaux LC**.

2 Sélectionnez les serveurs dont vous souhaitez exporter les journaux, cliquez sur le menu déroulant **Journaux LC**, puis cliquez sur **Collecter les journaux LC**.

Remplacement de pièce

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, sélectionnez les serveurs ou un groupe de serveurs, puis cliquez sur **Remplacement de pièce**.

> **REMARQUE : Le nom d'option devient Configurer un remplacement de pièce lorsque vous placez le pointeur sur Remplacement de pièce.**

La fenêtre **Configuration du remplacement de pièce** s'affiche.

2 Sélectionnez les serveurs dont vous souhaitez configurer un composant, puis cliquez sur **Remplacement de pièce**.

> **REMARQUE : Le nom d'option devient Configurer un remplacement de pièce lorsque vous placez le pointeur sur Remplacement de pièce.**

La fenêtre **Configuration du remplacement de pièce** s'affiche.

Interrogation et notification

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, puis cliquez sur **Interrogation et notification**.

2 Cliquez sur **Interrogation et notification**.

Lancement d'iDRAC

1 Dans OMIMSSC, développez **Configuration et déploiement** et sélectionnez l'une des options suivantes :

- Cliquez sur **Vue Serveur**. En fonction du serveur (s'il s'agit d'un hôte ou d'un serveur non attribué), cliquez sur l'onglet **Serveurs non attribués** ou **Hôtes**, puis cliquez sur l'adresse **IP iDRAC** du serveur.

  L'onglet **Serveurs non attribués** s'affiche par défaut.

  Pour afficher l'onglet Hôtes, cliquez sur **Hôtes**.
- Cliquez sur **Vue Cluster**. Développez le type de cluster et développez le groupe de cluster au niveau du serveur.

  L'onglet **Serveur** s'affiche.

2 Pour lancer la console iDRAC, cliquez sur **Adresse IP**.

3 Pour lancer la console iDRAC, cliquez sur **Adresse IP**.

Lancer le module d'entrée/sortie

À propos de cette tâche

Pour lancer la console du module d'entrée/sortie, effectuez les étapes suivantes :

Étapes

1 Dans OMIMSSC, développez **Configuration et déploiement**, cliquez sur **Vue Systèmes modulaires**. Développez le modèle au niveau des périphériques individuels.

Tous les périphériques sous ce modèle s'affichent.

2 Cliquez sur **Modules d'E/S**.

3 Cliquez sur l'**adresse IP** du périphérique.

Résolution des erreurs de synchronisation

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Serveur**, puis cliquez sur **Résoudre les erreurs de synchronisation**.

2 Cliquez sur **Résoudre les erreurs de synchronisation**.

Synchronisation d'OMIMSSC avec la console Microsoft inscrite

À propos de cette tâche

Étapes

1 Dans OMIMSSC, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Serveur**, puis cliquez sur **Synchroniser avec OMIMSSC** pour synchroniser tous les hôtes qui sont répertoriés dans la console MSSC inscrite avec l'appliance OMIMSSC.

2 Pour synchroniser tous les hôtes qui sont répertoriés dans la console MSSC inscrite avec l'appliance, cliquez sur **Synchroniser avec OMIMSSC**.

La synchronisation est une tâche dont la durée est longue. Affichez l'état de la tâche dans la page **Tâches et journaux**.

Attribuer et déployer

Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**. Sélectionnez les serveurs sur lesquels vous souhaitez déployer un modèle, puis cliquez sur **Déployer un Operational Template**.

La page **Déployer un Operational Template** s'affiche.

Exécuter une mise à jour

1 Dans OMIMSSC, cliquez sur **Centre de maintenance**, sélectionnez les serveurs ou les groupes de systèmes modulaires, ainsi qu'une source de mise à jour, puis cliquez sur **Exécuter la mise à jour**.

2 Sélectionnez les serveurs ou les groupes de systèmes modulaires, ainsi qu'une source de mise à jour, puis cliquez sur **Exécuter la mise à jour**.

3 Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Créer**.

Pour effectuer le suivi de la tâche, l'option **Accéder à la liste des tâches** est sélectionnée par défaut.

