OpenManage Integration pour Microsoft System Center version 7.3 pour Microsoft Endpoint Configuration Manager et System Center Configuration Virtual Machine Manager

Guide unifié de l'utilisateur

Juin 2021
Rév. A00

DELL EMC

Remarques, précautions et avertissements

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

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

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

Table des matières

Chapitre 1: Présentation de OMIMSSC 9
Nouveautés 9

Chapitre 2: OMIMSSC licence 11
Options prises en charge pour la fonctionnalité de licence 11
Importer la licence dans OMIMSSC 12
Vue Centre de licences 13

Chapitre 3: OMIMSSC composants 14

Chapitre 4: Matrice de support pour OMIMSSC 16
Versions System Center prises en charge 16
Configuration réseau requise 18
Infrastructure administration using Microsoft System Center Console 20
Configuration matérielle requise pour OMIMSSC 20
Configuration matérielle de l'extension de console OMIMSSC pour SCVMM 21

Chapitre 5: Déployer OMIMSSC 22
Télécharger OMIMSSC à partir du Web 22
Configurer l'appliance OMIMSSC sur Hyper-V 22
Configurer l'appliance OMIMSSC sur ESXi 23
Inscrire plusieurs consoles Microsoft 24
Lancer le portail d'administration OMIMSSC pour télécharger les composants d'OMIMSSC 24
Installer l'extension de console OMIMSSC pour MECM 24
Installer l'extension de console OMIMSSC pour SCVMM 25

Chapitre 6: Inscrire la console Microsoft dans OMIMSSC 26
Accéder à OMIMSSC à partir de la console de Microsoft inscrite 26
Ajouter une adresser FQDN OMIMSSC dans le navigateur 27
Lancer l'extension de console OMIMSSC pour MECM 27
Importer l'extension de console OMIMSSC pour SCVMM 27
Lancer l'extension de console OMIMSSC pour SCVMM 27

Chapitre 7: Gérer OMIMSSC et ses composants 28
Afficher des détails de l'appliance OMIMSSC 28
Afficher la gestion des utilisateurs OMIMSSC 28
Gérer un certificat HTTPS 28
Mettre à jour des certificats de serveurs OMIMSSC inscrits 28
Génération d'une requête de signature de certificat (CSR) 29
Chargement d'un certificat HTTPS 29
Restauration du certificat HTTPS par défaut 29
Afficher ou actualiser des consoles inscrites 29
Modifier le mot de passe de l'appliance OMIMSSC 30
Redémarrer l'appliance OMIMSSC 30

Modifier des comptes MECM et SCVMM dans le portail d'administration OMIMSSC....30
Réparer ou modifier des programmes d'installation....30

Chapitre 8: Sauvegarde et restauration de l'appliance OMIMSSC....32
Sauvegarder l'appliance OMIMSSC....32
Restauration de l'appliance OMIMSSC....33

Chapitre 9: Désinstallation OMIMSSC....34
Annuler l'inscription de console Microsoft depuis OMIMSSC....34
Désinstaller l'extension de console OMIMSSC pour MECM....34
Désinstaller l'extension de console OMIMSSC pour SCVMM....35
Autres étapes de désinstallation....35
Supprimer des RunAsAccounts propres à l'appliance....35
Supprimer le profil d'application OMIMSSC....35
Supprimer la machine virtuelle de l'appliance....35

Chapitre 10: Mettre à niveau OMIMSSC....36

Chapitre 11: Gérer les profils d'identification et d'hyperviseur....37
Profil d'informations d'identification dans MECM et SCVMM....37
Créer un profil d'identification....37
Modifier un profil de référence....38
Supprimer un profil d'informations d'identification....38
Profil d'hyperviseur dans SCVMM....39
Créer un profil d'hyperviseur....39
Modifier le profil d'hyperviseur....40
Supprimer un profil d'hyperviseur....40

Chapitre 12: Détecter des appareils et synchroniser des serveurs avec la console OMIMSSC....41
Découvrir des appareils dans OMIMSSC....41
Découverte d'appareils dans l'extension de console OMIMSSC pour MECM....41
Découverte d'appareils dans l'extension de console OMIMSSC pour SCVMM....41
Conditions préalables pour la découverte d'appareils....42
Découvrir des serveurs par découverte automatique....42
Découvrir des serveurs par découverte manuelle....42
Découvrir les systèmes modulaires MX7000 à l'aide de la découverte manuelle....43
Synchroniser l'extension de console OMIMSSC avec l'instance MECM inscrite....44
Synchroniser l'extension de console OMIMSSC avec l'instance SCVMM inscrite....44
Synchroniser avec la console Microsoft....44
Résoudre des erreurs de synchronisation....45
Afficher le mode System Lockdown....45

Chapitre 13: Supprimer des appareils de OMIMSSC....46
Retirer des systèmes modulaires de OMIMSSC....46

Chapitre 14: Vues dans OMIMSSC....47
Vue Serveur....47
Console iDRAC....48
Vue des systèmes modulaires....48

Console OpenManage Enterprise Modular ... 49
Modules d'entrée/sortie ... 49
Vue cluster ... 50
Vue Centre de maintenance ... 50
Centre des tâches et des journaux ... 50

Chapitre 15: Gérer des Operational Template ... 52
Operational Template prédéfinis ... 53
À propos de la configuration de serveurs de référence ... 53
À propos de la configuration du système modulaire de référence ... 53
Créer un Operational Template à partir de serveurs de référence ... 54
Composant de système d'exploitation Windows pour l'extension de console OMIMSSC pour MECM ... 55
Composant de système d'exploitation Windows pour l'extension de console OMIMSSC pour SCVMM ... 56
Composant non-Windows pour les extensions de console OMIMSSC ... 56
Créer un Operational Template à partir de systèmes modulaires de référence ... 56
Créer des clusters à l'aide d'un Operational Template ... 57
Créer un commutateur logique pour les clusters HCI de serveurs Windows ... 57
Créer des clusters HCI de serveurs Windows ... 58
Afficher le Operational Template ... 59
Modifier un Operational Template ... 59
Configurer des valeurs spécifiques au système (valeurs de pool) à l'aide d'un modèle opérationnel sur plusieurs serveurs ... 60
Attribuer un Operational Template et exécuter la conformité au modèle opérationnel pour les serveurs ... 60
Attribuer un Operational Template pour des systèmes modulaires ... 61
Déploiement de modèles opérationnels ... 61
Déployer un Operational Template sur des serveurs ... 62
Déployer un Operational Template pour système modulaire ... 63
Annuler l'attribution d'un Operational Template ... 63
Supprimer un Operational Template ... 63

Chapitre 16: Déployer le système d'exploitation à l'aide d'OMIMSSC ... 65
À propos de la mise à jour de l'image WinPE ... 65
Fournir un fichier WIM pour MECM ... 65
Fournir un fichier WIM pour SCVMM ... 65
Extraire des pilotes à partir du pack de pilotes du serveur OpenManage ... 66
Mettre à jour une image WinPE ... 66
Préparer le déploiement de système d'exploitation sur la console MECM ... 67
Séquence de tâches-MECM ... 67
Définir un emplacement de partage par défaut pour le support de démarrage Lifecycle Controller ... 68
Créer un support de séquence de tâches (ISO de démarrage) ... 68
Préparer un déploiement de système d'exploitation non-Windows ... 69

Chapitre 17: Provisionner les appareils avec OMIMSSC ... 70
Workflow pour les scénarios de déploiement ... 70
Déployer le système d'exploitation Windows à l'aide de l'extension de console OMIMSSC pour MECM ... 72
Déployer l'hyperviseur à l'aide de l'extension de console OMIMSSC pour SCVMM ... 72
Redéployer un système d'exploitation Windows avec OMIMSSC ... 73
Déployer le système d'exploitation non-Windows à l'aide d'extensions de console OMIMSSC ... 73
Créer des clusters HCI de serveurs Windows à l'aide de Operational Template prédéfinis ... 73

Mettre à jour le firmware des serveurs et des appareils MX7000 ... 74
Configurer des composants remplacés ... 76
Exporter et importer des profils de serveur ... 76

Chapitre 18: Mettre à jour des firmwares OMIMSSC ... 77
À propos des groupes de mise à jour ... 77
Afficher des groupes de mise à jour ... 78
Créer des groupes de mise à jour personnalisée ... 78
Modifier des groupes de mise à jour personnalisée ... 78
Retirer des groupes de mise à jour personnalisée ... 78
À propos des sources de mise à jour ... 79
Configurer un HTTPS local ... 80
Afficher la source de mise à jour ... 80
Créer une source de mise à jour ... 80
Modifier la source de mise à jour ... 81
Modifier la source de mise à jour ... 81
Intégration avec Dell EMC Repository Manager (DRM) ... 81
Intégration de DRM à OMIMSSC ... 82
Définir la fréquence d'interrogation ... 82
Afficher et actualiser l'inventaire d'appareils ... 83
Appliquer les filtres ... 84
Supprimer des filtres ... 84
Mettre à niveau et rétrograder les versions de firmware à l'aide de la méthode d'exécution de mise à jour ... 84
Mises à jour via CAU ... 85

Chapitre 19: Gérer les appareils avec OMIMSSC ... 87
Restauration de serveur ... 87
Archive sécurisée (Protection vault) ... 87
Exporter des profils de serveur ... 88
Importer le profil du serveur ... 88
Appliquer les paramètres de firmware et de configuration sur un composant remplacé ... 89
Collecter des journaux LC pour les serveurs ... 90
Afficher des journaux LC ... 91
Description de fichier ... 91
Exporter l'inventaire ... 92
Gérer des tâches ... 92

Chapitre 20: Déployer le cluster Azure Stack HCI ... 93

Chapitre 21: Dépannage ... 94
Ressources nécessaires à la gestion OMIMSSC ... 94
Vérification des autorisations d'utilisation de l'extension de console OMIMSSC pour MECM ... 94
Configuration de l'accès utilisateur à WMI ... 95
Vérification des autorisations PowerShell d'utilisation de l'extension de console OMIMSSC pour SCVMM ... 96
Installation et mise à niveau de scénarios dans OMIMSSC ... 96
Échec de l'inscription ... 96
Échec du test de connexion ... 97
Échec du lancement d'OMIMSSC après l'installation de l'extension de console MECM ... 97
Échec de la connexion à l'extension de console OMIMSSC pour SCVMM ... 97

Erreur d'accès à l'extension de console après la mise à jour de SCVMM R2 ... 97
Adresse IP non attribuée à l'appliance OMIMSSC ... 98
Blocage de SCVMM lors de l'importation de l'extension de console OMIMSSC ... 98
Échec de la connexion aux extensions de console OMIMSSC ... 98
Blocage de SC2012 VMM SP1 pendant la mise à jour ... 98
OMIMSSC Scénarios du portail d'administration ... 98
Message d'erreur lors de l'accès au portail d'administration d'OMIMSSC via le navigateur Mozilla Firefox ... 98
Échec de l'affichage du logo Dell EMC dans le portail d'administration d'OMIMSSC ... 99
Scénarios de découverte, synchronisation et inventaire dans OMIMSSC ... 99
Échec de la découverte des serveurs ... 99
Échec de la découverte automatique des serveurs iDRAC ... 99
Serveurs découverts non ajoutés à la collecte Tous les serveurs Dell Lifecycle Controller ... 99
Échec de la découverte des serveurs en raison d'informations d'identification incorrectes ... 99
Création de groupe de châssis VRTX incorrect après la découverte des serveurs ... 100
Impossible de synchroniser les serveurs hôtes avec la console MECM inscrite ... 100
Impossible de supprimer un groupe de mise à jour de cluster vide pendant la découverte automatique ou la synchronisation ... 100
Impossible de créer un cluster lors de l'application des fonctionnalités de cluster ... 100
Impossible de récupérer l'état de la tâche de mise à jour compatible adaptée au cluster ... 100
Manquement à effectuer les tâches de maintenance sur les serveurs redécouverts ... 101
Scénarios génériques dans OMIMSSC ... 101
Échec d'accès au partage CIFS à l'aide du nom d'hôte ... 101
Erreur d'affichage de la page Tâches et journaux dans l'extension de console ... 101
Échec des opérations sur les systèmes gérés ... 101
Échec du lancement de l'aide en ligne pour OMIMSSC ... 101
OMIMSSC Échec de tâches en raison d'un mot de passe de partage réseau non pris en charge ... 101
Scénarios de mise à jour de firmware dans OMIMSSC ... 102
Échec du test de connexion pour la source de mise à jour locale ... 102
Échec de la création d'une source de mise à jour DRM ... 102
Impossible de créer un référentiel au cours d'une mise à jour du micrologiciel ... 102
Échec de mise à jour de firmware de clusters ... 102
Impossible de mettre à jour le micrologiciel car la file d'attente des tâches est pleine ... 103
Échec de mise à jour de firmware en utilisant une source de mise à jour DRM ... 103
Mise à jour de firmware de quelques composants, quelle que soit la sélection ... 104
Échec de la suppression d'un groupe de mise à jour personnalisée ... 104
Échec de mise à jour de l'image WinPE ... 104
Modification de la couleur de cloche d'interrogation et de notification après mise à jour de la fréquence ... 104
Scénarios de déploiement de système d'exploitation dans OMIMSSC ... 104
Scénarios génériques de déploiement du système d'exploitation ... 104
Scénarios de déploiement de système d'exploitation pour les utilisateurs MECM ... 105
Scénarios de déploiement de système d'exploitation pour les utilisateurs SCVMM ... 106
Scénarios de création de clusters HCI de serveurs Windows pour les utilisateurs SCVMM ... 107
Scénarios de profil de serveur dans OMIMSSC ... 107
Échec de l'exportation des profils de serveur ... 107
L'importation d'une tâche de profil de serveur expire au bout de deux heures ... 107
Scénarios de journaux LC dans OMIMSSC ... 108
Échec de l'exportation des journaux LC au format .CSV ... 108
Échec de l'ouverture de fichiers journaux LC ... 108
Échec du test de connexion ... 108

Chapitre 22: Annexe I : valeurs des attributs de fuseau horaire..... 109

Chapitre 23: Annexe II : renseigner les valeurs de pool..... 112

Chapitre 24: Accès au contenu de support à partir du site de support Dell EMC..... 117

1

Présentation de OMIMSSC

Ce document est un guide de l'utilisateur unifié qui fournit toutes les informations relatives à l'utilisation, à l'installation et aux pratiques d'excellence d'OMIMSSC.

OpenManage Integration for Microsoft System Center (OMIMSSC) est fourni en tant qu'appliance avec l'intégration de la suite de produits Microsoft System Center. OMIMSSC permet la gestion du cycle de vie complet des serveurs Dell PowerEdge à l'aide du contrôleur iDRAC (Integrated Dell Remote Access Controller) doté du Lifecycle Controller (LC).

OMIMSSC offre le déploiement du système d'exploitation, les solutions Dell EMC HCI pour Microsoft Windows Server, des correctifs matériels, la mise à jour de firmware et la maintenance des serveurs et des systèmes modulaires. Intégrez OMIMSSC à Microsoft Endpoint Configuration Manager (SCCM) (précédemment connu sous le nom de System Center Configuration Manager, SCCM) pour gérer les serveurs Dell PowerEdge dans le datacenter traditionnel ou intégrez OMIMSSC à Microsoft System Center Virtual Machine Manager (SCVMM) pour gérer les serveurs Dell PowerEdge dans des environnements Cloud et virtuels.

Pour plus d'informations sur les modifications apportées aux noms MECM, SCVMM et SCCM, consultez la documentation Microsoft.

Sujets :

- Nouveautés

Nouveautés

- Prise en charge de Microsoft Endpoint Configuration Manager (MECM) version 2103.
- Prise en charge de Microsoft Endpoint Configuration Manager (MECM) version 2010.
- Prise en charge de Microsoft Endpoint Configuration Manager (MECM) version 2006.
- Prise en charge de System Center Virtual Machine Manager (SCVMM) version 2019 UR3.
- Prise en charge de System Center Virtual Machine Manager (SCVMM) version 2019 UR2.
- Prise en charge de System Center Virtual Machine Manager (SCVMM) version 2016 UR10.
- Prise en charge de la gestion personnalisée des certificats SSL.
- Les mises à jour adaptées aux clusters pour HCI et les clusters de basculement incluent désormais la possibilité d'effectuer des mises à jour de pilotes, ainsi que du BIOS et du firmware pour les clusters basés sur Windows Server.
- Prise en charge des nouveaux serveurs PowerEdge basés sur l'iDRAC 9 et sur Intel.
  - R750
  - R750xa
  - R650
  - C6520
  - MX750c
  - XE2420
- Prise en charge de la création de clusters HCI basés sur Windows Server, de la gestion et de la mise à jour adaptée aux clusters des nœuds AX et S2D Ready.
  - AX6515
  - AX740xd
  - AX640
  - R440
- Prise en charge de l'injection de pilotes WinPE à l'aide du pack de pilotes du serveur Dell EMC OpenManage.

  REMARQUE : DTK est un produit de fin de vie de Dell EMC. Utilisez le pack de pilotes du serveur Dell EMC OpenManage pour les pilotes WinPE.
- Prise en charge des versions de déploiement de système d'exploitation ESXi 7.0 U2, 7.0 U1 et 6.7 U3.
- Prise en charge des versions de déploiement du système d'exploitation RHEL 7.9, 8.0, 8.3 et 8.4.
- Document utilisateur restructuré. (Le guide d'installation, le guide de l'utilisateur et les informations de dépannage sont regroupés dans un seul document unifié).

- Prise en charge du déploiement de l'appliance Dell EMC OMIMSSC pour OpenManage Integration pour Microsoft Endpoint Configuration Manager (MECM) et System Center Virtual Machine Manager (SCVMM) version 7.3 sur les versions VMware ESXi suivantes à l'aide du fichier .ova :
  - Version 6.5
  - Version 6.7
  - Version 7.0

avec la prise en charge existante du déploiement de l'appliance OMIMSSC de Dell EMC pour MECM et SCVMM sur Hyper-V en utilisant le fichier .vhd.

2

OMIMSSC licence

OMIMSSC possède deux types de licences :

- La licence d'évaluation : il s'agit d'une version d'évaluation de la licence contenant une licence d'évaluation pour cinq serveurs (hôtes ou non attribués) qui est importée automatiquement après l'installation. Ceci s'applique uniquement aux serveurs de 11e génération Dell EMC (minimum).
- La licence de production : vous pouvez acheter la licence de production auprès de Dell EMC pour n'importe quel nombre de serveurs à gérer par OMIMSSC. Cette licence inclut un support produit et des mises à jour de l'appliance OMIMSSC.

Lorsque vous achetez une licence, le fichier .XML (clé de licence) est téléchargeable sur le service Dell Digital Locker. Si vous ne parvenez pas à télécharger votre ou vos clés de licence, contactez le service de support Dell en vous rendant sur `dell.com/support/softwarecontacts` pour localiser le numéro de téléphone de votre zone géographique pour votre produit.

Vous pouvez découvrir les serveurs dans OMIMSSC en utilisant un fichier de licence unique. Si un serveur est découvert dans OMIMSSC, une licence est utilisée. Et si un serveur est supprimé, une licence est libérée. Une entrée est créée dans le journal d'activité d'OMIMSSC pour les activités suivantes :

- un fichier de licence est importé ;
- un serveur est supprimé d'OMIMSSC et une licence est libérée ;
- une licence est utilisée après la découverte d'un serveur.

Après la mise à niveau d'une licence d'évaluation vers une licence de production, la licence d'évaluation est remplacée par la licence de production. Le nombre de **Nœuds de licence** est égal au nombre de licences de production achetées.

Sujets :

- Options prises en charge pour la fonctionnalité de licence
- Importer la licence dans OMIMSSC
- Vue Centre de licences

Options prises en charge pour la fonctionnalité de licence

Vous trouverez ci-dessous les options prises en charge pour la fonctionnalité de licence dans OMIMSSC

Acheter une nouvelle licence

Lorsque vous passez une commande pour l'achat d'une nouvelle licence, Dell vous envoie un e-mail de confirmation de commande et vous pouvez télécharger le nouveau fichier de licence à partir de la boutique en ligne Dell. La licence est au format .xml. Si la licence est au format .zip, extrayez le fichier .xml de licence à partir du fichier .zip avant le chargement.

Empiler plusieurs licences

Vous pouvez empiler plusieurs licences de production pour augmenter le nombre de serveurs pris en charge à la somme des serveurs présents dans les licences chargées. Une licence d'évaluation ne peut pas être empilée. Le nombre de serveurs pris en charge ne peut pas être augmenté par empilage et nécessite l'utilisation de plusieurs appliances OMIMSSC.

Si plusieurs licences sont déjà chargées, le nombre de serveurs pris en charge correspond au nombre total de serveurs indiqué dans les licences au moment où la dernière licence a été téléchargée.

Remplacer les licences

S'il y a un problème avec votre commande, ou lorsque vous essayez de télécharger un fichier modifié ou corrompu, un message d'erreur s'affiche. Vous pouvez demander un autre fichier de licence au service Dell Digital Locker. Une fois que vous avez reçu une licence de remplacement, la licence de remplacement contient les mêmes ID de droits que la licence précédente. Lorsque vous chargez une licence de remplacement, la licence est remplacée si une licence a déjà été chargée avec les mêmes ID de droit.

Réimporter des licences

Si vous tentez d'importer le même fichier de licence, un message d'erreur s'affiche. Achetez une nouvelle licence et importez le nouveau fichier de licence.

Importer plusieurs licences

Vous pouvez importer plusieurs fichiers de licence avec différents ID de droits pour augmenter le nombre de serveurs que vous pouvez découvrir et maintenir dans OMIMSSC.

licences de mise à niveau

Vous êtes autorisé à utiliser OMIMSSC avec le fichier de licence existant pour toutes les générations de serveurs prises en charge. Si le fichier de licence ne prend pas en charge la dernière génération de serveurs, achetez de nouvelles licences.

Licence d'évaluation

Lorsqu'une licence d'évaluation expire, plusieurs zones clés cessent de fonctionner et affichent un message d'erreur.

Consommation des licences dans OMIMSSC après la découverte des serveurs

Lorsque vous tentez d'ajouter un hôte ou de découvrir un serveur sur matériel vierge, vous êtes averti de votre utilisation, et il est recommandé d'acheter de nouvelles licences dans les cas suivants :

- Si le nombre de serveurs sous licence dépasse le nombre de licences achetées.
- Si vous avez découvert un nombre de serveurs équivalant au nombre de licences achetées.
- Si vous dépassez le nombre de licences achetées, vous bénéficiez d'une licence de grâce.
- Si vous avez dépassé le nombre de licences achetées et toutes les licences de grâce.

REMARQUE : La licence de grâce représente 20 % du nombre total de licences achetées. Par conséquent, les licences réelles que vous pouvez utiliser dans OMIMSSC correspondent au nombre total de licences achetées, plus la licence de grâce.

Importer la licence dans OMIMSSC

Après l'achat d'une licence, importez-la dans OMIMSSC en procédant comme suit :

1. Dans le portail d'administration OMIMSSC, cliquez sur **Centre de licence**.
2. Cliquez sur **Importer la licence** et naviguez pour sélectionner le fichier de licence téléchargé à partir de la boutique en ligne Dell.

   REMARQUE : Vous ne pouvez que des fichiers de licence valides. Si le fichier est corrompu ou altéré, un message d'erreur s'affiche en conséquence. Téléchargez à nouveau le fichier à partir de la boutique en ligne Dell ou contactez un représentant de Dell pour obtenir un fichier de licence valide.

Vue Centre de licences

1. Ouvrez un navigateur et fournissez l'URL de l'appliance OMIMSSC.

   La page de connexion du portail d'administration OMIMSSC s'affiche.

2. Cliquez sur **Centre de licences**.

   La page comprend les informations suivantes :

   Récapitulatif des licences : affiche les détails de la licence pour OMIMSSC.
   - **Nœuds des licences** : nombre total de licences achetées.
   - **Nœuds utilisés** : nombre de serveurs détectés et qui utilisent la licence.
   - **Nœuds disponibles** : autres nœuds sous licence que vous pouvez détecter dans OMIMSSC.

   Gestion des licences : affiche chaque fichier de licence importé ainsi que ses détails, tels que l'ID de droits, la description du produit, la date à laquelle le fichier de licence a été importé, la date à partir de laquelle le fichier de licence est valide, ainsi que la liste de toutes les générations de serveur prises en charge par la licence.

3

OMIMSSC composants

Voici la liste des composants d'OMIMSSC et leurs noms utilisés dans ce guide :

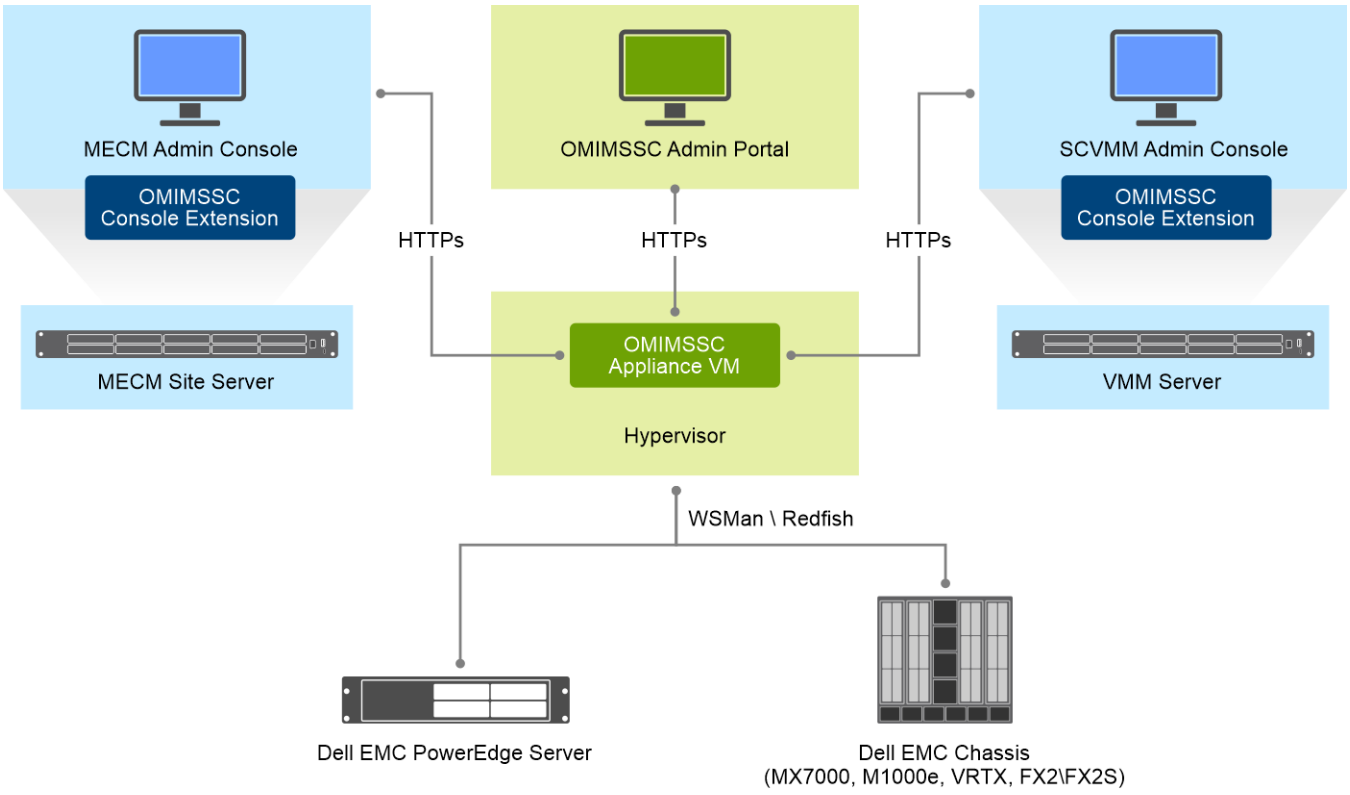
Tableau 1. Composants dans OMIMSSC

Composants	Description
OpenManage Integration for Microsoft System Center Machine virtuelle de l'appliance, également connue sous le nom d'appliance OMIMSSC.	Héberge l'appliance OMIMSSC sur un Hyper-V en tant que machine virtuelle basée sur CentOS et effectue les tâches suivantes : ● Interagit avec les serveurs Dell EMC via l'iDRAC, à l'aide de commandes WSMan (Web Services-Management). ● Interagit avec les périphériques Dell EMC PowerEdge MX7000 via OpenManage Enterprise Module (OME-Modular) à l'aide de commandes de l'API REST.
Portail d'administration	Les activités suivantes sont gérées à l'aide du portail d'administration : ● Gestion des licences ● Enregistrement de System Center avec OMIMSSC ● Gestion de l'appliance ● Mise à niveau et sauvegarde de l'appliance ● Téléchargement du journal de l'appliance
OpenManage Integration for Microsoft System Center console, également connue sous le nom de console OMIMSSC.	La même extension de console est utilisée sur les consoles MECM et SCVMM. Elle est également appelée : ● OMIMSSC Extension de console pour MECM ● OMIMSSC Extension de console pour SCVMM

Les systèmes de gestion sont les systèmes sur lesquels sont installés l'appliance OMIMSSC et ses composants.

Les systèmes gérés sont les serveurs qui sont gérés par OMIMSSC.

Architecture OMIMSSC



4

Matrice de support pour OMIMSSC

Sujets :

- Versions System Center prises en charge
- Configuration réseau requise
- Infrastructure administration using Microsoft System Center Console
- Configuration matérielle requise pour OMIMSSC
- Configuration matérielle de l'extension de console OMIMSSC pour SCVMM

Versions System Center prises en charge

Toutes les versions MECM et SCVMM disponibles pour OMIMSSC sont les suivantes :

OMIMSSC **Centre de systèmes pris en charge**

- Microsoft System Center Configuration Manager (SCCM) version 2012 R2
- Microsoft System Center Configuration Manager (SCCM) version 2012 R2 SP1
- Microsoft System Center Configuration Manager (SCCM) version 1809
- Microsoft System Center Configuration Manager (SCCM) version 1810
- Microsoft System Center Configuration Manager (SCCM) version 1902
- Microsoft System Center Configuration Manager (SCCM) version 1906
- Microsoft Endpoint Configuration Manager (MECM) version 1910
- Microsoft Endpoint Configuration Manager (MECM) version 2002
- Microsoft Endpoint Configuration Manager (MECM) version 2103
- Microsoft Endpoint Configuration Manager (MECM) version 2010
- Microsoft Endpoint Configuration Manager (MECM) version 2006
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2012 R2
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2016
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2016 UR8
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2016 UR9
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2016 UR3
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2019
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2019 UR1
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2019 UR2
- Microsoft System Center Virtual Machine Manager (SCVMM) version 2019 UR10

Tableau 2. Périphériques pris en charge

Système Dell EMC	Version prise en charge
Serveurs PowerEdge basés sur l'iDRAC 9	• Pack de pilotes du système d'exploitation pour plates-formes prises en charge : ○ R750, R750xa et R650 - 21.03.10 et versions ultérieures ○ XE2420 - 20.11.04 ○ R6515, R7515, C6525, et R6525 - 19.12.08 ○ R7525 - 19.12.07 ○ C6520 - 21.03.10 ou ultérieure ○ MX750c - 21.03.10 ou ultérieure • Version de Lifecycle Controller et version d'Integrated Dell EMC Remote Access Controller pour les plates-formes AMD prises en charge : ○ R750, R750xa et R650 - 4.40.20.00 et versions ultérieures

Tableau 2. Périphériques pris en charge (suite)

Système Dell EMC	Version prise en charge
	○ XE2420 - 4.40.10.00 ○ C6520 - 4.40.20.0 ou version ultérieure ○ MX750c - 4.40.20.0 ou version ultérieure ● Pack de pilotes Dell EMC OpenManage Server version 10.0.1 ● **MECM** ○ R6515 et R7515 - 3.40.40.40 ou version ultérieure ○ C6525 et R6525 - 3.42.42.42 ou version supérieure ○ R7525 - 4.10.10.10 ou version ultérieure ● **SCVMM** ○ R6515, R7515, C6525, R6525 et R7525-4.30.30.30 ou versions ultérieures **REMARQUE :** Le déploiement du système d'exploitation avec la méthode boot to vFlash \ stage to vFLash et les fonctions de sauvegarde du profil du serveur ne sont pas pris en charge.
Serveurs PowerEdge 14e génération	● Pack de pilotes du système d'exploitation : 17.05.21 ● Version de Lifecycle Controller et version d'Integration Dell EMC Remote Access Controller - 3.00.00.00 ou ultérieure ● Pack de pilotes Dell EMC OpenManage Server version 10.0.1
Serveurs PowerEdge 13e génération	● Pack de pilotes du système d'exploitation : 16.08.13 ● Lifecycle Controller version-2.40.40.40 ou ultérieure ● Integration Dell Remote Access Controller version 2.40.40.40 ou ultérieure ● Pack de pilotes Dell EMC OpenManage Server version 10.0.1
Serveurs PowerEdge 12e génération	● Pack de pilotes du système d'exploitation : pour les serveurs R220 & FM120 - 16.08.13 ● Autre pack de pilotes du système d'exploitation pour plates-formes prises en charge : 15.07.07 ● Lifecycle Controller version 2.40.40.40 ou ultérieure ● Integration Dell Remote Access Controller version 2.40.40.40 ou ultérieure ● Pack de pilotes Dell EMC OpenManage Server version 10.0.1
Chassis Management Console (CMC)	● FX2 1.4 ou ultérieure ● M1000e 5.2 ou ultérieure ● VRTX 2.2 ou ultérieure
Dell EMC OpenManage Enterprise-Modular	● Châssis 1.0 PowerEdge MX7000
Nœuds Ready d'espaces de stockage direct pris en charge (à l'aide du système d'exploitation Windows Server) en tant que nœuds cibles pour les solutions Dell EMC HCI pour Microsoft Windows Server.	Nœuds AX : AX-640, AX-740xd et AX-6515. Nœuds Ready d'espaces de stockage direct : R440, R640, R740xd et R740xd2

REMARQUE : La prise en charge de la 11e génération de serveurs PowerEdge est supprimée à partir de la version 7.2.1 d'OMIMSSC.

Tableau 3. Systèmes d'exploitation pris en charge (Déploiement) :

Systèmes d'exploitation	Version prise en charge
Microsoft Windows	● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2
Pour les systèmes d'exploitation hors Windows	● RHEL 8.0, 8.3, 8.4 ● RHEL 7.2, 7.3, 7.4, 7.5

Tableau 3. Systèmes d'exploitation pris en charge (Déploiement) : (suite)

Systèmes d'exploitation	Version prise en charge
	• RHEL 6.9
VMware ESXi	• ESXi 7.0 U2 - A00 • ESXi 7.0 U1 - A05 • ESXi 6.7 U3 - A10 • ESXi 6.7 - A06 • ESXi 6.5 U3 • ESXi 6.5 U1 - A11 • ESXi 6.5 - A03 • ESXi 6.0 U3 - A15 • ESXi 6.0 - A02 **REMARQUE :** Téléchargez l'image sur https://www.dell.com/support/, et reportez-vous à la page Pilotes et téléchargements du modèle de serveur spécifique conformément aux versions prises en charge par OMIMSSC.

OMIMSSC Clusters pris en charge

- Création et gestion de clusters compatibles HCI pour Windows Server 2016 et 2019 sur la console SCVMM
- Gestion des clusters d'hôtes hyper-V de Windows 2012 R2, 2016 et 2019 sur la console SCVMM

Configuration réseau requise

Cette section répertorie toutes les exigences relatives aux ports pour configurer votre appliance virtuelle et les nœuds gérés.

Tableau 4. Appliance virtuelle

Numéro de port	Protocoles	Type de port	Niveau de chiffrement maximum	Direction	Destination	Utilisation	Description
53	DNS	TCP	Aucun	Sortant	Appliance OMIMSSC vers serveur DNS	Client DNS	Utilisé comme connectivité au serveur DNS ou résolution des noms d'hôte.
68	DHCP	UDP	Aucun	Entrant	Serveur DHCP vers appliance OMIMSSC	Configuration du réseau dynamique	Pour obtenir des informations détaillées sur le réseau, telles que l'adresse IP, la passerelle, le masque de réseau et le DNS.
69	TFTP	UDP	128 bits	Sortant	OMIMSSC vers iDRAC	Protocole simplifié de transfert de fichiers	Permet de mettre à jour le serveur sans système d'exploitation vers la version de firmware minimale prise en charge.
123	NTP	UDP	Aucun	Entrant	NTP vers appliance OMIMSSC	Synchronisation de l'heure	Pour synchroniser avec un fuseau horaire spécifique.
80/443	HTTP/HTTPS	TCP	Aucun	Sortant	Appliance OMIMSSC vers Internet	Accès Dell Online Data	Utilisé comme connectivité à la garantie en ligne (Internet), au firmware et aux dernières informations RPM.
443	HTTPS	TCP	128 bits	Entrant	UI OMIMSSC vers appliance OMIMSSC	Serveur HTTPS	Services Web offerts par OMIMSSC. Ces services Web sont consommés par vSphere Client et le portail d'administration Dell.

Tableau 4. Appliance virtuelle (suite)

Numéro de port	Protocoles	Type de port	Niveau de chiffrement maximum	Direction	Destination	Utilisation	Description
443	HTTPS	TCP	128 bits	Entrant	Serveur ESXi vers appliance OMIMSSC	Serveur HTTPS	Utilisé dans le flux de déploiement du système d'exploitation afin que les scripts post-installation communiquent avec l'appliance OMIMSSC.
443	HTTPS	TCP	128 bits	Entrant	iDRAC vers appliance OMIMSSC	Découverte automatique	Serveur de provisionnement utilisé pour la détection automatique de nœuds gérés.
443	WS-MAN	TCP	128 bits	Entrée/ Sortie	Appliance OMIMSSC vers/depuis iDRAC	Communication iDRAC	Communications iDRAC ou CMC ou OME-Modular utilisées pour gérer et surveiller les nœuds gérés.
111	HTTPS	TCP	Aucun	Entrant	iDRAC vers appliance OMIMSSC	Appel de procédure distante	Utilisé pour déterminer l'adresse de la fonction RPC.
4433	HTTPS	TCP	Aucun	Entrant	iDRAC vers appliance OMIMSSC	Découverte automatique	Utilisé pour la découverte automatique.
445/139	SMB	TCP	128 bits	Sortant	Appliance OMIMSSC vers CIFS	Communication CIFS	Pour communiquer avec le partage Windows.
2049	NFS	UDP/TCP	Aucun	Entrée/ Sortie	Appliance OMIMSSC vers NFS	Partage public	Partage public NFS exposé par l'appliance OMIMSSC vers les nœuds gérés et utilisé dans la mise à jour de firmware et les flux de déploiement du système d'exploitation.
4001 à 4004	NFS	UDP/TCP	Aucun	Entrée/ Sortie	Appliance OMIMSSC vers NFS	Partage public	Ces ports doivent être maintenus ouverts pour exécuter les services statd, quotd, lockd et mountd par les protocoles V2 et V3 du serveur NFS.
Défini par l'utilisateur	N'importe lequel	UDP/TCP	Aucun	Sortant	Appliance OMIMSSC vers serveur proxy	Proxy	Pour communiquer avec le serveur proxy.

Tableau 5. Nœuds gérés (ESXi)

Numéro de port	Protocoles	Type de port	Niveau de chiffrement maximum	Direction	Destination	Utilisation	Description
443	WS-MAN	TCP	128 bits	Entrant	Appliance OMIMSSC vers ESXi	Communication iDRAC	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.
443	HTTPS	TCP	128 bits	Entrant	Appliance OMIMSSC vers ESXi	Serveur HTTPS	Utilisée pour fournir des informations à la station de gestion. Ce port doit s'ouvrir à partir d'ESXi.

Pour plus d'informations sur l'iDRAC et pour obtenir des informations sur le port CMC, reportez-vous au *Guide de l'utilisateur de Integrated Dell Remote Access Controller* et au *Guide de l'utilisateur de Dell Chassis Management Controller* disponibles à l'adresse **https://www.dell.com/support**.

Pour plus d'informations sur les ports OME-Modular, voir le *Guide de l'utilisateur de Dell EMC OME-Modular* disponible à l'adresse **https://www.dell.com/support**.

Infrastructure administration using Microsoft System Center Console

Microsoft System Center user account privileges

All the required account privileges to use OMIMSSC are as follows:

User must be member of the following groups in System Center Consoles for Account privileges to use OMIMSSC console extension.

Table 6. User accounts with required privileges

Users	Privileges/Roles
For enrollment	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a member of administrator role in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.
For logging in to console extensions	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a delegated admin or an administrator in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.

Configuration matérielle requise pour OMIMSSC

Avant d'installer OMIMSSC, assurez-vous d'effectuer les installations logicielles pré-requises suivantes selon les trois composants OMIMSSC listés :

- OMIMSSC Appliance :
  - Installez Windows Server et activez le rôle Hyper-V.
  - Vous pouvez maintenant inscrire autant de consoles MECM ou SCVMM que souhaité avec une appliance OMIMSSC, car OMIMSSC prend en charge l'inscription de plusieurs consoles. Selon le nombre de consoles que vous prévoyez d'inscrire, la configuration matérielle requise est la suivante :

    Tableau 7. La configuration matérielle requise

Composants	Pour une console MECM ou SCVMM	Pour N consoles MECM ou SCVMM
RAM	8 Go	8 Go*N
Nombre de processeurs	4	4*N

- Installez l'une des versions suivantes du système d'exploitation Windows :
  - Windows Server 2019
  - Windows Server 2016
  - Windows server 2012 R2
  - Windows Server 2012
- Installez l'une des versions d'ESXi suivantes :
  - Version 6.5
  - Version 6.7
  - Version 7.0
- OMIMSSC portail d'administration : Installez l'un des navigateurs pris en charge suivants :
  - Internet Explorer 10 ou supérieur
  - Mozilla Firefox 30 ou supérieur

- Google Chrome 23 ou supérieur
- Microsoft Edge

Configuration matérielle de l’extension de console OMIMSSC pour SCVMM

Pour installer l’extension de console OMIMSSC pour SCVMM :

- Installez les mêmes versions de console d'administration SCVMM et serveur SCVMM.
- La fonctionnalité clustering de basculement est activée sur le serveur SCVMM.
- L’utilisateur inscrit doit disposer de droits d’administrateur sur le serveur SCVMM.
- L’utilisateur inscrit doit disposer de droits d’administrateur sur le cluster géré.

5

Déployer OMIMSSC

Sujets :

- Télécharger OMIMSSC à partir du Web
- Configurer l'appliance OMIMSSC sur Hyper-V
- Configurer l'appliance OMIMSSC sur ESXi
- Inscrire plusieurs consoles Microsoft
- Lancer le portail d'administration OMIMSSC pour télécharger les composants d'OMIMSSC

Télécharger OMIMSSC à partir du Web

Pour télécharger OMIMSSC depuis https://www.dell.com/support procédez comme suit :

1. Cliquez sur **Parcourir tous les produits** > **Logiciel** > **Gestion des systèmes Enterprise** > **OpenManage Integration pour Microsoft System.**
2. Sélectionnez la version requise d'OMIMSSC.
3. Cliquez sur l'onglet **Pilotes et téléchargements**.
4. Téléchargez le fichier vhd d'OMIMSSC.
5. Extrayez le fichier vhd, puis configurez l'appliance OMIMSSC.
   La taille du fichier vhd est d'environ 5 Go, ce qui signifie que le déploiement prendra environ cinq à dix minutes.
6. Spécifiez l'emplacement de décompression des fichiers, puis cliquez sur le bouton Décompresser pour extraire les fichiers :
   - **OMIMSSC_<file version>_for_VMM_and_ConfigMgr**

Configurer l'appliance OMIMSSC sur Hyper-V

Assurez-vous de respecter les points suivants sur l'Hyper-V sur lequel vous configurez l'appliance OMIMSSC :

- Le commutateur virtuel est configuré et disponible.
- Allouez de la mémoire pour la machine virtuelle de l'appliance OMIMSSC en fonction du nombre de consoles Microsoft que vous prévoyez d'inscrire. Pour plus d'informations, reportez-vous à la section Exigences communes.