12

Appendix

Provide the time zone attribute values manually in MX7000 devices by referring to the bellow table:

Tableau 6. Time zone details

Time zone ID	Time zone difference
TZ_ID_1	(GMT-12:00) International Date Line West
TZ_ID_2	(GMT+14:00) Samoa
TZ_ID_3	(GMT-10:00) Hawaii
TZ_ID_4	(GMT-09:00) Alaska
TZ_ID_5	(GMT-08:00) Pacific Time (US and Canada)
TZ_ID_6	(GMT-08:00) Baja California
TZ_ID_7	(GMT-07:00) Arizona
TZ_ID_8	(GMT-07:00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07:00) Mountain Time (US and Canada)
TZ_ID_10	(GMT-06:00) Central America
TZ_ID_11	(GMT-06:00) Central Time (US and Canada)
TZ_ID_12	(GMT-06:00) Guadalajara, Mexico City, Monterrey
TZ_ID_13	(GMT-06:00) Saskatchewan
TZ_ID_14	(GMT-05:00) Bogota, Lima, Quito
TZ_ID_15	(GMT-05:00) Eastern Time (US and Canada)
TZ_ID_16	(GMT-05:00) Indiana (East)
TZ_ID_17	(GMT-04:30) Caracas
TZ_ID_18	(GMT-04:00) Asuncion
TZ_ID_19	(GMT-04:00) Atlantic Time (Canada)
TZ_ID_20	(GMT-04:00) Cuiaba
TZ_ID_21	(GMT-04:00) Georgetown, La Paz, Manaus, San Juan
TZ_ID_22	(GMT-04:00) Santiago
TZ_ID_23	(GMT-03:30) Newfoundland
TZ_ID_24	(GMT-03:00) Brasilia
TZ_ID_25	(GMT-03:00) Buenos Aires
TZ_ID_26	(GMT-03:00) Cayenne, Fortaleza

Time zone ID	Time zone difference
TZ_ID_27	(GMT-03:00) Greenland
TZ_ID_28	(GMT-03:00) Montevideo
TZ_ID_29	(GMT-02:00) Mid-Atlantic
TZ_ID_30	(GMT-01:00) Azores
TZ_ID_31	(GMT-01:00) Cape Verde Is
TZ_ID_32	(GMT+00:00) Casablanca
TZ_ID_33	(GMT+00:00) Coordinated Universal Time
TZ_ID_34	(GMT+00:00) Dublin, Edinburgh, Lisbon, London
TZ_ID_35	(GMT+00:00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
TZ_ID_37	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
TZ_ID_38	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
TZ_ID_39	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
TZ_ID_40	(GMT+01:00) West Central Africa
TZ_ID_41	(GMT+02:00) Windhoek
TZ_ID_42	(GMT+02:00) Amman
TZ_ID_43	(GMT+03:00) Istanbul
TZ_ID_44	(GMT+02:00) Beirut
TZ_ID_45	(GMT+02:00) Cairo
TZ_ID_46	(GMT+02:00) Damascus
TZ_ID_47	(GMT+02:00) Harare, Pretoria
TZ_ID_48	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
TZ_ID_49	(GMT+02:00) Jerusalem
TZ_ID_50	(GMT+02:00) Minsk
TZ_ID_51	(GMT+03:00) Baghdad
TZ_ID_52	(GMT+03:00) Kuwait, Riyadh
TZ_ID_53	(GMT+03:00) Moscow, St. Petersburg, Volgograd
TZ_ID_54	(GMT+03:00) Nairobi
TZ_ID_55	(GMT+03:30) Tehran
TZ_ID_56	(GMT+04:00) Abu Dhabi, Muscat
TZ_ID_57	(GMT+04:00) Baku
TZ_ID_58	(GMT+04:00) Port Louis
TZ_ID_59	(GMT+04:00) Tbilisi
TZ_ID_60	(GMT+04:00) Yerevan