Pour configurer l'appliance OMIMSSC :

1. Déployez la machine virtuelle de l'appliance OMIMSSC en procédant comme suit :
   a. Dans **Windows Server**, **Gestionnaire Hyper-V**, depuis le menu **Actions**, sélectionnez **Nouveau** et cliquez sur **Nouvelle machine virtuelle**.
      L'**Assistant Nouvelle machine virtuelle** s'affiche.
   b. Dans **Avant de commencer**, cliquez sur **Suivant**.
   c. Dans **Spécifier un nom et un emplacement**, indiquez un nom pour la machine virtuelle.
      Si vous souhaitez stocker la machine virtuelle à un autre emplacement, sélectionnez **Stocker la machine virtuelle à un autre emplacement**, cliquez sur **Parcourir** et accédez au nouvel emplacement.
   d. Dans **Spécifier la génération**, sélectionnez **Génération 1**, puis cliquez sur **Suivant**.
   e. Dans **Affecter la mémoire**, attribuez la capacité de mémoire mentionnée dans les conditions préalables.
   f. Dans **Configurer la mise en réseau**, sous **Connexion**, sélectionnez le réseau que vous souhaitez utiliser, puis cliquez sur **Suivant**.
   g. Dans **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque dur virtuel existant**, accédez à l'emplacement du fichier VHD **OMIMSSC_<file version>_for_VMM_and_ConfigMgr**, puis sélectionnez le fichier.
      La taille du fichier vhd est d'environ 5 Go, ce qui signifie que le déploiement prendra environ cinq à dix minutes.
   h. Sous **Récapitulatif**, vérifiez les informations que vous avez fournies, puis cliquez sur **Terminer**.
   i. Définissez le **Nombre de processeurs virtuels** sur 4. Par défaut, le nombre de processeurs est défini sur 1.
      Pour définir le nombre de processeurs :

i. Cliquez avec le bouton droit sur l'appliance OMIMSSC et sélectionnez **Paramètres**.
ii. Dans **Paramètres**, sélectionnez **Processeur** et définissez le **Nombre de processeurs virtuels** sur `4`.

2. Effectuez les tâches suivantes une fois que l'appliance OMIMSSC démarre :

REMARQUE : Il est recommandé d'attendre cinq minutes avant de vous connecter en tant qu'**Administrateur** afin que tous les services soient lancés.

a. Dans **Connexion localhost** : saisissez admin.
b. Dans **Saisissez le nouveau mot de passe administrateur** : saisissez un mot de passe.

REMARQUE : Dell EMC recommande de configurer et d'utiliser des mots de passe forts pour authentifier l'utilisateur de l'appliance `admin` et l'extension de console.

c. Dans **Confirmer le nouveau mot de passe administrateur** : saisissez de nouveau le mot de passe et appuyez sur **Entrée** pour continuer.
d. Dans les options listées, sélectionnez **Configurer le réseau**, appuyez sur **Entrée** et effectuez les opérations suivantes :
   - Dans **NetworkManagerTUI**, sélectionnez **Configurer le nom de l'hôte du système**, fournissez le nom de l'appliance OMIMSSC et cliquez sur **OK**.

     Par exemple : `Hostname.domain.com`

     REMARQUE : Vous pouvez modifier l'adresse IP de l'appliance OMIMSSC en sélectionnant l'option **Configurer le réseau**. Vous ne pouvez pas modifier l'adresse IP ou le nom de l'hôte de l'appliance OMIMSSC après ce point.
   - Si vous fournissez une adresse IP statique, sélectionnez **Modifier une connexion**, puis sélectionnez **Ethernet0**.

     Sélectionnez **CONFIGURATION IPv4**, **Manuel** et cliquez sur **Afficher**. Indiquez l'adresse de configuration IP, l'adresse de passerelle, l'IP du serveur DNS et cliquez sur **OK**.

e. Notez l'URL du portail d'administration OMIMSSC à partir de l'appliance OMIMSSC.

REMARQUE : Ajoutez l'adresse IP de l'appliance OMIMSSC et le FQDN dans Zones de recherche directe et Zones de recherche indirecte dans DNS.

REMARQUE : Les journaux de l'appliance sont accessibles aux utilisateurs non administrateurs. Toutefois, ces journaux ne contiennent pas de données sensibles. Comme solution de contournement, protégez l'URL de l'appliance.

Configurer l'appliance OMIMSSC sur ESXi

Avant de déployer OMIMSSC à l'aide d'ESXi, assurez-vous d'extraire le fichier OVA du fichier ZIP compressé vers un lecteur local. Pour déployer OMIMSSC sur ESXi, procédez comme suit :

1. Démarrez ESXi à l'aide de l'adresse IP.
   La page de connexion VMware ESXi s'affiche.
2. Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur Se connecter.
3. Dans le volet de gauche, sélectionnez Machines virtuelles.
4. Pour créer une machine virtuelle, sélectionnez Créer ou Enregistrer une machine virtuelle.
   L'Assistant Nouvelle machine virtuelle s'affiche.
   a. Dans la section Sélectionner un type de création, sélectionnez Déployer une machine virtuelle à partir d'un fichier OVF ou OVA.
   b. Cliquez sur Suivant.
   c. Dans la section Sélectionner des fichiers OVF et VMDK, saisissez un nom pour la machine virtuelle que vous souhaitez créer.
   d. Cliquez pour sélectionner des fichiers ou faire un glisser-déposer.
   e. Double-cliquez sur le fichier OMIMSSC_xx.ova. Le pack de gestion OVA est chargé dans le processus d'installation.
   f. Cliquez sur Suivant.
   g. Dans la section Sélectionner le stockage, sélectionnez le stockage ou le datastore dans lequel vous souhaitez stocker les fichiers de configuration et du disque virtuel.
   h. Cliquez sur Suivant.
   i. Dans la section Options de déploiement, sélectionnez les mappages réseau requis.
      - La fonctionnalité de provisionnement de disque Dynamique est sélectionnée par défaut.
      - L'option de mise sous tension automatique de la machine virtuelle est activée.
   j. Cliquez sur Suivant.

k. Dans la section Prêt à terminer, vérifiez les paramètres que vous avez spécifiés, puis cliquez sur Terminer.

   Le processus de création de la VM démarre. Vous pouvez afficher l'état de l'opération dans le volet Tâches récentes.

5. Activez l'option Synchroniser l'heure de l'invité avec celle de l'hôte sur la machine virtuelle hébergée sur ESXi :
   a. Sélectionnez la machine virtuelle et cliquez sur Modifier les options.
   b. Sélectionnez Options VM.
   c. Sélectionnez VMware Tools > Heure > Synchroniser l'heure de l'invité avec celle de l'hôte.

Inscrire plusieurs consoles Microsoft

Gérez les ressources de l'appliance OMIMSSC lorsque plusieurs consoles Microsoft sont inscrites avec OMIMSSC.

En fonction du nombre de consoles Microsoft que vous envisagez d'inscrire sur l'appliance OMIMSSC, assurez-vous que la configuration matérielle requise est respectée. Pour plus d'informations, reportez-vous à la section Configuration matérielle requise commune pour OMIMSSC.

Pour configurer les ressources pour plusieurs consoles Microsoft, procédez comme suit :

1. Lancez et connectez-vous à l'appliance OMIMSSC.
2. Naviguez jusqu'à **Configurer les paramètres d'inscription**, puis cliquez sur **Entrée**.
3. Fournissez le nombre de consoles que vous prévoyez d'inscrire avec l'appliance OMIMSSC.
   Les ressources requises sont répertoriées.

Lancer le portail d'administration OMIMSSC pour télécharger les composants d'OMIMSSC

1. Lancez un navigateur et connectez-vous au portail d'administration OMIMSSC en utilisant les informations d'identification utilisées lors de la connexion à l'appliance OMIMSSC.

   Format : `https://<IP address or FQDN>`

   REMARQUE : Ajoutez l'URL du portail d'administration OMIMSSC dans **Site Intranet local**. Pour plus d'informations, reportez-vous à la section Ajout d'une adresse IP OMIMSSC dans le navigateur.
2. Cliquez sur **Téléchargements**, puis sur **Télécharger le programme d'installation** pour télécharger l'extension de console requise.

Installer l'extension de console OMIMSSC pour MECM

- Assurez-vous d'installer OMIMSSC sur le serveur de site MECM avant de l'utiliser sur la console d'administration MECM.
- Il est recommandé de fermer Configuration Manager avant d'installer, de mettre à niveau ou de désinstaller l'extension de console OMIMSSC pour MECM.

1. Double-cliquez sur `OMIMSSC_MECM(SCCM)_Console_Extension.exe`.
   L'écran de **bienvenue** s'affiche.
2. Cliquez sur **Suivant**.
3. Dans la page **Contrat de licence**, sélectionnez **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.
4. Dans la page **Dossier de destination**, un dossier d'installation est sélectionné par défaut. Pour modifier l'emplacement, cliquez sur **Modifier** et accédez à un nouvel emplacement, puis cliquez sur **Suivant**.
5. Dans la page **Prêt à installer le programme**, cliquez sur **Installer**.

   Le dossier suivant est créé après l'installation de l'extension de console :
   - Log : ce dossier contient les informations de journal se rapportant à la console.
6. Dans **Installation réussie**, cliquez sur **Terminer**.

Recommandation : à partir des configurations installées MECM 2103, l'option **Seules les extensions de console approuvées pour la hiérarchie** dans les propriétés de paramètres **Hiérarchie MECM** doit être désactivée pour que le point de lancement de la console OMIMSSC s'affiche dans la console MECM. Pour plus d'informations, reportez-vous à la section de la console Configuration Manager dans la Documentation de Microsoft.

Installer l'extension de console OMIMSSC pour SCVMM

- Installez l'extension de console OMIMSSC sur le serveur de gestion SCVMM et la console SCVMM. Ce n'est qu'après avoir installé la console OMIMSSC que vous pouvez importer l'extension de console vers SCVMM.

1. Cliquez deux fois sur le fichier `OMIMSSC_SCVMM_Console_Extension.exe`.
   L'écran de **bienvenue** s'affiche.
2. Cliquez sur **Suivant**.
3. Dans la page **Contrat de licence**, sélectionnez **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.
4. Dans la page **Dossier de destination**, un dossier d'installation est sélectionné par défaut. Pour modifier l'emplacement, cliquez sur **Modifier** et accédez à un nouvel emplacement, puis cliquez sur **Suivant**.
5. Dans la page **Prêt à installer le programme**, cliquez sur **Installer**.

   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.
   - OMIMSSC_UPDATE : ce dossier est constitué de toutes les activités qui sont nécessaires pour mettre à jour Cluster Aware (CAU). Ce dossier possède des autorisations de lecture et d'écriture uniquement pour les opérations CAU. Les autorisations WMI (Windows Management Instrumentation) sont configurées pour ce dossier. Pour plus d'informations, reportez-vous à la documentation Windows.
6. Dans la page **Assistant InstallShield terminé**, cliquez sur **Terminer**.
7. Importez l'extension de console OMIMSSC pour SCVMM dans la console SCVMM. Pour plus d'informations, consultez la section Importation de l'extension de console OMIMSSC pour SCVMM.

6

Inscrire la console Microsoft dans OMIMSSC

Assurez-vous que les conditions préalables suivantes et les privilèges du compte requis sont réunis :

- Pour les utilisateurs MECM, l'extension de console OMIMSSC pour la console MECM est installée.
- Pour les utilisateurs SCVMM, l'extension de console OMIMSSC pour SCVMM est installée.

Vérifiez que les informations suivantes sont disponibles :

- Informations d'identification de l'utilisateur du système sur lequel Microsoft System Center est configuré, voir les privilèges du compte requis.
- FQDN de MECM ou FQDN de SCVMM.

Pour inscrire une console MECM ou SCVMM avec OMIMSSC, procédez comme suit :

1. Connectez-vous au portail d'administration OMIMSSC.
2. Cliquez sur **Paramètres**, **Inscription de console**, puis cliquez sur **Inscrire**.
   La page **Inscrire une console** s'affiche.
3. Saisissez le nom et la description de la console.
4. Fournissez le FQDN du serveur de site MECM ou du serveur SCVMM, ainsi que les informations d'identification.
5. Cliquez sur **Créer** pour créer un profil de référence de type Windows, afin d'accéder à la console MECM ou SCVMM.
   - Sélectionnez le **Type de profil de référence** comme **Profil de référence Windows**.
   - Indiquez un nom de profil et une description.
   - Sous **Informations d'identification**, entrez le nom d'utilisateur et le mot de passe.
   - Renseignez les détails du domaine dans **Domaine**.

   REMARQUE : Fournissez le nom de domaine avec les détails du domaine de premier niveau, lors de la création du profil de référence pour l'inscription de 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 MECM ou SCVMM. Utilisez plutôt un autre compte d'utilisateur de domaine pour vous connecter à MECM ou SCVMM.

   Par exemple, si le nom de domaine est `mydomain` et que le domaine de premier niveau est `com`, fournissez le nom de domaine dans le profil de référence en tant que : `mydomain.com`.
6. Pour vérifier les connexions entre l'appliance OMIMSSC et la console Microsoft, cliquez sur **Tester la connexion**.
7. Pour inscrire la console après un test de connexion réussi, cliquez sur **Inscrire**.
   Après l'inscription, OMIMSSC crée un compte dans SCVMM avec le nom **Profil d'enregistrement d'extension de console SCVMM OMIMSSC**. Assurez-vous que ce profil n'est pas supprimé, car vous ne pouvez pas effectuer d'opérations dans OMIMSSC si ce profil est supprimé. Inscrivez le serveur du site MECM de manière à utiliser l'extension de console OMIMSSC sur la console d'administration MECM.

Sujets :

- Accéder à OMIMSSC à partir de la console de Microsoft inscrite

Accéder à OMIMSSC à partir de la console de Microsoft inscrite

Lancez OMIMSSC depuis la console MECM ou SCVMM inscrite.

Ajouter une adresser FQDN OMIMSSC dans le navigateur

Avant de lancer OMIMSSC, ajoutez l'adresse FQDN d'OMIMSSC en tant que prérequis dans la liste de sites **Intranet local** en effectuant les étapes suivantes :

1. Cliquez sur **Paramètres d'IE**, puis sur **Options Internet**.
2. Cliquez sur **Avancé** puis, sous **Paramètres**, recherchez la section **Sécurité**.
3. Décochez l'option **Ne pas enregistrer les pages chiffrées sur le disque** et cliquez sur **OK**.

Lancer l'extension de console OMIMSSC pour MECM

Affichez le tableau des privilèges d'utilisateur mentionné dans Privilèges du compte.

Dans la console MECM, cliquez sur **Équipements et conformité**, **Présentation**, puis sur **Extension de console OMIMSSC pour MECM**.

REMARQUE : Si vous vous connectez à la console MECM en utilisant le protocole RDP (Remote Desktop Protocol), la session OMIMSSC risque d'être fermée si le RDP est fermé. Par conséquent, reconnectez-vous après avoir rouvert la session RDP.

Importer l'extension de console OMIMSSC pour SCVMM

Pour importer l'extension de console OMIMSSC pour SCVMM, procédez comme suit :

1. Lancez la console SCVMM en utilisant le privilège d'administration ou en tant qu'administrateur délégué.
2. Cliquez sur **Paramètres**, puis sur **Importer le complément de console**.
   L'**Assistant Importer le complément de console** s'affiche.
3. Cliquez sur **Parcourir** et sélectionnez le fichier .zip de `C:\Program Files\OMIMSSC\VMM Console Extension`, cliquez sur **Suivant**, puis cliquez sur **Terminer**.
   Assurez-vous que le complément est valide.

Lancer l'extension de console OMIMSSC pour SCVMM

1. Dans la console SCVMM, sélectionnez **Structure**, puis les groupes de serveurs **Tous les hôtes**.

   REMARQUE : Pour lancer OMIMSSC, vous pouvez sélectionner n'importe quel groupe d'hôtes auquel vous avez accès.

2. Dans le ruban **Accueil**, sélectionnez **OMIMSSC Dell EMC**.

7

Gérer OMIMSSC et ses composants

Sujets :

- Afficher des détails de l'appliance OMIMSSC
- Afficher la gestion des utilisateurs OMIMSSC
- Gérer un certificat HTTPS
- Afficher ou actualiser des consoles inscrites
- Modifier le mot de passe de l'appliance OMIMSSC
- Redémarrer l'appliance OMIMSSC
- Modifier des comptes MECM et SCVMM dans le portail d'administration OMIMSSC

Afficher des détails de l'appliance OMIMSSC

1. Lancez le portail d'administration OMIMSSC à partir d'un navigateur.
2. Ouvrez une session sur le portail d'administration OMIMSSC en utilisant les mêmes informations d'identification que celles utilisées lors de la connexion à la machine virtuelle de l'appliance OMIMSSC et cliquez sur **Détails de l'appliance**. L'adresse IP et le nom de l'hôte de l'appliance OMIMSSC s'affichent.

Afficher la gestion des utilisateurs OMIMSSC

1. Lancez le portail d'administration OMIMSSC à partir d'un navigateur.
2. Ouvrez une session sur le portail d'administration OMIMSSC en utilisant les mêmes informations d'identification que celles utilisées lors de la connexion à la machine virtuelle de l'appliance OMIMSSC et cliquez sur **Gestion des utilisateurs d'OMIMSSC**. Le statut des utilisateurs, précédemment connectés à MECM ou SCVMM, s'affiche.

Gérer un certificat HTTPS

OMIMSSC utilise des certificats basés sur la norme PKI x.509 pour l'accès HTTP sécurisé (HTTPS).

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

Pour renforcer la sécurité, il est recommandé d'utiliser les certificats Autorité de certification (AC) ou CA d'entreprise (interne) signés.

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

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

- Un certificat autosigné

  OMIMSSC génère des certificats autosignés lorsque le nom d'hôte de l'appliance est configuré.

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

Mettre à jour des certificats de serveurs OMIMSSC inscrits

L'OMIMSSC utilise l'API OpenSSL pour créer la requête de signature de certificat (RSC) à l'aide de la norme de chiffrement standard RSA, dotée d'une longueur de clé de 2 048 bits.

La RCS générée par OMIMSSC obtient un certificat signé numériquement, provenant d'une autorité de certification de confiance (CA). OMIMSSC utilise ce certificat numérique pour activer HTTPS sur le serveur Web afin de sécuriser la communication. Vous pouvez télécharger un certificat signé par une CA à l'aide du portail d'administration.

Pour plus d'informations sur la gestion des certificats HTTPS dans OMIMSSC, consultez le *Guide de l'utilisateur d'OpenManage Integration pour Microsoft System Center Version 7.3 pour Microsoft Endpoint Configuration Manager et System Center Virtual Machine Manager 7.3, disponible sur* https://www.dell.com/support.

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

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

REMARQUE : Assurez-vous que l'option **Télécharger un fichier** est activée pour télécharger une CSR. Cette option s'applique aux utilisateurs d'**Internet Explorer** et peut être activée à partir d'*Options Internet -> Sécurité -> Internet -> Niveau personnalisé -> Téléchargements*.

Pour générer une CSR, procédez comme suit :

1. Sur la page **Portail d'administration**, sélectionnez **Paramètres > Sécurité**, cliquez sur **Générer une requête de signature de certificat** dans la zone **Certificats SSL**. Un message s'affiche indiquant que si une nouvelle CSR est générée, les certificats créés à l'aide de la CSR précédente ne peuvent plus être chargés sur l'appliance.
2. Si vous poursuivez la requête, dans la boîte de dialogue **Générer une requête de signature de certificat**, saisissez des informations sur le nom commun, l'organisation, la localité, l'état, le pays, l'autre nom d'objet primaire, l'autre nom d'objet secondaire et l'adresse e-mail. Cliquez sur **Générer**.
3. Cliquez sur **Télécharger**, puis sauvegardez la CSR résultant dans un emplacement accessible.

Chargement d'un certificat HTTPS

Assurez-vous que le certificat utilise le format PEM.

Utilisez les certificats HTTPS pour sécuriser les communications avec l'appliance OMIMSSC et les systèmes hôtes ou OMIMSSC. Pour configurer ce type de communications sécurisées, envoyez le certificat CSR à une autorité de certification, puis téléchargez le certificat résultant en utilisant la console d'administration.

1. Sur la page **Portail d'administration**, cliquez sur **Paramètres-> Sécurité**, cliquez sur **Mettre à jour le certificat** dans la zone **Certificats SSL**.
2. Choisissez des options dans la boîte de dialogue **Télécharger un certificat**
3. Pour charger le certificat, cliquez sur **Parcourir**, puis sur **Charger**.
4. Une boîte de dialogue s'affiche pour indiquer que le téléchargement du certificat est terminé.

REMARQUE : Pendant le téléchargement du certificat, l'appliance OMIMSSC peut ne pas répondre pendant quelques minutes pendant le redémarrage des services. Il est recommandé de fermer toutes les sessions de navigateur existantes du portail d'administration OMIMSSC et du plug-in de console OMIMSSC sur les consoles MECM/SCVMM. Reconnectez-vous au portail d'administration OMIMSSC pour afficher le certificat téléchargé.

Restauration du certificat HTTPS par défaut

1. Sur la page **Portail d'administration**, sélectionnez **Paramètres-> Sécurité**, cliquez sur Restaurer le certificat par défaut dans la zone **Certificats SSL**.
2. Dans la boîte de dialogue **RESTAURER LE CERTIFICAT PAR DÉFAUT**, cliquez sur **Oui**.

REMARQUE : Lors de la restauration du certificat par défaut, l'appliance OMIMSSC peut ne pas répondre pendant quelques minutes pendant le redémarrage des services. Il est recommandé d'effacer le cache du navigateur et de fermer les sessions de navigateur existantes du portail d'administration OMIMSSC et du plug-in de console OMIMSSC sur les consoles MECM/SCVMM. Reconnectez-vous au portail d'administration OMIMSSC pour afficher le certificat mis à jour.

Afficher ou actualiser des consoles inscrites

Vous pouvez afficher toutes les consoles Microsoft inscrites avec OMIMSSC en procédant comme suit :

1. Dans le portail d'administration OMIMSSC, cliquez sur **Paramètres**, puis cliquez sur **Inscription de console**.
   Toutes les consoles inscrites s'affichent.

2. Cliquez sur **Paramètres**, puis cliquez sur **Inscription de console**.
   Toutes les consoles inscrites s'affichent.
3. Pour afficher la liste la plus récente des consoles inscrites, cliquez sur **Actualiser**.

Modifier le mot de passe de l'appliance OMIMSSC

Pour modifier le mot de passe de la console de la machine virtuelle de l'appliance OMIMSSC, procédez comme suit :

1. Lancez la console de la machine virtuelle de l'appliance OMIMSSC et connectez-vous en utilisant les anciennes informations d'identification.
2. Naviguez jusqu'à **Modifier le mot de passe administrateur** et appuyez sur **Entrée**.
   L'écran de modification du mot de passe s'affiche.
3. Saisissez votre mot de passe actuel, puis le nouveau en respectant les critères fournis. Resaisissez le nouveau mot de passe et appuyez sur **Entrée**.
   Le statut après la modification du mot de passe s'affiche.
4. Pour revenir à la page d'accueil, appuyez sur **Entrée**.

REMARQUE : L'appliance redémarrera après modification du mot de passe.

Redémarrer l'appliance OMIMSSC

Pour redémarrer l'appliance OMIMSSC, procédez comme suit :

1. Lancez et connectez-vous à la machine virtuelle de l'appliance OMIMSSC.
2. Naviguez jusqu'à **Redémarrer cette appliance virtuelle** et appuyez sur **Entrée**.
3. Pour confirmer, cliquez sur **Oui**.
   L'appliance OMIMSSC est redémarrée, ainsi que tous les services requis.
4. Connectez-vous à l'appliance OMIMSSC après le redémarrage de la machine virtuelle.

Modifier des comptes MECM et SCVMM dans le portail d'administration OMIMSSC

À l'aide de cette option, vous pouvez modifier les mots de passe des comptes MECM et SCVMM dans la console OMIMSSC.

Vous pouvez modifier les mots de passe d'administrateur MECM et SCVMM à partir du portail d'administration OMIMSSC. Ce processus est une activité séquentielle.

1. Modifiez le mot de passe de compte administrateur MECM ou SCVMM dans Active Directory.
2. Modifiez le mot de passe dans OMIMSSC.

Procédez comme suit pour modifier le compte administrateur MECM ou SCVMM dans OMIMSSC :

1. Dans le portail d'administration OMIMSSC, cliquez sur **Paramètres**, puis sur **Inscription de console**.
   Les consoles inscrites s'affichent.
2. Cliquez sur **Paramètres**, puis sur **Inscription de console**.
   Les consoles inscrites s'affichent.
3. Sélectionnez une console à modifier, puis cliquez sur **Modifier**.
4. Fournissez le nouveau mot de passe, puis cliquez sur **Terminer** pour enregistrer les modifications.

Après la mise à jour du mot de passe, relancez la console Microsoft et les extensions de console OMIMSSC en utilisant les nouvelles informations d'identification.

Réparer ou modifier des programmes d'installation

Pour réparer l'un des fichiers du programme d'installation, reportez-vous aux rubriques suivantes :

- Réparation de l'extension de console OMIMSSC pour MECM
- Réparation de l'extension de console OMIMSSC pour SCVMM

Réparer l'extension de console OMIMSSC pour MECM

Pour réparer les fichiers OMIMSSC lorsqu'ils sont corrompus, procédez comme suit :

1. Exécutez l'extension de console OMIMSSC pour le programme d'installation MECM.
   L'écran de **bienvenue** s'affiche.
2. Cliquez sur **Suivant**.
3. Dans **Maintenance de programme**, sélectionnez **Réparer** et cliquez sur **Suivant**.
   L'écran **Prêt à réparer le programme** apparaît.
4. Cliquez sur **Installer**.
   Un écran de progression affiche la progression de l'installation. Une fois l'installation terminée, la fenêtre **Assistant InstallShield terminé** s'affiche.
5. Cliquez sur **Terminer**.

Réparer l'extension de console OMIMSSC pour SCVMM

Pour réparer les fichiers OMIMSSC lorsqu'ils sont corrompus, procédez comme suit :

1. Exécutez *l'extension de console OMIMSSC pour le programme d'installation SCVMM*.
2. Dans **Maintenance de programme**, sélectionnez **Réparer** et cliquez sur **Suivant**.
3. Dans **Prêt à réparer ou supprimer le programme**, cliquez sur **Réparer**.
4. Une fois la tâche de réparation terminée, cliquez sur **Terminer**.

8

Sauvegarde et restauration de l'appliance OMIMSSC

En utilisant l'option **Sauvegarde des données de l'appliance** depuis l'appliance OMIMSSC, enregistrez les informations d'OMIMSSC telles que les consoles Microsoft inscrites, les périphériques découverts, les profils, les sources de mise à jour, les modèles opérationnels, les licences et les tâches terminées dans les extensions de console OMIMSSC.

Sujets :

- Sauvegarder l'appliance OMIMSSC
- Restauration de l'appliance OMIMSSC

Sauvegarder l'appliance OMIMSSC

Cette fonctionnalité permet de sauvegarder la base de données des appliances OMIMSSC et les configurations importantes. Le fichier de sauvegarde est stocké sur le chemin partagé du CIFS avec un mot de passe chiffré fourni par l'utilisateur. Il est recommandé de sauvegarder régulièrement les données de l'appliance.

Configurations requises :

- Assurez-vous que vous créez un partage CIFS avec des informations d'identification d'accès et que vous autorisez les autorisations de lecture et d'écriture.
- Assurez-vous que le même mot de passe de chiffrement est utilisé pour la sauvegarde et la restauration. Le mot de passe de chiffrement ne peut pas être récupéré.

Suivez les étapes suivantes pour sauvegarder les données de l'appliance OMIMSSC sur le partage CIFS.

REMARQUE : Cette fonctionnalité est disponible à partir de la version 7.2.1 d'OMIMSSC et n'est pas disponible sur la console de la machine virtuelle de l'appliance.

1. Dans le portail d'administration OMIMSSC, cliquez sur **Paramètres**, puis sur **Restaurer l'appliance**.
2. Dans la page **Paramètres et détails de la sauvegarde**, indiquez le chemin d'accès au partage CIFS pour la sauvegarde au format `\\<IP address or FQDN>\<folder name>`.
3. Sélectionnez le **Profil d'informations d'identification pour le partage CIFS** dans le menu déroulant.
4. Saisissez le mot de passe de chiffrement dans les champs **Mot de passe** et **Saisir à nouveau le mot de passe**.
5. Cliquez sur **Tester la connexion** pour vérifier la connectivité entre l'appliance OMIMSSC et le partage CIFS. Assurez-vous que le dossier de sauvegarde mentionné existe et est accessible.
6. Cliquez sur **Sauvegarder** pour sauvegarder les données de l'appliance OMIMSSC.

Étapes suivantes

Pour confirmer à nouveau que la sauvegarde est réussie, allez dans le dossier de sauvegarde. Deux fichiers sont créés dans le dossier de sauvegarde au format suivant :

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

REMARQUE : La date et l'heure indiquées dans les fichiers de sauvegarde indiquent quand la sauvegarde a été effectuée. Ne renommez pas le fichier de sauvegarde.

REMARQUE : Assurez-vous que les données de l'appliance ont bien été sauvegardées et que la taille du fichier de sauvegarde est supérieure à 1 Ko. Si la taille du fichier est inférieure à 1 Ko, redémarrez l'appliance. Après le redémarrage de l'appliance, sauvegardez les données de l'appliance OMIMSSC.

Restauration de l'appliance OMIMSSC

- L'opération de restauration doit être exécutée uniquement sur une appliance récemment déployée. Assurez-vous qu'aucune opération n'a été effectuée sur la nouvelle appliance.
- Supprimez l'ancien complément de console SCVMM et mettez à niveau le complément de la console OMIMSSC en téléchargeant le nouveau programme d'installation. Pour plus d'informations, reportez-vous à la section *Mettre à niveau l'extension de console OMIMSSC pour MECM/SCVMM dans le guide unifié de l'utilisateur d'OpenManage Integration for Microsoft System Center*.

Restaurez les données de l'appliance OMIMSSC dans n'importe lequel des scénarios suivants :

- Avant de procéder à la mise à niveau vers une nouvelle version OMIMSSC
- Avant d'effectuer une migration à partir d'une appliance OMIMSSC vers une autre appliance OMIMSSC

Configurations requises :

Assurez-vous de restaurer les données avant d'effectuer des opérations sur la nouvelle appliance OMIMSSC.

Procédez comme suit pour restaurer les données de l'ancienne appliance OMIMSSC vers une nouvelle appliance OMIMSSC.

1. Dans le portail d'administration OMIMSSC, cliquez sur **Paramètres**, puis sur **Restaurer l'appliance**.
2. Il existe deux options disponibles pour la restauration des données de l'appliance.
   - `Option 1: Restore using IP address`

     Cette option doit être utilisée pour restaurer les données des versions 7.2 et 7.2.1 d'OMIMSSC.

     Dans Adresse IP, indiquez l'adresse IP de l'ancienne appliance OMIMSSC, puis cliquez sur Restaurer.

     REMARQUE : Les données sont restaurées sur la nouvelle appliance OMIMSSC.
   - Option 2 : restaurer à l'aide d'un partage CIFS personnalisé

     Cette option doit être utilisée pour restaurer les données à partir de la version 7.2.1 et versions ultérieures.

     REMARQUE : Les informations d'identification d'accès au partage CIFS sont stockées dans la base de données en tant que profil d'identification. Pour des mesures de sécurité supplémentaires, un mot de passe de chiffrement doit être fourni pour déchiffrer le fichier sauvegardé.

   a. Indiquez le chemin de l'emplacement du partage CIFS au format `\\<IP address or FQDN>\<folder name>\<filename>.tar.gz`.
   b. Sélectionnez le profil d'informations d'identification pour le partage CIFS dans le menu déroulant.
   c. Saisissez le mot de passe de chiffrement du fichier et cliquez sur Restaurer.

   La page **Restaurer** est automatiquement déconnectée.
3. Pour afficher le statut de restauration après le redémarrage de l'appliance OMIMSSC :

   Il est recommandé d'attendre quelques minutes avant de vous connecter, de sorte que tous les services soient lancés.

   a. Connectez-vous au portail d'administration OMIMSSC.
   b. Développez **Paramètres**, puis cliquez sur **Journaux**.
   c. Téléchargez le fichier dlciappliance_main.log et recherchez le message suivant pour une restauration réussie :

   ```
   Successfully restored OMIMSSC Appliance
   ```
4. Dans le cas d'une console SCVMM, réimportez le nouveau complément de console après avoir réussi à effectuer une opération de restauration sur l'appliance OMIMSSC.

Effectuez les opérations suivantes après la restauration de l'ancienne appliance OMIMSSC :

- Il est recommandé de recréer les tâches planifiées après la restauration de l'ancienne appliance OMIMSSC.
- Pour les profils d'hyperviseur exportés depuis une version antérieure d'OMIMSSC, assurez-vous de modifier le profil pour fournir le chemin d'accès au fichier ISO et le profil des informations d'identification Windows.
- Créez une nouvelle demande CSR et importez un certificat valide.

9

Désinstallation OMIMSSC

Pour désinstaller OMIMSSC :

1. Annulez l'inscription de la console OMIMSSC depuis le portail d'administration OMIMSSC. Pour plus d'informations, reportez-vous à la section Annulation de l'inscription de la console OMIMSSC.
2. Désinstallez l'extension de la console OMIMSSC pour la console Microsoft enregistrée. Pour plus d'informations, reportez-vous à la section Désinstallation de l'extension de console OMIMSSC pour MECM ou Désinstallation de l'extension de console OMIMSSC pour SCVMM.
3. Supprimez la machine virtuelle de l'appliance OMIMSSC. Pour plus d'informations, reportez-vous à la section Suppression de la machine virtuelle de l'appliance OMIMSSC.
4. Supprimez les comptes spécifiques à l'appliance. Pour plus d'informations, reportez-vous à la section Autres tâches de désinstallation.

Sujets :

- Annuler l'inscription de console Microsoft depuis OMIMSSC
- Désinstaller l'extension de console OMIMSSC pour MECM
- Désinstaller l'extension de console OMIMSSC pour SCVMM
- Autres étapes de désinstallation
- Supprimer la machine virtuelle de l'appliance

Annuler l'inscription de console Microsoft depuis OMIMSSC

Si vous avez inscrit plusieurs consoles Microsoft avec une appliance OMIMSSC, vous pouvez annuler l'inscription d'une console et continuer à travailler avec OMIMSSC. Pour procéder à la désinstallation, consultez le *Guide de l'utilisateur d'OpenManage Integration pour Microsoft System Center*.

Pour annuler l'inscription d'une console Microsoft, procédez comme suit :

1. Dans OMIMSSC, cliquez sur **Inscription de console**.
   Toutes les consoles inscrites avec l'appliance OMIMSSC s'affichent.
2. Sélectionnez la console et cliquez sur **Annuler l'inscription** pour supprimer l'enregistrement de la console avec l'appliance.
3. Désinstallez le plug-in de la console.

   REMARQUE :
   - Après avoir annulé l'inscription et désinstallé une console, les serveurs hôtes associés à la console sont déplacés vers la liste de serveurs non associés dans OMIMSSC.

4. (Facultatif) Si la console est inaccessible, cliquez sur **Oui** à l'invite pour forcer l'annulation de l'inscription de la console.
   - Si une console OMIMSSC est déjà ouverte lors de l'annulation de l'inscription, assurez-vous de fermer la console Microsoft pour terminer l'annulation de l'inscription.
   - Pour les utilisateurs SCVMM :
     - Si vous forcez l'annulation de l'inscription de la console SCVMM depuis OMIMSSC lorsque le serveur SCVMM est inaccessible, supprimez manuellement le **Profil d'application** dans SCVMM.

Désinstaller l'extension de console OMIMSSC pour MECM

Double-cliquez sur `OMIMSSC_MECM(SCCM)_Console_Extension.exe`, sélectionnez **Supprimer** et suivez les instructions affichées à l'écran.

Désinstaller l'extension de console OMIMSSC pour SCVMM

Pour désinstaller l'extension de console OMIMSSC pour SCVMM :

1. Retirez l'extension de console pour **Désinstaller un programme**.
   - Dans **Panneau de configuration**, cliquez sur **Programmes**, puis sur **Désinstaller un programme**
   - Sélectionnez **Complément de console DLCI pour SCVMM**, puis cliquez sur **Désinstaller**.
2. Supprimez l'extension de console dans SCVMM.
   - Dans la console SCVMM, cliquez sur **Paramètres**.
   - Effectuez un clic droit sur **OMIMSSC** et sélectionnez **Supprimer**.

Autres étapes de désinstallation

Pour supprimer l'extension de la console OMIMSSC de SCVMM, supprimez les comptes et profils suivants :

- RunAsAccounts propres à l'appliance
- OMIMSSC Profil d'application

Supprimer des RunAsAccounts propres à l'appliance

Pour supprimer les RunAsAccounts propres à l'appliance de la console SCVMM :

1. Dans la console SCVMM, cliquez sur **Paramètres**.
2. Cliquez sur **Comptes à exécuter tel quel**.
3. Dans la liste des comptes, supprimez les comptes propres à l'appliance.
   Les comptes propres à l'appliance comportent le préfixe `Dell_`.

Supprimer le profil d'application OMIMSSC

1. Dans la console SCVMM, cliquez sur **Bibliothèque**, **Profils**, puis cliquez sur **Profils d'applications**.
   Tous les profils d'application utilisés dans SCVMM s'affichent.
2. Sélectionnez et supprimez le **Profil d'enregistrement OMIMSSC**.

Supprimer la machine virtuelle de l'appliance

Pour supprimer la machine virtuelle de l'appliance :

1. Dans **Windows Server**, sous **Gestionnaire Hyper-V**, cliquez avec le bouton droit sur la machine virtuelle de l'appliance et cliquez sur **Mettre hors tension**.
2. Cliquez avec le bouton droit sur la machine virtuelle de l'appliance, puis cliquez sur **Supprimer**.

REMARQUE : Avant de supprimer la machine virtuelle de l'appliance, effectuez une sauvegarde car il s'agit de la dernière possibilité de réaliser une sauvegarde avant de supprimer la machine virtuelle de l'appliance.

10

Mettre à niveau OMIMSSC

Vous pouvez mettre à niveau l'appliance OMIMSSC vers la dernière version en sauvegardant les données de l'appliance OMIMSSC (notamment les paramètres et les configurations), puis en restaurant le fichier sauvegardé dans la dernière version de l'appliance OMIMSCC.

Pour plus d'informations sur la sauvegarde et la restauration de l'appliance OMIMSSC, reportez-vous à la section Sauvegarde de l'appliance OMIMSSC et à la section Restauration de l'appliance OMIMSSC.

Le tableau suivant fournit des informations sur la stratégie de mise à niveau vers la version 7.3 de l'appliance OMIMSCC. Certaines versions nécessitent une mise à niveau intermédiaire avant une mise à niveau vers la version 7.3 :

Tableau 8. Stratégie de mise à niveau vers la version 7.3 de l'appliance OMIMSCC

Version actuelle de l'appliance OMIMCC	Version intermédiaire de la mise à niveau	Version OMIMSCC cible
7.2.1	N/A (ou mise à niveau directe)	7.3
7.2	N/A (ou mise à niveau directe)	7.3
7.1.1	7.2.1	7.3
7.1	7.2.1	7.3

11

Gérer les profils d'identification et d'hyperviseur

Les profils contiennent toutes les données qui sont requises pour effectuer des opérations dans OMIMSSC.

Sujets :

- Profil d'informations d'identification dans MECM et SCVMM
- Profil d'hyperviseur dans SCVMM

Profil d'informations d'identification dans MECM et SCVMM

Les profils d'informations d'identification simplifient l'utilisation et la gestion des informations d'identification de l'utilisateur en authentifiant les capacités basées sur les rôles de l'utilisateur. Chaque profil d'informations d'identification contient un nom d'utilisateur et un mot de passe pour un seul compte d'utilisateur.

OMIMSSC utilise des profils d'informations d'identification pour se connecter à l'iDRAC des systèmes gérés.

Vous pouvez créer quatre types de profils de référence :

- Profil de référence de périphérique : permet de se connecter à l'iDRAC ou à CMC. En outre, vous pouvez utiliser ce profil afin de découvrir un serveur, résoudre des problèmes de synchronisation et déployer un système d'exploitation. Ce profil est spécifique d'une console. Vous pouvez utiliser et gérer ce profil uniquement dans une console où il est créé.
- Profil de référence Windows : permet d'accéder aux dossiers de partage dans le système d'exploitation Windows.
- Informations d'identification de serveur proxy : permet de fournir les informations d'identification du proxy pour l'accès à des sites FTP pour les mises à jour.

  REMARQUE : Tous les profils autres que le profil de périphérique sont des ressources partagées. Vous pouvez utiliser et gérer ces profils à partir de n'importe laquelle des consoles inscrites.

Créer un profil d'identification

Lors de la création d'un profil de référence, tenez compte des points suivants :

- Pendant la découverte automatique, si un profil de référence par défaut n'est plus disponible pour iDRAC, les informations d'identification iDRAC par défaut sont utilisées. Par défaut, le nom d'utilisateur iDRAC est `root` et le mot de passe est `calvin`.

  REMARQUE : Avant de découvrir tout serveur, Dell EMC recommande de créer un profil d'informations d'identification de l'iDRAC par défaut avec un mot de passe sécurisé. Ce profil d'informations d'identification par défaut sera utilisé pour la découverte automatique. Pour plus d'informations sur les exigences en matière de la stratégie de mots de passe, reportez-vous au guide de l'utilisateur de l'iDRAC.
- Pour obtenir des informations sur les systèmes modulaires, le serveur modulaire est accessible avec le profil CMC par défaut. Par défaut, le nom d'utilisateur CMC est `root` et le mot de passe est `calvin`.
- (Uniquement pour les utilisateurs SCVMM) Lorsqu'un profil de référence de type de périphérique est créé, le compte **RunAsAccount** associé est créé dans **SCVMM** pour gérer le périphérique. Le nom du compte **RunAsAccount** est `Dell_CredentialProfileName`.
- Assurez-vous de ne pas modifier ou supprimer le compte **RunAsAccount** dans la console SCVMM.

1. Dans OMIMSSC, effectuez l'une des étapes suivantes pour créer un **profil de référence** :
   - Dans le tableau de bord OMIMSSC, cliquez sur **Créer un profil de référence**.
   - Dans le volet de navigation, cliquez sur **Profils** > **Profil de référence**, puis sur **Créer**.
2. Cliquez sur **Créer**.
   La page **Profil de référence** s'affiche.

3. Dans **Type de références**, sélectionnez le type de profil de référence que vous voulez utiliser.
4. Indiquez un nom de profil et une description.

   REMARQUE : L'option **Profil par défaut pour** est applicable uniquement pour un profil de référence de type Périphérique.

5. Sous **Informations d'identification**, entrez le nom d'utilisateur et le mot de passe.
   - Si vous créez un **Profil de référence de périphérique**, définissez ce profil comme profil par défaut pour vous connecter à iDRAC ou CMC en sélectionnant l'option **Profil par défaut pour**. Sélectionnez **Aucun** si vous décidez de ne pas définir le profil en tant que profil par défaut.

     REMARQUE : Le profil d'informations d'identification par défaut n'est pas spécifique à la console. Si le profil d'informations d'identification est sélectionné par défaut dans la console actuelle, les autres consoles ne sont pas configurées par défaut pour le type sélectionné.
   - Si vous créez un **Profil de référence Windows**, entrez les détails du domaine dans **Domaine**.

     REMARQUE : Lors de la création du profil d'identification pour l'inscription à la console, si le nom NETBIOS est configuré dans Active Directory (AD), fournissez le nom NETBIOS comme domaine. Si le nom NETBIOS n'est pas configuré dans AD, fournissez le nom de domaine avec les détails du domaine de premier niveau (TLD).