Time zone ID	Time zone difference
TZ_ID_61	(GMT+04:30) Kabul
TZ_ID_62	(GMT+05:00) Ekaterinburg
TZ_ID_63	(GMT+05:00) Islamabad, Karachi
TZ_ID_64	(GMT+05:00) Tashkent
TZ_ID_65	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
TZ_ID_66	(GMT+05:30) Sri Jayawardenepura
TZ_ID_67	(GMT+05:45) Kathmandu
TZ_ID_68	(GMT+06:00) Astana
TZ_ID_69	(GMT+06:00) Dhaka
TZ_ID_70	(GMT+06:00) Novosibirsk
TZ_ID_71	(GMT+06:30) Yangon (Rangoon)
TZ_ID_72	(GMT+07:00) Bangkok, Hanoi, Jakarta
TZ_ID_73	(GMT+07:00) Krasnoyarsk
TZ_ID_74	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
TZ_ID_75	(GMT+08:00) Irkutsk
TZ_ID_76	(GMT+08:00) Kuala Lumpur, Singapore
TZ_ID_77	(GMT+08:00) Perth
TZ_ID_78	(GMT+08:00) Taipei
TZ_ID_79	(GMT+08:00) Ulaanbaatar
TZ_ID_80	(GMT+08:30) Pyongyang
TZ_ID_81	(GMT+09:00) Osaka, Sapporo, Tokyo
TZ_ID_82	(GMT+09:00) Seoul
TZ_ID_83	(GMT+09:00) Yakutsk
TZ_ID_84	(GMT+09:30) Adelaide
TZ_ID_85	(GMT+09:30) Darwin
TZ_ID_86	(GMT+10:00) Brisbane
TZ_ID_87	(GMT+10:00) Canberra, Melbourne, Sydney
TZ_ID_88	(GMT+10:00) Guam, Port Moresby
TZ_ID_89	(GMT+10:00) Hobart
TZ_ID_90	(GMT+10:00) Vladivostok
TZ_ID_91	(GMT+11:00) Magadan, Solomon Is New Caledonia
TZ_ID_92	(GMT+12:00) Auckland, Wellington
TZ_ID_93	(GMT+12:00) Fiji
TZ_ID_94	(GMT+13:00) Nuku'alofa

Time zone ID	Time zone difference
TZ_ID_95	(GMT+14:00) Kiritimati
TZ_ID_96	(GMT+02:00) Athens, Bucharest

13

Accès aux documents à partir du site de support Dell EMC

Vous pouvez accéder aux documents requis en utilisant l'un des liens suivants :

- Pour les documents de gestion des systèmes Dell EMC Enterprise — www.dell.com/esmmanuals
- Pour les documents Dell EMC OpenManage — www.dell.com/openmanagemanuals
- Pour les documents de gestion des systèmes Dell EMC Remote Enterprise — www.dell.com/esmmanuals
- Pour les documents iDRAC et Dell Lifecycle Controller — www.dell.com/idracmanuals
- Pour les documents de gestion des systèmes Dell EMC OpenManage Connections Enterprise — www.dell.com/esmmanuals
- Pour les documents d'outils de facilité de la gestion Dell EMC — www.dell.com/serviceabilitytools
- a Rendez-vous sur www.dell.com/support.
  b Cliquez sur **Parcourir tous les produits**.
  c Dans la section **Tous les produits**, cliquez sur **Logiciel et sécurité**, puis cliquez sur le lien requis parmi les suivants :
  - **Analyse**
  - **Gestion des systèmes Client**
  - **Applications d'entreprise**
  - **Gestion des systèmes Enterprise**
  - **Solutions du secteur public**
  - **UTILITAIRES :**
  - **Châssis principal**
  - **Outils de facilité de la gestion**
  - **Solutions de virtualisation**
  - **Systèmes d'exploitation**
  - **Support**

  d Pour afficher un document, cliquez sur le produit requis, puis cliquez sur la version requise.
- Avec les moteurs de recherche :
  - Saisissez le nom et la version du document dans la zone de recherche.

Contacter Dell

Prérequis

REMARQUE : Si vous ne possédez pas une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, acte de vente ou catalogue de produits Dell.

À propos de cette tâche

Dell offre plusieurs options de service et de support en ligne et par téléphone. La disponibilité des produits varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre région. Pour contacter le service commercial, technique ou client de Dell :

Étapes

1 Rendez-vous sur **Dell.com/support**.
2 Sélectionnez la catégorie d'assistance.
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 de service ou de support en fonction de vos besoins.