     Par exemple, si le nom de domaine est `mydomain` et que le domaine de premier niveau est `com`, fournissez le nom de domaine dans le profil de référence en tant que : `mydomain.com`
   - Si vous créez des **informations d'identification de serveur proxy**, indiquez l'URL du serveur proxy au format `http://hostname:port` ou `http://IPaddress:port` dans **URL du serveur proxy**.

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

REMARQUE : Lorsque vous créez un profil d'identification de type périphérique dans SCVMM, celui-ci crée un **RunAsAccount** correspondant dont le nom a pour préfixe, **Dell_**. Assurez-vous que l'utilisateur inscrit a accès au **RunAsAccount** correspondant pour des opérations telles que le déploiement du système d'exploitation, qui utilise le profil d'identification du périphérique créé.

Modifier un profil de référence

Tenez compte des éléments suivants avant de modifier un profil de référence :

- Une fois la création terminée, vous ne pouvez pas modifier le type d'un profil de référence. Cependant, vous pouvez modifier d'autres champs.
- Vous ne pouvez pas modifier un profil de référence s'il est en cours d'utilisation.

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

1. Sélectionnez le profil de référence que vous souhaitez modifier, cliquez sur **Modifier** et mettez à jour le profil.
2. Pour enregistrer les modifications apportées, cliquez sur **Enregistrer**.

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

Supprimer un profil d'informations d'identification

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 d'informations d'identification 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.

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

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

Profil d'hyperviseur dans SCVMM

Un profil d'hyperviseur contient un fichier ISO WinPE personnalisé (le fichier ISO WinPE est utilisé pour le déploiement d'hyperviseur), un groupe d'hôtes, et un profil d'hôte issu de SCVMM, ainsi que des pilotes LC pour injection. Seuls les utilisateurs de l'extension de console OMIMSSC pour SCVMM peuvent créer et gérer des profils d'hyperviseur.

Créer un profil d'hyperviseur

Créez un profil d'hyperviseur et utilisez-le pour déployer des hyperviseurs.

- Mettez à jour l'image ISO WinPE et accédez au dossier de partage dans lequel l'image est enregistrée. Pour en savoir plus sur la mise à jour de l'image WinPE, reportez-vous à la section Mise à jour WinPE.

  Mettez à jour l'image ISO WinPE et accédez au dossier de partage dans lequel l'image est enregistrée. Pour en savoir plus sur la mise à jour de l'image WinPE, reportez-vous à la section Mise à jour WinPE du document *OpenManage Integration for Microsoft System Center for Configuration Manager and Virtual Machine Manager User's Guide (Guide unifié de l'utilisateur d'OpenManage Integration for Microsoft System Center pour Configuration Manager et Virtual Machine Manager)*.

- Dans SCVMM, créez un groupe d'hôtes, un profil d'hôte ou un profil d'ordinateur physique. Pour en savoir plus sur la création de groupes d'hôtes dans la console SCVMM, consultez la documentation de Microsoft.

1. Dans OMIMSSC, effectuez l'une des tâches suivantes :
   - Dans le tableau de bord OMIMSSC, cliquez sur **Créer des profils d'hyperviseur**.
   - Dans le volet de navigation de gauche, cliquez sur **Profils et modèles**, **Profil d'hyperviseur**, puis **Créer**.

   L'**Assistant Profil d'hyperviseur** s'affiche.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.
3. Dans **Profil d'hyperviseur**, saisissez le nom et la description du profil, puis cliquez sur **Suivant**.
4. Dans la page **Informations SCVMM**,
   a. Pour **Destination du groupe d'hôtes SCVMM**, sélectionnez un groupe d'hôtes SCVMM dans le menu déroulant pour ajouter l'hôte à ce groupe.
   b. Dans **Profil d'hôte SCVMM/Profil d'ordinateur physique**, sélectionnez un profil d'hôte ou un profil d'ordinateur physique à partir de SCVMM qui inclut des informations de configuration à appliquer sur les serveurs.

      Dans SCVMM, sélectionnez l'une des méthodes de partition de disque suivantes dans un **profil d'ordinateur physique** :
      - Lorsque vous démarrez en mode UEFI, sélectionnez l'option **Table de partition GUID (GPT)**.
      - Lorsque vous démarrez en mode BIOS, sélectionnez l'option **Enregistrement de carte principale (MBR)**.
5. Dans **Source d'image d'amorçage WinPE**, fournissez les informations suivantes, puis cliquez sur **Suivant**.
   a. Pour **Nom du fichier ISO WinPE réseau**, fournissez le chemin d'accès au dossier de partage contenant le nom de fichier WinPE mis à jour. Pour plus d'informations sur la mise à jour du fichier WinPE, reportez-vous à la section Mise à jour WinPE.
   b. Pour **Nom du fichier ISO WinPE réseau**, fournissez le chemin d'accès au dossier de partage contenant le nom de fichier WinPE mis à jour. Pour la mise à jour du fichier WinPE, reportez-vous à la section Mise à jour WinPE du document *OpenManage Integration for Microsoft System Center for Configuration Manager and Virtual Machine Manager User's Guide (Guide de l'utilisateur d'OpenManage Integration for Microsoft System Center pour Configuration Manager et Virtual Machine Manager)*.
   c. Pour **Profil de référence**, sélectionnez les informations d'identification ayant accès au dossier de partage contenant le fichier WinPE.
   d. (Facultatif) Pour créer un profil de référence Windows, cliquez sur **Créer**. Pour en savoir plus sur la création d'un profil de référence, reportez-vous à la section Création d'un profil de référence.
   e. (Facultatif) Pour créer un profil de référence Windows, cliquez sur **Créer**. Pour en savoir plus sur la création d'un profil de référence, reportez-vous à la section Création d'un profil de référence du document *OpenManage Integration for Microsoft System Center for Configuration Manager and Virtual Machine Manager User's Guide (Guide d'e l'utilisateur d'OpenManage Integration for Microsoft System Center pour Configuration Manager et Virtual Machine Manager)*.
6. (Facultatif) Pour activer l'injection de pilotes LC, effectuez les étapes suivantes :

   REMARQUE : Assurez-vous que vous cochez la case **Activer l'injection de pilotes Dell Lifecycle Controller**, car les derniers packs de pilotes de système d'exploitation pour cartes NIC sont disponibles dans les derniers pilotes de système d'exploitation.

   a. Sélectionnez **Activer l'injection de pilotes Dell Lifecycle Controller**.
   b. Sélectionnez le système d'exploitation que vous souhaitez déployer afin que les pilotes correspondants soient sélectionnés.

7. Sous **Résumé**, cliquez sur **Terminer**.

Pour afficher les modifications apportées, actualisez la page **Profil d'hyperviseur**.

Modifier le profil d’hyperviseur

Tenez compte des points suivants lorsque vous modifiez un profil d'hyperviseur :

- Vous pouvez modifier le profil d’hôte, groupe d’hôtes et les pilotes à partir du Lifecycle Controller.
- Vous pouvez modifier le nom ISO WinPE. Cependant, vous ne pouvez pas modifier l’image ISO.

1. Sélectionnez le profil à modifier et cliquez sur **Modifier**.
2. Fournissez les informations requises, puis cliquez sur **Terminer**.

Pour afficher les modifications apportées, actualisez la page **Profil d'hyperviseur**.

Supprimer un profil d’hyperviseur

Sélectionnez le profil d'hyperviseur que vous voulez supprimer et cliquez sur **Supprimer**.

Pour afficher les modifications apportées, actualisez la page **Profil d'hyperviseur**.

12

Détecter des appareils et synchroniser des serveurs avec la console OMIMSSC

La détection est le processus d'ajout des systèmes modulaires pris en charge et des serveurs sans système d'exploitation ou des serveurs hôtes ou des nœuds PowerEdge dans OMIMSSC.

La synchronisation avec la console MSSC est un processus qui consiste à ajouter des serveurs hôtes de la console Microsoft inscrite (MECM ou SCVMM) dans OMIMSSC. Par conséquent, à l'aide de l'un des processus, vous pouvez ajouter des appareils à OMIMSSC. Ce n'est qu'après avoir découvert des appareils que vous pouvez les gérer dans OMIMSSC.

Sujets :

- Découvrir des appareils dans OMIMSSC
- Synchroniser l'extension de console OMIMSSC avec l'instance MECM inscrite
- Résoudre des erreurs de synchronisation
- Afficher le mode System Lockdown

Découvrir des appareils dans OMIMSSC

Découvrez les systèmes modulaires MX7000, les hôtes et les serveurs non attribués dans OMIMSSC. Des informations sur les appareils découverts sont enregistrées dans l'appliance OMIMSSC.

À l'aide de l'une des méthodes suivantes, vous pouvez découvrir les serveurs Dell EMC à l'aide de leur adresse IP iDRAC :

- Découverte de serveurs par découverte automatique
- Découverte de serveurs par découverte manuelle

REMARQUE : L'appareil découvert est marqué comme étant compatible avec le matériel lorsqu'il contient les versions prises en charge du firmware LC, d'iDRAC et du BIOS nécessaires pour fonctionner avec OMIMSSC.. Pour plus d'informations sur les versions prises en charge, voir les notes de mise à jour OpenManage Integration for Microsoft System Center.

Découvrez les systèmes modulaires avec une adresse IP de périphérique en utilisant la méthode de découverte des systèmes modulaires à l'aide de la découverte manuelle.

Découverte d'appareils dans l'extension de console OMIMSSC pour MECM

Découvrez les appareils dans l'extension de console OMIMSSC pour MECM. Une fois un serveur découvert, le serveur est ajouté à un groupe prédéfini dans OMIMSSC, et l'un de ces groupes ou l'une de ces collectes MECM prédéfini(e)s (**Collecte Tous les serveurs Dell Lifecycle Controller** et **Collecte Serveurs Dell importés**) qui sont créé(e)s sous les **Collectes d'appareil**.

Si le serveur découvert n'est pas présent dans MECM, ou s'il n'y a pas de collections ou de groupes prédéfinis dans MECM, les collections prédéfinies sont créées et le serveur identifié est ajouté au groupe respectif.

Découverte d'appareils dans l'extension de console OMIMSSC pour SCVMM

Découvrez les systèmes modulaires, les hôtes Hyper-V et les serveurs non attribués dans l'extension de console OMIMSSC pour SCVMM. Après la découverte, les périphériques sont ajoutés aux groupes de mise à jour prédéfinis respectifs.

Conditions préalables pour la découverte d'appareils

Les systèmes gérés sont les périphériques qui sont gérés à l'aide d'OMIMSSC. La configuration matérielle pour la découverte des serveurs à l'aide des extensions de console OMIMSSC est la suivante :

- OMIMSSC L'extension de console pour MECM prend en charge les modèles de serveurs modulaires, monolithiques et tour sur les serveurs de 12e génération et de générations supérieures.
- OMIMSSC L'extension de console pour SCVMM prend en charge les modèles de serveurs modulaires et monolithiques sur les serveurs de 12e génération et de générations supérieures.
- Pour la configuration de la source et de la destination, utilisez le même type de disques : uniquement des disques SSD (solid-state), SAS ou Série ATA (SATA).
- Pour garantir le succès du clonage RAID du profil matériel des disques du système, utilisez un nombre et une taille identiques ou supérieurs à la taille et au nombre des disques présents dans la source.
- Les disques virtuels RAID en tranches ne sont pas pris en charge.
- L'iDRAC avec LOM partagé n'est pas pris en charge.
- RAID configuré sur un contrôleur externe n'est pas pris en charge.
- Activez l'option Collecter l'inventaire système au redémarrage (CSIOR) dans les systèmes gérés. Pour plus d'informations, consultez la documentation d'iDRAC.

Découvrir des serveurs par découverte automatique

Afin de découvrir automatiquement les serveurs, connectez les serveurs au réseau et mettez les serveurs sous tension. OMIMSSC découvre automatiquement les serveurs non attribués à l'aide de la fonctionnalité d'activation à distance d'iDRAC. OMIMSSC fonctionne comme un serveur de provisionnement et utilise une référence iDRAC pour découvrir automatiquement les serveurs.

1. Dans OMIMSSC, créez un profil d'informations d'identification de type d'appareil en fournissant les informations d'identification iDRAC, puis définissez-le comme profil par défaut pour les serveurs. Pour en savoir plus sur la création d'un profil de référence, reportez-vous à la section Création d'un profil de référence.
2. Désactivez le compte d'administrateur existant dans les paramètres iDRAC dans le périphérique géré.

   REMARQUE : Il est recommandé de disposer d'un compte d'utilisateur invité avec droits d'utilisateur opérateur pour vous connecter à l'iDRAC dans le cas où une découverte automatique échoue et de définir un mot de passe fort.

3. Activez la fonction Auto Discovery dans les paramètres iDRAC du périphérique géré. Pour plus d'informations, consultez la documentation d'iDRAC.
4. Dans les paramètres iDRAC de l'appareil géré, indiquez l'adresse IP de l'appliance OMIMSSC dans **Adresse IP du serveur de provisionnement**, puis redémarrez le serveur.

Découvrir des serveurs par découverte manuelle

Pour découvrir manuellement des serveurs PowerEdge à l'aide d'une adresse IP ou d'une plage d'adresses IP. Pour découvrir des serveurs, indiquez l'adresse IP iDRAC et les informations d'identification de type de périphérique d'un serveur. Lorsque vous découvrez des serveurs à l'aide d'une plage d'adresses IP, spécifiez une plage d'adresses IP (IPv4) au sein d'un sous-réseau en incluant le début et la fin de la plage et les informations d'identification de type de périphérique d'un serveur.

Assurez-vous qu'un profil de référence par défaut est disponible.

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**.
3. Sous **Découvrir**, sélectionnez l'option de votre choix :
   - **Découvrir à l'aide d'une adresse IP** : permet de découvrir un serveur à l'aide d'une adresse IP.
   - **Découvrir à l'aide d'une plage d'adresses IP** : permet de découvrir tous les serveurs à l'aide d'une plage d'adresses IP.
4. Sélectionnez le profil de référence du type de périphérique requis ou cliquez sur **Créer** pour créer un profil de référence pour le type de périphérique.

   Le profil sélectionné est appliqué à tous les serveurs.
5. Dans **Adresse IP iDRAC**, indiquez l'adresse IP du serveur que vous voulez découvrir.
6. Pour l'option **Découvrir à l'aide d'une adresse IP ou d'une plage d'adresses IP**, effectuez l'une des opérations suivantes :

- Dans **Début de la plage d'adresses IP**, puis dans **Fin de la plage d'adresse IP**, spécifiez la plage d'adresses IP que vous voulez inclure. Ceci correspond à la plage de début et de fin.
- Sélectionnez **Activer la plage à exclure** si vous voulez exclure une plage d'adresses IP. Puis dans **Début de la plage d'adresses IP** et **Fin de la plage d'adresse IP**, indiquez la plage que vous voulez exclure.

7. Saisissez un nom de tâche unique, la description de la tâche, puis cliquez sur **Terminer**.

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

   La page **Centre des tâches et des journaux** s'affiche. Développez la tâche de découverte pour afficher l'avancement de la tâche sous l'onglet **Exécution**.

Après avoir découvert un serveur, celui-ci est ajouté à l'onglet **Hôtes**, ou à l'onglet **Non attribués** de la page **Vue Serveur** de la section **Configuration et déploiement**.

- Lors de la découverte d'un serveur sur lequel est déployé un système d'exploitation, et si le serveur est déjà présent dans la console MECM ou SCVMM, le serveur est répertorié en tant que serveur hôte sous l'onglet **Hôtes**.
- Lorsque vous découvrez un serveur PowerEdge qui n'est pas répertorié dans MECM ou SCVMM, le serveur est répertorié en tant que serveur non attribué sous l'onglet **Non attribués** dans toutes les extensions de console OMIMSSC, dans le cas où plusieurs consoles Microsoft sont inscrites dans une seule appliance OMIMSSC.

Après avoir découvert un serveur, le serveur est marqué comme étant compatible avec le matériel lorsqu'il contient les versions prises en charge du firmware LC, d'iDRAC et du BIOS nécessaires pour fonctionner avec OMIMSSC. Pour afficher les versions du firmware des composants du serveur, passez le curseur sur la colonne **Compatibilité matérielle** en regard de la ligne du serveur. Pour plus d'informations sur les versions prises en charge, voir les notes de mise à jour OpenManage Integration for Microsoft System Center.

Une licence est utilisée pour chaque serveur découvert. Le nombre de **nœuds de licence** dans la page **Centre de licence** diminue au fur et à mesure que des serveurs sont découverts.

REMARQUE : Pour utiliser les serveurs découverts dans les versions précédentes de l'appliance OMIMSSC, effectuez une nouvelle découverte de ces serveurs.

REMARQUE : Lorsque vous vous connectez à OMIMSSC en tant qu'administrateur délégué, vous pouvez afficher tous les serveurs hôtes et les serveurs non attribués qui ne sont pas propres à l'utilisateur connecté. Par conséquent, vous ne pouvez pas effectuer d'opérations sur ces serveurs. Assurez-vous que vous disposez des privilèges nécessaires avant d'effectuer des opérations sur ces serveurs.

Découvrir les systèmes modulaires MX7000 à l'aide de la découverte manuelle

Pour découvrir manuellement un système modulaire PowerEdge MX7000 à l'aide d'une adresse IP ou d'une plage d'adresses IP, fournissez l'adresse IP du système modulaire et les informations d'identification de type de périphérique du système modulaire. Lorsque vous découvrez les systèmes modulaires à l'aide d'une plage d'adresses IP, spécifiez une plage IP (IPv4) au sein d'un sous-réseau en incluant la plage de début et de fin et les informations d'identification du type de périphérique des systèmes modulaires.

Assurez-vous que le profil de référence par défaut d'un système modulaire que vous souhaitez découvrir est disponible.

Pour découvrir des systèmes modulaires, procédez comme suit :

1. Dans OMIMSSC, cliquez sur **Configuration et déploiement**, cliquez sur **Vue Systèmes modulaires**, puis cliquez sur **Découvrir**.
2. Cliquez sur **Découvrir**.
3. Sous **Découvrir**, sélectionnez l'option de votre choix :
   - **Découvrir à l'aide d'une adresse IP** : permet de découvrir un système modulaire à l'aide d'une adresse IP.
   - **Découvrir à l'aide d'une plage d'adresses IP** : permet de découvrir tous les systèmes modulaires dans une plage d'adresses IP.
4. Sélectionnez le profil de référence du type de périphérique requis ou cliquez sur **Créer** pour créer un profil de référence pour le type de périphérique.

   Le profil sélectionné est appliqué à tous les serveurs.
5. Dans **Adresse IP**, indiquez l'adresse IP du système modulaire que vous souhaitez découvrir.
6. Pour l'option **Découvrir à l'aide d'une adresse IP ou d'une plage d'adresses IP**, effectuez l'une des opérations suivantes :
   - Dans **Début de la plage d'adresses IP**, puis dans **Fin de la plage d'adresse IP**, spécifiez la plage d'adresses IP que vous voulez inclure. Ceci correspond à la plage de début et de fin.
   - Sélectionnez **Activer la plage à exclure** si vous voulez exclure une plage d'adresses IP. Puis dans **Début de la plage d'adresses IP** et **Fin de la plage d'adresse IP**, indiquez la plage que vous voulez exclure.

7. Dans **Méthodes de découverte des systèmes modulaires**, sélectionnez l'une des options suivantes :
   - **Découverte superficielle** : permet de découvrir les systèmes modulaires et également le nombre de serveurs présents dans le système modulaire.
   - **Découverte détaillée** : permet de découvrir les systèmes modulaires et les périphériques présents dans le système modulaire, tels que les modules d'entrée/sortie (IOM) et les périphériques de stockage.

     REMARQUE : Pour découvrir MX7000 et ses composants de façon détaillée, vérifiez que PowerEdge MX7000 et tous ses composants prennent en charge l'adresse IPV4.
8. Entrez un nom de tâche unique, puis cliquez sur **Terminer**.

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

   Pour afficher la progression de la tâche sous l'onglet **Exécution**, développez la tâche de découverte dans **Centre des tâches et des journaux**.

Synchroniser l'extension de console OMIMSSC avec l'instance MECM inscrite

Vous pouvez effectuer une synchronisation de tous les serveurs (hôtes et non attribués) de la console MECM inscrite pour OMIMSSC. En outre, vous obtenez les dernières informations d'inventaire de firmware sur les serveurs après la synchronisation.

Avant la synchronisation d'OMIMSSC et de la console MECM inscrite, assurez-vous que les conditions suivantes sont réunies :

- Disposez des détails du profil de référence iDRAC par défaut pour les serveurs.
- Mettez à jour la **collecte par défaut Dell** avant de synchroniser OMIMSSC avec MECM. Cependant, si un serveur non attribué est détecté dans MECM, il est ajouté à la **Collecte de serveurs Dell Imported**. Pour ajouter ce serveur dans **Collecte par défaut Dell**, ajoutez l'adresse IP iDRAC du serveur dans la page **OOB**.
- Assurez-vous qu'il n'existe aucune entrée dupliquée de périphérique dans MECM.

Après la synchronisation d'OMIMSSC avec MECM, si l'appareil n'est pas présent dans MECM, la collecte **Tous les serveurs Dell Lifecycle Controller** et la collecte **Importer un serveur Dell** sous **Collectes de périphériques** sont créées et le serveur est ajouté à ce groupe respectif.

Synchroniser l'extension de console OMIMSSC avec l'instance SCVMM inscrite

Vous pouvez effectuer une synchronisation de tous les hôtes Hyper-V, des clusters hôtes Hyper-V, des hôtes Hyper-V modulaires et des serveurs non attribués des consoles SCVMM à l'aide de l'extension de console OMIMSSC pour SCVMM. En outre, vous obtenez les dernières informations d'inventaire de firmware sur les serveurs après la synchronisation.

Tenez compte des points suivants avant la synchronisation d'OMIMSSC avec SCVMM :

- Disposez des détails du profil de référence iDRAC par défaut pour les serveurs.
- Si le contrôleur BMC (Baseboard Management Controller) du serveur hôte n'est pas configuré avec l'adresse IP iDRAC, vous ne pouvez pas synchroniser le serveur hôte avec OMIMSSC. Par conséquent, configurez BMC dans SCVMM (pour plus d'informations, consultez l'article MSDN à l'adresse `technet.microsoft.com`), puis synchronisez OMIMSSC avec SCVMM.
- SCVMM prend en charge de nombreux hôtes dans l'environnement, si bien que la synchronisation est une tâche dont l'exécution est assez longue.

Synchroniser avec la console Microsoft

Pour ajouter des serveurs gérés dans la console Microsoft pour OMIMSSC, effectuez les étapes suivantes :

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**.

Résoudre des erreurs de synchronisation

Les serveurs qui ne sont pas synchronisés avec OMIMSSC sont répertoriés avec leur adresse IP iDRAC et leur nom de l'hôte.

REMARQUE : Tous les serveurs qui ne sont pas synchronisés en raison de problèmes tels que des informations d'identification non valides, ou l'adresse IP iDRAC, ou la connectivité, ou d'autres problèmes ; assurez-vous de résoudre le problème avant d'effectuer la synchronisation.

REMARQUE : Pendant la resynchronisation, les serveurs hôtes qui sont supprimés de l'environnement MSSC inscrit sont déplacés vers l'onglet **Serveurs non attribués** dans les extensions de console OMIMSSC. Si un serveur est mis hors service, supprimez ce serveur de la liste des serveurs non attribués.

Pour resynchroniser les serveurs présentant des problèmes de profil de référence :

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**.
3. Sélectionnez les serveurs à resynchroniser, puis sélectionnez le profil de référence ou, pour créer un profil de référence, cliquez sur **Créer**.
4. Indiquez un nom de tâche et, le cas échéant, sélectionnez l'option **Accéder à la liste des tâches** pour afficher l'état de la tâche automatiquement après sa soumission.
5. Cliquez sur **Terminer** pour soumettre la tâche.

Afficher le mode System Lockdown

Le paramètre du mode System Lockdown est disponible dans l'iDRAC pour la 14e génération de serveurs et les générations supérieures. Lorsque ce paramètre est activé, la configuration du système, notamment les mises à jour du firmware, sont verrouillées. Une fois System Lockdown activé, les utilisateurs ne peuvent plus modifier les paramètres de configuration. Ce paramètre est destiné à protéger le système des modifications non-intentionnelles. Pour effectuer des opérations sur les serveurs gérés, assurez-vous que vous désactivez le paramètre sur leur console iDRAC. Dans la console OMIMSSC, l'état du mode System Lockdown est représenté par une image de verrou avant l'adresse IP iDRAC du serveur.

1. Une image de verrou s'affiche avec l'adresse IP iDRAC des serveurs si le paramètre est activé sur ce système.
2. Une image de verrou désactivé s'affiche avec l'adresse IP iDRAC des serveurs si le paramètre est désactivé sur ce système.

REMARQUE : Avant de lancer les extensions de console OMIMSSC, vérifiez le paramètre de mode System Lockdown de l'iDRAC sur les serveurs gérés.

Pour plus d'informations sur le mode System Lockdown de l'iDRAC, consultez la documentation d'iDRAC disponible à l'adresse `dell.com/support`.

13

Supprimer des appareils de OMIMSSC

S'il n'est plus nécessaire de gérer les serveurs répertoriés, ils peuvent être retirés de la liste des serveurs gérés. Si le serveur est retiré de la gestion dans System Center, il peut être retiré de l'appliance OMIMSSC.

Pour retirer un serveur, procédez comme suit :

Tenez compte des points suivants avant le retrait d'un serveur :

- Une fois que vous avez retiré un serveur, la licence utilisée est libérée.
- Vous pouvez retirer un serveur qui est répertorié dans OMIMSSC en fonction des critères suivants :
  - Un serveur non attribué qui est répertorié dans l'onglet **Serveurs non attribués**.
  - Si vous retirez un serveur hôte qui est provisionné dans une console MECM ou SCVMM inscrite et présent dans OMIMSSC sous l'onglet **Hôtes**, retirez d'abord le serveur dans MECM ou SCVMM, puis retirez-le d'OMIMSSC.

1. Dans la console OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur** :
   - Pour supprimer des serveurs non attribués, sous l'onglet **Serveurs non attribués**, sélectionnez le serveur, puis cliquez sur **Supprimer**.
   - Pour supprimer des serveurs hôtes, sous l'onglet **Serveurs hôtes**, sélectionnez le serveur, puis cliquez sur **Supprimer**.
2. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

Sujets :

- Retirer des systèmes modulaires de OMIMSSC

Retirer des systèmes modulaires de OMIMSSC

Pour supprimer un système modulaire, procédez comme suit :

1. Dans la console OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Systèmes modulaires**.
2. Sélectionnez les systèmes modulaires et cliquez sur **Supprimer**.

14

Vues dans OMIMSSC

Affichez tous les périphériques découverts dans OMIMSSC dans la page **Configuration et déploiement**, ainsi que leurs informations d'inventaire de matériel et de micrologiciel. En outre, vous pouvez afficher toutes les tâches et leur état dans la page **Centre des tâches et des journaux**.

Sujets :

- Vue Serveur
- Vue des systèmes modulaires
- Vue cluster
- Vue Centre de maintenance
- Centre des tâches et des journaux

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**.

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 firmware.

Sous l'onglet **Hôtes**, affichez le nom de l'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 firmware.

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 modèle opérationnel.
- 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 :

1. Dans l'extension de console OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**.
2. Développez **Configuration et déploiement** et cliquez sur **Vue Serveur**.
3. Pour afficher les serveurs sans système d'exploitation, cliquez sur l'onglet **Serveurs non attribués**.
4. 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 MECM 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 MECM, avec un nom de groupe interne. Si vous sélectionnez le nom de groupe interne, tous les hôtes qui sont découverts et gérés dans MECM et OMIMSSC s'affichent.

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 firmware et déployer le système d'exploitation sur ces serveurs, attribuez et déployez des Operational Template. Pour plus d'informations, reportez-vous à la section Operational Template.
- 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 firmware et déployer le système d'exploitation sur ces serveurs, attribuez et déployez des Operational Template. Pour plus d'informations, reportez-vous à la section Attribuer un Operational Template pour les serveurs et Déployer un Operational Template pour les serveurs.
- 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.
- 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 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.

Console iDRAC

Pour lancer la console iDRAC, effectuez les étapes suivantes :

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

Vue des systèmes modulaires

La page **Vue des Systèmes modulaires** répertorie tous les systèmes modulaires qui sont découverts dans OMIMSSC.

Affichez l'adresse IP CMC, le numéro de série, le modèle, la version de firmware, l'état de conformité au modèle du système modulaire d'un Operational Template attribué, le nombre de serveurs, les modules d'entrée/sortie (E/S) et les périphériques de stockage présents sur ce système modulaire. Configurez le matériel et mettez à jour le firmware du système modulaire en déployant le Operational Template.

Vous pouvez effectuer les tâches suivantes sur la page **Vue Systèmes modulaires** :

- Découvrir les systèmes modulaires à l'aide de la découverte manuelle
- Supprimer un système modulaire
- Pour afficher les informations d'inventaire les plus récentes, actualisez la page.
- Attribuer un Operational Template pour un système modulaire
- Déployer un Operational Template pour système modulaire
- Afficher les modules d'E/S
- Lancement des modules d'E/S

Pour afficher le système modulaire découvert dans OMIMSSC :

1. Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Systèmes modulaires**.
   Tous les noms des modèles découverts de systèmes modulaires s'affichent.
2. Pour afficher un système modulaire spécifique, cliquez sur un nom de modèle sous **Vue Systèmes modulaires**.

   Tous les systèmes modulaires de ce modèle sont affichés avec leurs numéros de série.
3. Pour afficher tous les périphériques présents dans ce système modulaire, cliquez sur le numéro de série.

   Tous les serveurs, les modules d'entrée/sortie et les périphériques de stockage ainsi que leurs détails sont affichés.

REMARQUE : Tous les périphériques du système modulaire et leurs informations s'affichent uniquement après la découverte détaillée du système modulaire.

- Par défaut, l'onglet **En cours** s'affiche.

  Tous les serveurs qui sont détectés dans ce système modulaire s'affichent.

- Pour afficher tous les modules d'entrée/sortie présents dans un système modulaire, cliquez sur l'onglet **Modules d'E/S**.
- Pour afficher tous les périphériques de stockage présents dans le système modulaire, cliquez sur l'onglet **Périphériques de stockage**.

Après avoir découvert les systèmes modulaires, prenez en compte les points suivants :

- La colonne **Modèle opérationnel** s'affiche en tant que **Non attribué**, une fois que les systèmes modulaires sont découverts. Afin de mettre à jour le firmware et déployer le système d'exploitation sur ces systèmes modulaires, attribuez et déployez des Operational Template. Pour plus d'informations, reportez-vous à la section Gestion des Operational Template.
- 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 firmware et déployer le système d'exploitation sur ces systèmes modulaires, attribuez et déployez des Operational Template. Pour plus d'informations, reportez-vous à la section Attribuer un Operational Template pour les systèmes modulaires et Déployer un Operational Template pour les systèmes modulaires.
- Affichez le nombre d'entrées/sorties, de périphériques de stockage et de serveurs présents dans les systèmes modulaires après la découverte superficielle. Effectuez une découverte détaillée pour afficher plus de détails sur les composants présents dans un système modulaire.

Console OpenManage Enterprise Modular

Pour lancer la console OpenManage Enterprise Modular, effectuez les étapes suivantes :

1. Dans OMIMSSC, développez **Configuration et déploiement** et cliquez sur **Systèmes modulaires**.
2. Cliquez sur l'**adresse de périphérique** du système modulaire.

Modules d'entrée/sortie

Tous les modules d'entrée/sortie, ainsi que leur adresse IP, leur numéro de série, le type d'entrée/sortie, le modèle, la version de micrologiciel et les informations de logement s'affichent.

Lancez la console des modules d'E/S à partir de la page Modules d'entrée/sortie.

Pour afficher des informations sur les modules d'entrée/sortie, effectuez les étapes suivantes :

1. Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Systèmes modulaires**. Développez la **vue Systèmes modulaires** et cliquez sur le numéro de série.

   Tous les numéros de série de ce modèle s'affichent.
2. Cliquez sur un modèle de système modulaire pour développer les périphériques répertoriés sous celui-ci. Pour afficher un système modulaire, cliquez sur le numéro de série.
3. Pour afficher le module d'entrée/sortie, cliquez sur l'onglet **Modules d'E/S**.

Console de modules d'entrée/sortie

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

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.

Vue cluster

La page **Vue Cluster** répertorie tous les clusters découverts dans OMIMSSC. Affichez le nom de domaine complet (FQDN) du cluster, son numéro de série et le nombre de serveurs présents dans ce cluster. Vous pouvez également créer un commutateur logique pour les clusters HCI de serveurs Windows, puis créer des clusters d'espaces de stockage direct à l'aide du Operational Template prédéfini.

Vous pouvez exécuter les tâches suivantes sur la page **Vue Cluster** :

- Création d'un commutateur logique (uniquement pour les utilisateurs SCVMM 2016 et 2019)
- Création de clusters HCI de serveurs Windows (uniquement pour les utilisateurs SCVMM 2016 et 2019)
- Lancement de la console iDRAC
- Pour afficher les clusters découverts les plus récents, actualisez la page.

Pour afficher les groupes de cluster découverts dans OMIMSSC :

1. Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Cluster**.
   Tous les différents types de clusters sont regroupés et répertoriés.
2. Pour afficher des informations sur certains types de clusters, développez le type de cluster.
   Tous les clusters de ce type sont répertoriés dans le volet de gauche.
3. Pour afficher les serveurs présents dans un cluster, cliquez sur un nom de cluster.

Vue Centre de maintenance

La page **Centre de maintenance** répertorie tous les appareils découverts dans les groupes et les ressources qui sont requis pour la maintenance des appareils dans OMIMSSC. Pour afficher les groupes de clusters HCI de serveurs Windows dans la page **Centre de maintenance**, assurez-vous que vous avez choisi **Tous les groupes de mise à jour** dans le menu déroulant **Groupe de mise à jour**. Affichez l'inventaire de firmware du périphérique, gérez les périphériques en conservant leur firmware 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.

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 HTTPS prédéfinie. Par conséquent, vous devez télécharger le dernier catalogue afin d'afficher le dernier rapport de comparaison. Pour télécharger le dernier catalogue, modifiez et enregistrez les sources de mise à jour HTTPS.

REMARQUE : La version de base d'un composant spécifique d'un appareil est marquée comme non disponible si la mise à jour n'est pas présente dans le catalogue source de mise à jour sélectionné.

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 firmware
- Mettre à niveau et rétrograder les versions de firmware 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** :

Dans OMIMSSC, cliquez sur **Centre de maintenance**.
La page **Centre de maintenance** s'affiche.

Centre des tâches et des journaux

Affichez des informations sur les tâches lancées dans OMIMSSC ainsi que l'état de progression des tâches et les sous-tâches correspondantes. En outre, vous pouvez filtrer et afficher les tâches d'une catégorie de tâche spécifique.

Vous pouvez afficher les tâches qui sont lancées à partir d'OMIMSSC, dans le portail d'administration OMIMSSC et l'extension de console OMIMSSC.

- OMIMSSC Le portail d'administration affiche les tâches qui sont lancées à partir de toutes les consoles OMIMSSC et par tous les utilisateurs
- OMIMSSC Console : affiche les tâches spécifiques à un utilisateur et à une console

Les noms des tâches sont générés par le système ou fournis par les utilisateurs, et les sous-tâches sont nommées d'après l'adresse IP ou le nom d'hôte des systèmes gérés. Développez la sous-tâche pour afficher les journaux d'activité pour cette tâche. Les tâches sont classées dans quatre groupes :

- **En cours** : affiche toutes les tâches qui sont actuellement en cours d'exécution.
- **Historique** : affiche toutes les tâches exécutées par le passé et leur état de tâche.
- **Planifiée** : affiche toutes les tâches planifiées à une date et une heure futures. Vous pouvez également annuler ces tâches planifiées.
- **Journaux génériques** : affiche les messages de journal courants spécifiques à l'appliance OMIMSSC qui ne sont pas propres à une tâche ou à d'autres activités. Chaque tâche s'affiche avec un nom d'utilisateur et un nom de domaine complet de console basé sur l'emplacement à partir duquel elle a été lancée.
  - **Messages de journal d'appliance** : affiche tous les messages de journal spécifiques de l'appliance OMIMSSC, comme le redémarrage de l'appliance OMIMSSC. Vous pouvez afficher cette catégorie de messages uniquement à partir du portail d'administration OMIMSSC.
  - **Messages de journal génériques** : affiche tous les messages de journal courants pour les différentes catégories de tâches répertoriées dans les onglets **En cours**, **Historique** et **Planifiée**. Ces journaux sont propres à une console et un utilisateur.

    Par exemple, si une tâche de mise à jour de firmware est en cours pour un groupe de serveurs, l'onglet affiche les messages de journal liés à la création du référentiel SUU (Server Update Utility) pour cette tâche.

Les différents états d'une tâche qui est définie dans OMIMSSC sont les suivants :

- **Annulée** : la tâche est annulée manuellement, ou après le redémarrage de l'appliance OMIMSSC.
- **Réussie** : la tâche s'est terminée avec succès.
- **Échouée** : la tâche a échoué.
- **En cours** : la tâche est en cours d'exécution.
- **Planifiée** : la tâche a été planifiée pour une date et une heure ultérieures.

  REMARQUE : Si plusieurs tâches sont soumises en même temps pour le même périphérique, elles échouent. Par conséquent, assurez-vous que vous planifiez des tâches pour le même périphérique à des heures différentes.
- **En attente** : la tâche est mise dans une file d'attente.
- **Planification récurrente** : la tâche est planifiée à intervalles réguliers.

1. Dans OMIMSSC, cliquez sur **Centre des tâches et des journaux**.
2. Pour afficher une catégorie spécifique de tâches, telles que **Planifiée**, **Historique**, ou **Générique**, cliquez sur l'onglet souhaité.

   Développez une tâche pour afficher tous les périphériques inclus dans cette tâche. Développez davantage pour afficher les messages de journal pour cette tâche.

   REMARQUE : Tous les messages de journalisation génériques liés aux tâches sont répertoriés dans l'onglet **Générique** et non l'onglet **En cours** ou **Historique**.
3. (Facultatif) Appliquez des filtres pour afficher différents groupes de tâches et l'état de tâche dans la colonne **État**.

15

Gérer des Operational Template

Les Operational Template comportent la configuration complète des périphériques et sont utilisés pour déployer le système d'exploitation et mettre à jour le firmware pour les serveurs PowerEdge et les systèmes modulaires dans l'environnement Microsoft.

Le Operational Template réplique le matériel et le firmware d'un serveur de référence sur de nombreux autres serveurs lors du provisionnement pour les systèmes d'exploitation. Il contient les composants de firmware, de matériel et de système d'exploitation dont l'attribut est défini sur la valeur actuelle du serveur de référence. Ces valeurs peuvent être modifiées avant d'appliquer ce modèle à tous les périphériques. En outre, vous pouvez vérifier l'état de conformité par rapport à un Operational Template attribué et afficher le rapport de conformité dans une page de récapitulatif.

Seuls les composants qui sont disponibles dans le serveur de référence sont récupérés et affichés dynamiquement en tant que composants du Operational Template. Par exemple, si le serveur ne dispose pas de composant FC, celui-ci ne s'affiche pas dans le Operational Template.

Pour plus d'informations sur le serveur de référence et le système modulaire de référence, reportez-vous à la section À propos de la configuration de serveur de référence et À propos de la configuration des systèmes modulaires de référence.

Le tableau suivant décrit les composants répertoriés dans le Operational Template et leurs fonctions d'affichage et de déploiement :

Tableau 9. Fonctionnalité du Operational Template

Composant	Déployer la configuration	mise à jour de firmware	Afficher la configuration	État de conformité au modèle opérationnel
BIOS	Oui	Oui	Oui	Oui
iDRAC	Oui	Oui	Oui	Oui
Carte NIC/CNA	Oui	Oui	Oui	Oui
RAID	Oui	Oui	Oui	Oui
FC	Oui	Oui	Oui	Oui
Windows	Oui	—	Non	—
RHEL	Oui	—	Non	—
ESXI	Oui	—	Non	—
Module de gestion	Oui	Oui	Oui	Oui

Sujets :

- Operational Template prédéfinis
- À propos de la configuration de serveurs de référence
- À propos de la configuration du système modulaire de référence
- Créer un Operational Template à partir de serveurs de référence
- Créer un Operational Template à partir de systèmes modulaires de référence
- Créer des clusters à l'aide d'un Operational Template
- Afficher le Operational Template
- Modifier un Operational Template
- Configurer des valeurs spécifiques au système (valeurs de pool) à l'aide d'un modèle opérationnel sur plusieurs serveurs
- Attribuer un Operational Template et exécuter la conformité au modèle opérationnel pour les serveurs
- Déploiement de modèles opérationnels
- Annuler l'attribution d'un Operational Template
- Supprimer un Operational Template

Operational Template prédéfinis

Les modèles prédéfinis contiennent toutes les configurations qui sont requises pour créer des clusters HCI de serveurs Windows ou Windows Server Software-Defined (SMDD). OMIMSSC prend en charge la création de clusters sur les modèles de nœud Ready de clusters HCI de serveurs Windows AX-6515, AX-740XD, AX-640, RN740XD, RN740XD2 et RN640, ainsi que leurs adaptateurs réseau.

Tableau 10. Liste des Operational Template prédéfinis

Nom du Operational Template	Description
AX-6515_QLogic	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-6515
AX-6515_Mellanox	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-6515
AX-740xd_RN740xd_QLogic	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-740xd et RN740xd
AX-740xd_RN740xd_Mellanox	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-740xd et RN740xd
AX-640_RN640_Mellanox	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-640 et RN640
AX-640_RN640_QLogic	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles AX-640 et RN640
RN440_QLogic	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles RN440
RN740xd2_Mellanox	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles RN740xd2
RN740xd2_QLogic	Ce modèle opérationnel est destiné aux solutions HCI de Dell EMC pour Microsoft Windows Server pour les modèles RN740xd2

Tenez compte des éléments suivants avant le déploiement d'un Operational Template :

- Les modèles prédéfinis sont disponibles uniquement pour des systèmes de gestion exécutant SCVMM 2016 et 2019.
- Le modèle de clusters HCI de serveurs Windows prédéfini montre la carte NIC dans le logement 1. Toutefois, lors du déploiement du Operational Template, la configuration de carte NIC est appliquée au logement de droite. S'il y a plusieurs cartes NIC sur le périphérique, toutes les cartes NIC sont configurées avec la même configuration qui est spécifiée dans le Operational Template.

À propos de la configuration de serveurs de référence

Une configuration de serveur avec une séquence d'amorçage préférée, le BIOS, les paramètres RAID, la configuration matérielle, les attributs de mise à jour de micrologiciel, et les paramètres de système d'exploitation qui conviennent parfaitement pour une entreprise sont appelés la configuration de serveur de référence.

Découvrez un serveur de référence et capturez les paramètres du serveur de référence dans un Operational Template et répliquez-le sur différents serveurs avec la même configuration matérielle.

À propos de la configuration du système modulaire de référence

Une configuration de système modulaire avec une configuration réseau préférée, un compte d'utilisateur, la sécurité et les alertes, qui convient parfaitement pour une entreprise est appelée une configuration de système modulaire de référence ou un châssis de référence.

Découvrez un système modulaire de référence et capturez les paramètres du système modulaire de référence dans un Operational Template, et répliquez-le sur différents systèmes modulaires des mêmes modèles.

Créer un Operational Template à partir de serveurs de référence

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 MECM :
  - Créez une séquence de tâches. Pour plus d'informations, reportez-vous à la section Création d'une séquence de tâches.
  - Créez une séquence de tâches. Pour plus d'informations, reportez-vous au document Guide unifié de l'utilisateur d'OpenManage Integration for Microsoft System Center.
  - Pour le déploiement d'un système d'exploitation 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.

Vous pouvez créer un Operational Template en capturant la configuration du serveur de référence. Après la capture de la configuration, vous pouvez enregistrer directement le modèle ou modifier les attributs pour la source de mise à jour, la configuration matérielle et le composant Windows, selon vos besoins. Maintenant, vous pouvez enregistrer le modèle, qui peut être utilisé sur des serveurs PowerEdge homogènes.

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 **Profils** > **Modèle 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 de firmware
   - 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**.

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 modèle opérationnel 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.

   REMARQUE : Le modèle opérationnel ne capture pas le mot de passe lors de la récupération à partir du serveur de référence. Assurez-vous de définir les valeurs de mot de passe pour les attributs sélectionnés avant le déploiement.

   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 MECM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour MECM.
   - 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.

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

Recommandation : si votre serveur de référence iDRAC dispose d'une licence d'entreprise, et si vous voyez des attributs Télémétrie/SCEP, assurez-vous de désélectionner ces attributs, car ils sont uniquement pris en charge avec la licence datacenter.

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

Lors de la création ou de la modification d'un Operational Template pour le serveur, effectuez les étapes suivantes pour un composant Windows :

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.

   Pour en savoir plus sur la séquence de tâches, reportez-vous au document Guide unifié de l'utilisateur d'OpenManage Integration for Microsoft System Center.

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

REMARQUE : Le déploiement du système d'exploitation de Windows Server 2016 sur les plates-formes AMD ne prend pas en charge x2apic. Assurez-vous de désactiver les paramètres du BIOS x2apic et du processeur logique avant d'installer le système d'exploitation.

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

Lors de la création ou de la modification d'un Operational Template pour le serveur, effectuez les étapes suivantes pour un composant Windows :

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

REMARQUE : **Nom de l'hôte** et **Carte NIC de gestion de serveur** sont toujours des valeurs de pool. Pour la carte NIC de gestion de serveur, renseignez l'adresse MAC du port réseau par lequel vous souhaitez que le système d'exploitation communique avec SCVMM.

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**

REMARQUE : Le déploiement du système d'exploitation de Windows Server 2016 sur les plates-formes AMD ne prend pas en charge x2apic. Assurez-vous de désactiver les paramètres du BIOS x2apic et du processeur logique avant d'installer le système d'exploitation.

Composant non-Windows pour les extensions de console OMIMSSC

Lors de la création ou de la modification d'un Operational Template pour le serveur, effectuez les étapes suivantes pour un composant non-Windows :

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 de l'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.

Créer un Operational Template à partir de systèmes modulaires de référence

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.

Vous pouvez créer un Operational Template en capturant la configuration des systèmes modulaires de référence. Après la capture de la configuration, vous pouvez enregistrer directement le modèle ou modifier les attributs pour la source de mise à jour et la configuration matérielle, selon vos besoins. Maintenant, vous pouvez enregistrer le modèle, qui peut être utilisé pour configurer d'autres systèmes modulaires de même modèle.

REMARQUE : Si vous voulez configurer des utilisateurs Active Directory (AD) sur d'autres périphériques MX7000, assurez-vous de créer un Operational Template à partir d'un système modulaire MX7000 où tous les utilisateurs AD sont configurés.

REMARQUE : Les mots de passe du compte d'utilisateur ne sont pas capturés dans un modèle opérationnel à partir du système modulaire de référence pour des raisons de sécurité. Modifiez le Operational Template pour ajouter un nouveau compte d'utilisateur et un nouveau mot de passe, puis appliquez le Operational Template sur les systèmes modulaires gérés. Sinon, vous pouvez appliquer le Operational Template sans apporter aucune modification aux comptes d'utilisateur, et les mêmes mots de passe qui sont utilisés dans le système modulaire de référence sont appliqués sur le système modulaire géré.

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 **Profils** > **Modèle 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. Dans **Composants de périphérique**, cliquez sur un composant pour afficher les attributs disponibles et leurs valeurs.
   Les composants sont les suivants :
   - mise à jour de firmware
   - Module de gestion intégré

     REMARQUE : Assurez-vous que l'attribut **Serveur Web** est sélectionné. Si ce composant n'est pas activé, les systèmes modulaires Mx7000 ne sont pas accessibles via OMIMSSC après le déploiement du Operational Template.

     REMARQUE : Pour **Configuration SNMP** et **Configuration de Syslog**, assurez-vous que vous sélectionnez les quatre configurations disponibles dans chaque attribut pour les appliquer sur les périphériques gérés.
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.
7. Pour enregistrer le profil, cliquez sur **Terminer**.

Créer des clusters à l'aide d'un Operational Template

Ce chapitre fournit des informations sur la création des clusters HCI de serveurs Windows.

Créer un commutateur logique pour les clusters HCI de serveurs Windows

Créez un commutateur logique à partir d'OMIMSSC dans la console SCVMM.

REMARQUE : L'adresse IP qui est saisie dans la section **Configuration pour la gestion** remplace l'adresse IP qui est saisie dans un composant de système d'exploitation de Operational Template prédéfini de cluster HCI de serveurs Windows.

1. Dans OMIMSSC, développez **Configuration et déploiement**, cliquez sur **Vue Cluster**, puis cliquez sur **Créer un commutateur logique** pour le cluster.
2. Cliquez sur **Créer un commutateur logique pour le cluster**.
3. Indiquez un nom pour le commutateur logique, et sélectionnez le groupe d'hôtes présent dans SCVMM pour associer le commutateur logique.
4. Indiquez les informations requises, puis cliquez sur **Créer**.
   a. Dans **Configuration pour la gestion**, indiquez le **sous-réseau**, l'**adresse IP de début**, l'**adresse IP de fin**, le **serveur DNS**, le **suffixe DNS** et la **passerelle**.

      REMARQUE : Indiquez les informations de sous-réseau au format CIDR (Classless InterDomain Routing).

b. Dans **Configuration pour le stockage**, fournissez les détails du **LAN virtuel**, du **sous-réseau**, de l'**adresse IP de début** et de l'**adresse IP de fin**.

5. 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.

Pour vérifier que le commutateur logique est créé avec succès, vérifiez la présence du nom du commutateur logique dans le menu déroulant qui figure dans la page **Créer un cluster**.

Pour afficher les détails du commutateur logique, effectuez les étapes suivantes dans SCVMM :

1. Pour afficher le nom du commutateur logique, cliquez sur **Structure** et, dans **Mise en réseau**, cliquez sur **Commutateurs logiques**.
2. Pour afficher le profil du port de données sortantes du commutateur logique (UPP), cliquez sur **Structure** et, dans **Mise en réseau**, cliquez sur **Commutateurs logiques**.
3. Pour afficher le réseau du commutateur logique, cliquez sur **Structure** et, dans **Mise en réseau**, cliquez sur **Réseaux logiques**.

Créer des clusters HCI de serveurs Windows

- Assurez-vous que vous créez un réseau logique à l'aide de la fonctionnalité **Créer un commutateur logique** pour les clusters.
- Assurez-vous que vous utilisez SCVMM 2016 ou 2019.
- Assurez-vous que vous utilisez Windows Server 2016 ou 2019 Datacenter Edition.
- Assurez-vous que les configurations des serveurs gérés correspondent aux exigences en matière de versions de pilote et de firmware de solution HCI de serveurs Windows. Pour plus d'informations, consultez la documentation *Dell EMC Matrice de support des nœuds Ready HCI de serveurs Windows PowerEdge R740XD, R740XD2 et R640.*
- Pour plus d'informations sur l'infrastructure et la gestion des clusters HCI de serveurs Windows, consultez la documentation *Guide de déploiement des nœuds Ready HCI de serveurs Dell EMC Microsoft Windows pour une infrastructure hyperconvergée évolutive avec les nœuds Ready HCI de serveurs Windows RN740xd, RN740XD2, RN640, RN440 et AX6515.*

Tenez compte des points suivants avant de créer des clusters HCI de serveurs Windows :

- Vous pouvez créer un cluster HCI de serveurs Windows 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 clusters HCI de serveurs Windows. Mais, après avoir appliqué le modèle opérationnel prédéfini de cluster HCI de serveur Windows, 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 de l'utilisateur d'iDRAC disponible à l'adresse dell.com/support.
- Si l'option d'intercommunication système d'exploitation à iDRAC est activée, vous devez vous assurer que l'adresse IP est configurée dans le modèle opérationnel.

Pour créer un cluster HCI de serveurs Windows, effectuez les étapes suivantes :

1. Dans OMIMSSC, cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Cluster**.
   La page **Vue Cluster** s'affiche.
2. Pour créer un cluster, cliquez sur **Créer**.
   La page **Créer un cluster** s'affiche.
3. Indiquez un nom de cluster et sélectionnez le Operational Template prédéfini pour la création des clusters HCI de serveurs Windows.
   - 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**.
4. Pour ajouter des serveurs à un cluster, sélectionnez les serveurs en utilisant la case à cocher.
5. 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. Pour plus d'informations, reportez-vous à la section Remplir le fichier CSV de la valeur du pool
6. (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.
7. 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.

   REMARQUE : Lorsque le déploiement du système d'exploitation est en cours, vous verrez un profil d'hôte ou des profils d'ordinateur physique se cloner dans SCVMM (nom ajouté au GUID de serveur). Ces profils sont utilisés pour chaque OSD du serveur.

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.

Pour plus d'informations, consultez la section Créer un profil d'ordinateur physique dans la section des conditions préalables de la documentation Microsoft sur le provisionnement d'un hôte ou d'un cluster Hyper-V à partir d'ordinateurs sans système d'exploitation.

REMARQUE : Il est recommandé que le témoin de cluster soit configuré pour un cluster à deux nœuds. La configuration des témoins de cluster permet de maintenir un cluster ou un QuoRam de stockage lorsqu'un nœud ou une communication réseau échoue. Pour plus d'informations, consultez le Guide de déploiement de clusters HCI de serveurs Windows.

Afficher le Operational Template

Pour afficher les Operational Template créés :

Dans la console OMIMSSC, cliquez sur **Profils et modèles**, puis cliquez sur **Modèle opérationnel**. Tous les modèles qui sont créés sont répertoriés ici.

Modifier un Operational Template

Vous pouvez modifier la source de mise à jour, les configurations matérielles et le système d'exploitation d'un modèle opérationnel.

Tenez compte des points suivants avant la modification d'un Operational Template :

- Les valeurs de certains attributs dépendent des valeurs d'autres attributs. Lorsque vous modifiez des valeurs d'attribut manuellement, assurez-vous que vous modifiez également les attributs interdépendants. Si les valeurs interdépendantes ne sont pas modifiées comme il convient, l'application des configurations matérielles peut échouer.
- La création d'un Operational Template récupère toutes les configurations matérielles à partir du serveur de référence spécifié, qui peut contenir les attributs spécifiques au système. Par exemple, adresse IPv4 statique, numéro d'inventaire. Pour configurer les attributs spécifiques au système, reportez-vous à la section Configuration des valeurs spécifiques au système à l'aide d'un Operational Template
- Les attributs du Operational Template sont attribués aux valeurs actuelles du serveur de référence. Les Operational Template répertorient également les autres valeurs applicables aux attributs.
- Pour modifier des Operational Template prédéfinis et des Operational Template créés personnalisés, procédez comme suit :

REMARQUE : (Pour les utilisateurs et les serveurs SCVMM uniquement) Tous les attributs obligatoires (Les attributs obligatoires qui sont capturés dans le modèle opérationnel sont les attributs recommandés par Dell EMC pour le cluster HCI de serveurs Windows) requis pour les clusters HCI de serveurs Windows sont des attributs en lecture seule dans le modèle de cluster HCI de serveurs Windows prédéfini. Cependant, vous pouvez modifier le nom du modèle, des composants de système d'exploitation et des attributs de configuration matérielle facultatifs.

1. Sélectionnez le modèle à modifier et cliquez sur **Modifier**.
   La page Operational Template s'affiche.
2. (Facultatif) Saisissez le nom et une description pour le modèle, puis cliquez sur **Suivant**.
3. Pour afficher les attributs disponibles et leurs valeurs dans **Composants de périphérique**, cliquez sur un composant.
4. Modifiez les valeurs des attributs disponibles.

   REMARQUE : Cochez la case en regard de chaque composant étant donné que seules les configurations du composant sélectionné sont appliquées sur le système géré lorsque le Operational Template est appliqué.

   REMARQUE : Lorsque vous modifiez un Operational Template, seuls quelques attributs de composant AHCI (Advanced Host Controller Interface) qui sont en lecture seule sont répertoriés comme modifiables. Cependant, lorsque ces attributs en lecture seule ont été définis et que le Operational Template a été déployé, aucune modification n'est apportée au périphérique.

   - Pour les systèmes modulaires MX7000 :
     - Les configurations sont appliquées uniquement si tous les attributs d'un groupe sont sélectionnés. Par conséquent, assurez-vous que vous sélectionnez tous les attributs dans un groupe, même si vous souhaitez modifier un seul attribut dans le groupe.
     - Pour ajouter un nouvel utilisateur au moyen d'un Operational Template, sélectionnez tous les attributs des utilisateurs existants qui ont été exportés lors de la capture du Operational Template, sélectionnez les groupes d'utilisateurs récemment ajoutés et enregistrez le Operational Template.
     - Pour indiquer les valeurs de fuseau horaire, reportez-vous à l'Annexe.
5. Pour le composant de système d'exploitation, effectuez l'une des tâches suivantes en fonction de vos besoins :

- Pour le déploiement de système d'exploitation Windows dans MECM, reportez-vous à la section Composant Windows pour l'extension de console OMIMSSC pour MECM.
- 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. Pour enregistrer le profil, cliquez sur **Terminer**.

Recommandation : lorsque vous modifiez un modèle opérationnel, seuls quelques attributs de composant AHCI (Advanced Host Controller Interface) qui sont en lecture seule sont répertoriés comme modifiables. Cependant, lorsque ces attributs en lecture seule ont été définis et que le modèle opérationnel a été déployé, aucune modification n'est apportée à l'appareil.

Configurer des valeurs spécifiques au système (valeurs de pool) à l'aide d'un modèle opérationnel sur plusieurs serveurs

OMIMSSC sera récupéré en tant que configuration de l'appareil. Attributs propres à un système (l'adresse IPv4 statique pour l'iDRAC par exemple) s'afficheront sous la forme d'une valeur de pool dans le modèle opérationnel. Les attributs de valeur de pool qui sont des attributs dépendants sont sélectionnés par défaut, ainsi que d'autres attributs.

1. Sélectionnez le modèle à modifier et cliquez sur Modifier.
   La page Operational Template s'affiche.
2. (Facultatif) Saisissez le nom et une description pour le modèle, puis cliquez sur **Suivant**.
3. Pour afficher les attributs disponibles et leurs valeurs dans Composants de périphérique, cliquez sur un composant.
4. Développez le **Groupe d'attributs**. Si la valeur de l'attribut est une **valeur de pool**, l'attribut est identifié comme attribut spécifique du système. Pour plus d'informations sur le groupe d'attributs et les composants de tous les attributs spécifiques du système, reportez-vous au tableau 13 dans la section Attributs spécifiques du système dans le modèle opérationnel.
5. Si vous ne souhaitez pas appliquer ces attributs spécifiques au système, identifiez-les (mentionnés à l'étape 4) et désélectionnez-les lors de la modification d'un modèle opérationnel.
6. La saisie de ces attributs spécifiques au système peut être effectuée pour plusieurs serveurs via un fichier .CSV à l'aide de l'option **Exporter les attributs de pool** lors du déploiement d'un modèle opérationnel. Reportez-vous à la section Déploiement d'un modèle opérationnel sur des serveurs.

REMARQUE : Pour plus d'informations sur le remplissage d'un fichier CSV de valeur, reportez-vous à la section Remplissage d'un fichier CSV de valeur de pool et attributs spécifiques du système dans le modèle opérationnel

Recommandation : lors de la création d'un modèle opérationnel, si vous activez et désactivez la case à cocher d'un attribut dépendant qui a une valeur de pool, vous ne pouvez pas enregistrer le modèle opérationnel et le message d'erreur suivant s'affiche : `Select at least one attribute, under the selected components, before creating the Operational Template.` Par conséquent, sélectionnez un attribut dépendant qui a une valeur de pool ou le même attribut dépendant et enregistrez le modèle opérationnel. Créez ensuite un nouveau modèle opérationnel.

Attribuer un Operational Template et exécuter la conformité au modèle opérationnel pour les serveurs

Attribuez un Operational Template à un serveur, et exécutez la conformité au Operational Template. Uniquement après l'attribution d'un Operational Template à un serveur, vous pouvez afficher son état de conformité au Operational Template. Vous pouvez comparer une configuration de serveur avec un Operational Template en attribuant le modèle à un serveur. Une fois que vous avez attribué un Operational Template, la tâche de conformité s'exécute et l'état du Operational Template s'affiche une fois l'opération terminée.

Pour attribuer un Operational Template, effectuez les étapes suivantes :

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. Sélectionnez le modèle dans le menu déroulant Operational Template, saisissez 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 l'appareil.

   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.

Attribuer un Operational Template pour des systèmes modulaires

Attribuez un Operational Template à un système modulaire et exécutez la conformité au Operational Template. Cette opération compare la configuration d'un système modulaire et un Operational Template en attribuant le modèle sélectionné à un système modulaire. Après avoir attribué un Operational Template, la tâche de conformité s'exécute et l'état de conformité s'affiche à la fin de l'exécution.

Pour attribuer un Operational Template pour des systèmes modulaires, effectuez les étapes suivantes :

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 un** Operational Template s'affiche.

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

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

3. Sélectionnez le modèle dans le menu déroulant Operational Template, saisissez 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 : L'état de conformité au Operational Template exclut toute modification qui a été apportée aux attributs utilisateur.

   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 l'appareil.

   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

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.

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 *Paramètres du navigateur* du document Guide de l'utilisateur de *Dell EMC OpenManage Integration for Microsoft System Center version 7.2.1 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 le suivant `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.

Déployer un Operational Template sur des serveurs

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.

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 ou Windows 2019 sur les serveurs de 12^{e} génération.

REMARQUE : Le déploiement d'un modèle opérationnel sur des serveurs serait bloqué si le mode de verrouillage est activé sur les serveurs.

REMARQUE : Lorsque vous déployez Windows sur un périphérique basé sur l'UEFI, formatez le disque dur qui comprend la partition Windows en utilisant un système de fichiers de partitionnement GPT (tableau de partition GUID). Pour plus d'informations, consultez la section Partitions de disque dur basées sur UEFIGPT de la documentation Microsoft.

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

   REMARQUE : Si vous voyez l'invite *`Press any key to boot to CD \ DVD .....`* lors du démarrage à partir du support de séquence de tâches. Pour plus d'informations sur la suppression de l'invite et le démarrage automatique sur le support de séquence de tâches, consultez la section Installation de Windows sur un ordinateur EFI de la documentation Microsoft.

2. 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.
3. 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**.

   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.
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 le suivant `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.

Déployer un Operational Template pour système modulaire

Vous pouvez configurer les composants du système modulaire et mettre à jour les versions de firmware du système modulaire en déployant le Operational Template attribué.

REMARQUE : Dans une gestion multi-châssis (MCM), si le châssis principal est configuré avec **Propagation aux châssis membres**, la configuration et la mise à jour du châssis principal et des châssis membres d'OMIMSSC écrasent les modifications effectuées via la propagation.

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. (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.
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 le suivant `attribute-value-pool.csv`

   REMARQUE : Assurez-vous que vous sélectionnez un fichier CSV qui a tous les attributs corrects et que l'adresse IP CMC ou les informations d'identification CMC ne changent pas en raison du modèle, étant donné que la tâche n'est pas suivie par OMIMSSC après la modification de l'adresse IP CMC ou des informations d'identification CMC.

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

   REMARQUE : Il n'y a aucun attribut de valeur de pool spécifique du système pris en charge pour le système modulaire. Par conséquent, il n'y a aucune valeur de pool à exporter.

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

Annuler l'attribution d'un Operational Template

1. Dans OMIMSSC, effectuez l'une des tâches suivantes :
   - Cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Serveur**.
   - Cliquez sur **Configuration et déploiement**, puis cliquez sur **Vue Système modulaire**.

   Sélectionnez les périphériques 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 périphériques, puis cliquez sur **Attribuer un Operational Template et exécuter la conformité**.
   La page **Attribuer un Operational Template et exécuter la conformité** s'affiche.
3. Sélectionnez **Annuler l'attribution** dans le menu déroulant **Operational Template**, puis cliquez sur **Attribuer**.
   L'attribution du Operational Template aux périphériques sélectionnés est annulée.

Supprimer un Operational Template

Pour supprimer un Operational Template, effectuez les étapes suivantes :

Avant de supprimer un Operational Template, assurez-vous que :

- Le Operational Template sélectionné n'est associé à aucun serveur ou aucun système modulaire. S'il est associé à un périphérique, annulez l'attribution du modèle, puis supprimez le modèle.
- Aucune tâche associée au Operational Template n'est en cours d'exécution.
- Vous n'avez pas sélectionné un Operational Template prédéfini, car vous ne pouvez pas supprimer un modèle prédéfini.
- Les étapes de suppression sont les mêmes quel que soit le type de Operational Template.

Sélectionnez les modèles à supprimer, puis cliquez sur **Supprimer**. Pour confirmer, cliquez sur **Oui**.

16

Déployer le système d'exploitation à l'aide d'OMIMSSC

Avant de déployer un système d'exploitation Windows sur les serveurs gérés, mettez à jour l'image WinPE, créez une séquence de tâches, le fichier de support d'amorçage LC et le ISO amorçable de support de séquence de tâches. Les étapes peuvent varier pour les utilisateurs des consoles MECM et SCVMM. Reportez-vous à la section ci-dessous pour plus d'informations. Pour le déploiement de système d'exploitation non-Windows, n'oubliez pas les points mentionnés dans la section Préparation du déploiement de système d'exploitation non-Windows.

Sujets :

- À propos de la mise à jour de l'image WinPE
- Préparer le déploiement de système d'exploitation sur la console MECM
- Préparer un déploiement de système d'exploitation non-Windows

À propos de la mise à jour 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 MECM 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 du pack de pilotes Dell EMC OpenManage. Assurez-vous que les packs de pilotes correspondant au système d'exploitation sont installés dans Lifecycle Controller.

1. Pour créer une image WinPE contenant tous les pilotes requis, mettez à jour l'image à l'aide du pack de pilotes Dell EMC OpenManage.
2. 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.

Fournir un fichier WIM pour MECM

Copiez le fichier `boot.wim` à l'emplacement `\\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`

Fournir un fichier WIM pour SCVMM

L'image de base WINPE est requise pour l'injection des pilotes Dell critiques de démarrage à partir du pack de pilotes OpenManage Server. Cette image est générée par l'installation du serveur PXE dans SCVMM. Pour plus d'informations sur l'installation du serveur PXE dans SCVMM, reportez-vous à la documentation de Microsoft.

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

   Pour plus d'informations sur l'ajout du rôle WDS sur un serveur, et l'ajout d'un serveur PXE à SCVMM, reportez-vous à la section Provisionnement d'un Hyper-V hôte ou d'un cluster à partir d'ordinateurs sans système d'exploitation de la documentation Microsoft.
2. Copiez le fichier `boot.wim` depuis le serveur PXE présent à l'emplacement `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`

Les serveurs WDS et PXE ne sont nécessaires que pour générer l'image boot.in de type WinPE et ne doivent pas être utilisés dans les scénarios de déploiement.

Extraire des pilotes à partir du pack de pilotes du serveur OpenManage

Le DVD du pack de pilotes du serveur Dell EMC OpenManage est un package publié publiquement par Dell EMC qui regroupe les pilotes du système d'exploitation pour toutes les plates-formes. À partir de la version actuelle, OMIMSC devrait aider les administrateurs à créer l'image WinPE en utilisant le pack de pilotes OpenManage uniquement.

`To download OpenManage driver pack, launch` **https://www.dell.com/support**`/ -> Search for the keyword` **Dell EMC OpenMange server Driver Pack DVD** `and download the corresponding openManage server driver pack based on the supported platforms.`

1. Montez l'image ISO en tant que disque sur une machine Windows locale.
   REMARQUE : Assurez-vous d'utiliser la version WinPE appropriée.
2. Utilisez l'invite de commande et accédez au chemin `<MountedDrive>:\server_assistant\driver_tool\bin`.
3. Exécuter la commande `make_driver_dir.exe -i <MountedDrive> -d <ExtractedWinPEPath> -o <filter option> --extract`

   Supposons que le disque monté se trouve à l'emplacement F et que le chemin de sortie extrait est `C:\om_server_diver_pack`, utilisez les exemples suivants pour accéder aux pilotes extraits pour toutes les plates-formes prises en charge :

   a. Pour extraire des pilotes Windows 2016 et 2019 pour toutes les plates-formes prises en charge, utilisez `make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE10 --extract`
   b. Pour extraire des pilotes Windows 2012 R2 pour toutes les plates-formes prises en charge, utilisez `make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE5 --extract`

REMARQUE : Une fois l'extraction terminée, supprimez les pilotes du répertoire suivant `<ExtractedWinPEPath>\WINPE5\chipset\9D99N\SBDrv`.

Mettre à jour une image WinPE

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

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 DVD pilote OM**, pour **Chemin des pilotes OM**, indiquez l'emplacement des pilotes de Dell EMC OpenManage.
   Par exemple : `\\Shareip\sharefolder\<extracted share folder>`
4. Sous **Fichier de sortie**, pour **ISO ou Nom de fichier WIM**, saisissez un nom pour le fichier ainsi que le chemin de fichier partagé où l'image WinPE est générée.

   Entrez l'un des types de fichiers de sortie :

   - Fichier WIM pour MECM
   - 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**.
   - Fichier WIM pour MECM
   - Fichier ISO pour SCVMM
   - Fichier WIM pour MECM
   - Fichier ISO pour SCVMM

   Un nom de tâche unique est attribué à chaque mise à jour WinPE.
7. Cliquez sur **Mettre à jour**.
   L'image WinPE avec le nom du fichier fourni à l'étape précédente est créée sous \\Shareip\sharefolder\WIM.

Préparer le déploiement de système d'exploitation sur la console MECM

Avant de déployer un système d'exploitation sur les serveurs gérés découverts à l'aide d'OMIMSSC dans la console MECM, créez une séquence de tâches spécifique de Dell EMC ou personnalisée, un fichier de support de démarrage LC et le fichier ISO amorçable de support de séquence de tâches.

Séquence de tâches-MECM

Une séquence de tâches est une série de commandes qui est utilisée pour déployer le système d'exploitation sur le système géré à l'aide de MECM.

Avant de créer un Operational Template, Dell EMC vous recommande d'effectuer les conditions préalables suivantes.

1. Dans Configuration Manager, assurez-vous que le système est découvert et présent sous **Équipements et conformité** > **Collections de périphériques** > **Tous les serveurs Dell Lifecycle Controller**. Pour plus d'informations, reportez-vous à la section Découvrir les serveurs.
2. Installez la version du BIOS la plus récente sur le système.
3. Installez la version la plus récente de Lifecycle Controller sur le système.
4. Installez la version la plus récente du firmware d'iDRAC sur le système.

REMARQUE : lancez toujours la console Configuration Manager avec des privilèges d'administrateur.

Types de séquences de tâches

Vous pouvez créer une séquence de tâches de deux façons :

- En créant une séquence de tâches propre à Dell à l'aide du modèle de déploiement d'OMIMSSC.
- En créant une séquence de tâches personnalisée.

La séquence de tâches passe à la prochaine étape de la séquence de tâches indépendamment de la réussite ou de l'échec de la commande.

Créer une séquence de tâches propre à Dell

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

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. Faites un clic droit sur **Séquences de tâches**, puis cliquez sur **OMIMSSC Déploiement de serveur** > **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 **Fermer** dans la zone de message de confirmation qui s'affiche.

Créer 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** > **Séquence 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.

Modifier une séquence de tâches

REMARQUE : Lorsque de la modification d'une séquence de tâches sur MECM 2016 et 2019, les messages missing objects references n'indiquent pas le package **Setup windows and ConfigMgr**. Ajoutez le package, puis enregistrer la séquence de tâches.

1. Lancez Configuration Manager.
   L'écran Configuration Manager s'affiche.
2. Dans le volet de gauche, sélectionnez **Bibliothèque logicielle** > **Systèmes d'exploitation** > **Séquence de tâches**.
3. Cliquez avec le bouton droit sur la séquence de tâches que vous souhaitez modifier, puis cliquez sur **Modifier**.
   La fenêtre **Éditeur de séquence de tâches** s'affiche.
4. Cliquez sur **Ajouter** > **Dell Deployment** > **Appliquer les pilotes à partir du Dell Lifecycle Controller.**
   L'action personnalisée de votre déploiement de serveur Dell est chargée. Vous pouvez désormais apporter des modifications à la séquence de tâches.

   REMARQUE : Lorsque vous modifiez une séquence de tâches pour la première fois, le message d'erreur, **Setup Windows and Configuration Manager**, s'affiche. Pour corriger l'erreur, créez et sélectionnez le package de mise à niveau du client Configuration Manager. Pour plus d'informations sur la création de packages, consultez la documentation Configuration Manager sur **technet.microsoft.com**.

   REMARQUE : Lors de la modification d'une séquence de tâches sur MECM 2016 et 2019, les messages missing objects references n'indiquent pas le package Setup windows and ConfigMgr. Par conséquent, vous devez ajouter le package, puis enregistrer la séquence de tâches.

Définir un emplacement de partage par défaut pour le support de démarrage Lifecycle Controller

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

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**.

Créer 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 Standalone Media (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 serveur PowerEdge**.

   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.

Préparer un déploiement de système d'exploitation non-Windows

Assurez-vous que vous vous souvenez des points suivants pour le déploiement des systèmes d'exploitation non-Windows sur des systèmes gérés :

- Le fichier ISO est disponible dans un partage NFS (Network File System) ou CIFS (Common Internet File System) avec un accès en lecture et en écriture.
- Confirmez que le lecteur virtuel est disponible sur le système géré.
- Après le déploiement du système d'exploitation ESXi, le serveur est déplacé vers la collecte **Managed Lifecycle Controller (ESXi)** dans MECM.
- Après le déploiement de n'importe quel type de système d'exploitation non-Windows, les serveurs sont déplacés vers **Groupe de mise à jour d'hôte non Windows par défaut**.
- Il est conseillé de connecter la carte réseau au port réseau du serveur sur lequel le système d'exploitation est déployé.

17

Provisionner les appareils avec OMIMSSC

Ce chapitre contient des informations de haut niveau concernant la découverte, le déploiement de système d'exploitation, la création de clusters et la maintenance des périphériques Dell EMC à l'aide d'OMIMSSC.

Sujets :

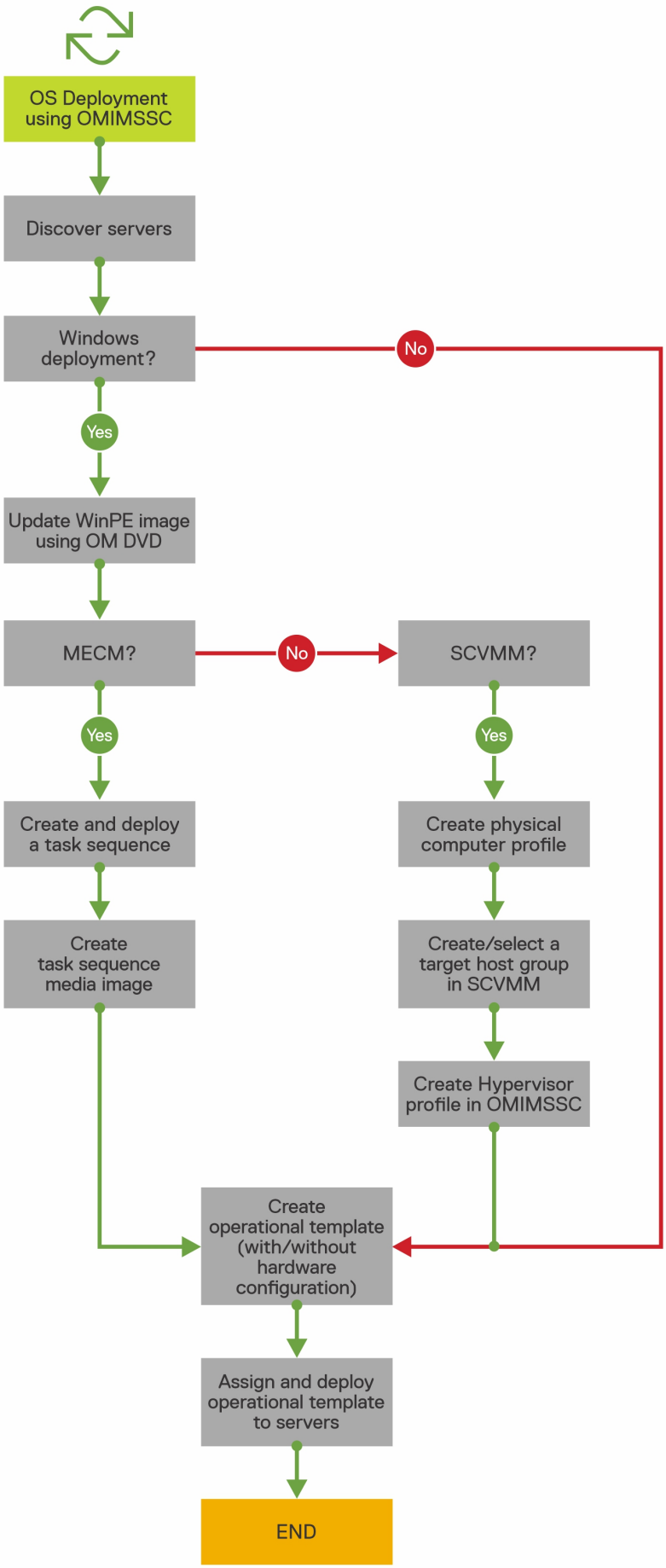
- Workflow pour les scénarios de déploiement
- Créer des clusters HCI de serveurs Windows à l'aide de Operational Template prédéfinis
- Mettre à jour le firmware des serveurs et des appareils MX7000
- Configurer des composants remplacés
- Exporter et importer des profils de serveur

Workflow pour les scénarios de déploiement

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

REMARQUE : Assurez-vous de mettre à niveau les versions de firmware de l'appareil vers les dernières versions disponibles sur `downloads.dell.com` avant le déploiement du système d'exploitation.

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


OS Deployment using OMIMSSC
Discover servers
Windows deployment?
No
Yes
Update WinPE image using OM DVD
MECM?
No
SCVMM?
Yes
Yes
Create and deploy a task sequence
Create physical computer profile
Create task sequence media image
Create/select a target host group in SCVMM
Create Hypervisor profile in OMIMSSC
Create operational template (with/without hardware configuration)
Assign and deploy operational template to servers
END

Déployer le système d'exploitation Windows à l'aide de l'extension de console OMIMSSC pour MECM

Pour déployer le système d'exploitation Windows via la console MECM à l'aide d'OMIMSSC, effectuez les étapes suivantes :

REMARQUE : Avant de déployer le système d'exploitation sur un serveur hôte, assurez-vous que l'état **Client** du serveur est **Aucun** dans MECM.

1. Téléchargez la dernière version du pack de pilotes du serveur Dell EMC OpenManage et créez une image WIM de démarrage Windows Preinstallation Environment (WinPE). Pour plus d'informations, reportez-vous à la section Mise à jour WinPE.
2. Importez cette image WIN dans la console MECM et créez une image d'amorçage dans MECM. Pour plus d'informations, consultez la *documentation de Microsoft*.
3. Créez une séquence de tâches dans MECM. Pour plus d'informations, reportez-vous à la section Création d'une séquence de tâches.
4. Créez une image de support de séquence de tâches dans MECM. Pour plus d'informations, consultez la *documentation de Microsoft*.

   REMARQUE : Pour configurer un déploiement de système d'exploitation sans assistance lors de la création d'un support de séquence de tâches, dans **Sélectionner le type de supports**, cochez la case **Autoriser le déploiement du système d'exploitation sans assistance**.

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 modèle opérationnel 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.

Déployer l'hyperviseur à l'aide de l'extension de console OMIMSSC pour SCVMM

Les différents scénarios pour le déploiement d'hyperviseur sont les suivants :

Tableau 11. Scénarios de déploiement d'hyperviseur

État	Action
Si vous avez besoin de la version la plus récente des pilotes d'usine.	Lors de la création d'un profil d'hyperviseur, activez l'injection de pilotes LC (Lifecycle Controller).
Si vous souhaitez conserver la configuration matérielle existante.	Lors de la création du Operational Template, désactivez la case pour tous les composants qui ne nécessitent aucune modification.

Pour déployer un hyperviseur via la console SCVMM à l'aide d'OMIMSSC, effectuez les étapes suivantes :

1. Téléchargez la dernière version du pack de pilotes Dell EMC OpenManage et créez une image ISO de démarrage Windows Preinstallation Environment (WinPE). Pour plus d'informations, reportez-vous à la section Mise à jour WinPE.
2. Créez un profil d'ordinateur physique et un groupe d'hôtes dans SCVMM. Pour plus d'informations, consultez la documentation de SCVMM.
3. Créez un profil d'hyperviseur dans l'extension de console OMIMSSC pour SCVMM. Pour plus d'informations, reportez-vous à la section Création d'un profil d'hyperviseur.
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 modèle opérationnel 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 modèle opérationnel 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 modèle opérationnel 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.

Redéployer un système d'exploitation Windows avec OMIMSSC

Pour redéployer un système d'exploitation Windows sur un serveur à l'aide de l'extension de console OMIMSSC pour MECM ou de l'extension de console OMIMSSC sur SCVMM, effectuez les étapes suivantes :

1. Supprimez le serveur de la console Microsoft. Pour plus d'informations, reportez-vous à la documentation Windows.
2. Redécouvrez le serveur ou synchronisez OMIMSSC avec la console Microsoft inscrite. Le serveur est ajouté en tant que serveur non attribué dans OMIMSSC. Pour plus d'informations sur la découverte, reportez-vous à la section Découverte de serveurs par découverte manuelle. Pour plus d'informations sur la synchronisation, reportez-vous à la section Synchronisation avec la console Microsoft inscrite.
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 modèle opérationnel 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.

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

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.

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 modèle opérationnel 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 collecte **Managed Lifecycle Controller Lifecycle Controller (ESXi)** dans MECM.

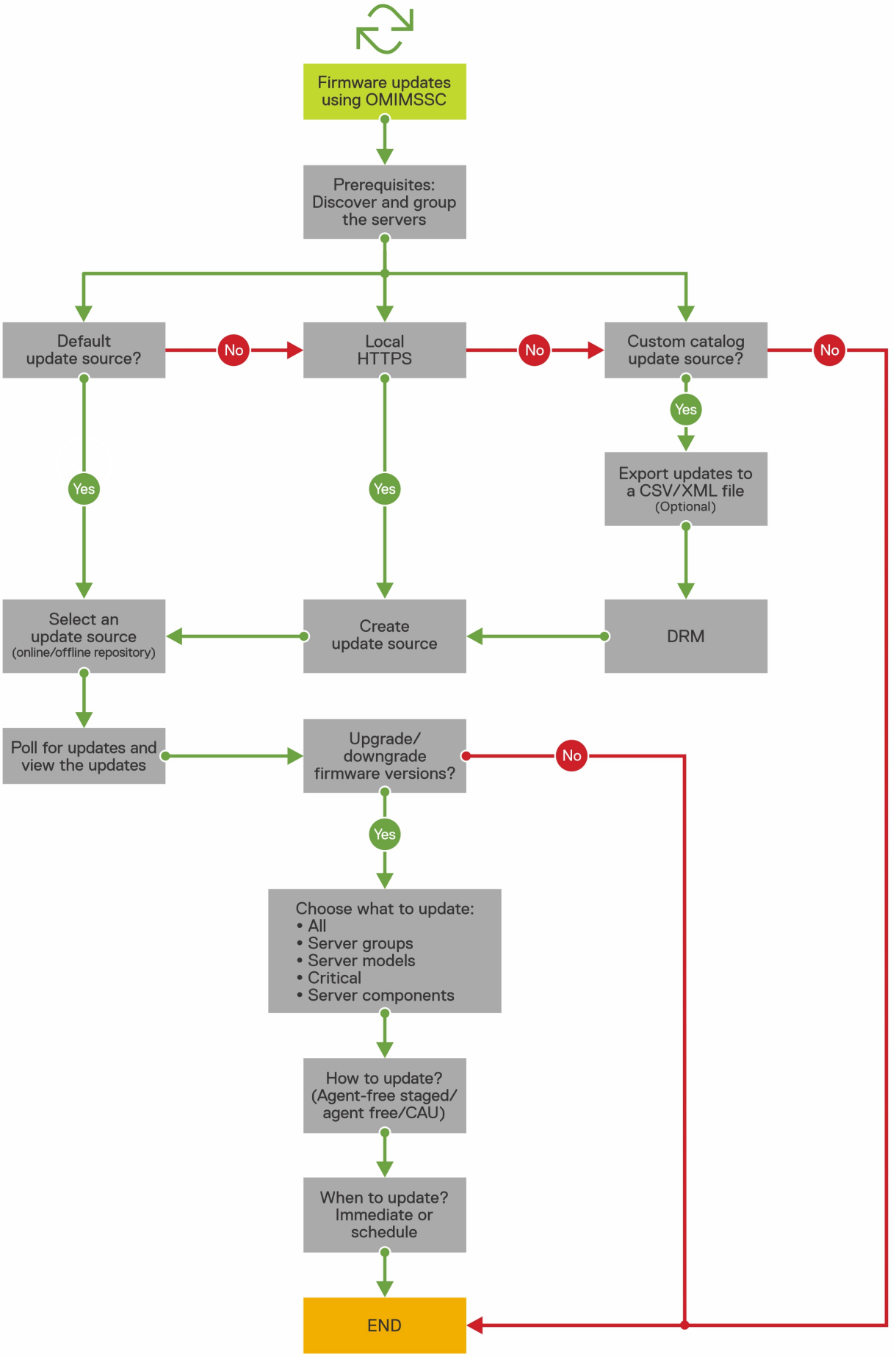
Créer des clusters HCI de serveurs Windows à l'aide de Operational Template prédéfinis

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 HCI de serveurs Windows. Pour plus d'informations, reportez-vous à la section Création de clusters HCI de serveurs Windows.

Mettre à jour le firmware des serveurs et des appareils MX7000

Voici une représentation graphique du workflow de mise à jour de firmware : mise à jour.


Firmware updates using OMIMSSC
Prerequisites: Discover and group the servers
Default update source?
No
Local HTTPS
No
Custom catalog update source?
No
Yes
Export updates to a CSV/XML file (Optional)
Yes
Yes
Select an update source (online/offline repository)
Create update source
DRM
Poll for updates and view the updates
Upgrade/ downgrade firmware versions?
No
Yes
Choose what to update:
• All
• Server groups
• Server models
• Critical
• Server components
How to update? (Agent-free staged/ agent free/CAU)
When to update? Immediate or schedule
END

Vous pouvez mettre à jour les appareils sélectionnés en utilisant des sources en ligne ou des sources locales (DRM/HTTPS)

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 HCI de serveurs Windows, sélectionnez une source de mise à jour prédéfinie spécifique pour les clusters HCI de serveurs Windows. 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 firmware à l'aide de la méthode d'exécution de mise à jour.

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

Configurer des composants remplacés

Pour que la version de firmware ou les paramètres de configuration du composant remplacé correspondent à ceux de l'ancien composant, reportez-vous à la section Application des paramètres de firmware et de configuration.

Exporter et importer des profils de serveur

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

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.

La fonctionnalité d'exportation et d'importation de profil de serveur n'est pas prise en charge sur

- les serveurs avec l'iDRAC version 4.40.00.00 et versions ultérieures.
- Serveurs PowerEdge basés sur l'iDRAC 9

  Utilisez le modèle opérationnel si vous envisagez de sauvegarder la configuration matérielle du serveur, le firmware et la ligne de base du système d'exploitation.

18

Mettre à jour des firmwares OMIMSSC

Maintenez les appareils Dell EMC à jour en effectuant une mise à niveau vers la dernière version de firmware afin de bénéficier de la sécurité, des corrections et des améliorations, à l'aide d'OMIMSSC. Mettez à jour le firmware des périphériques à l'aide des référentiels de mise à jour Dell EMC.

La mise à jour de firmware est prise en charge uniquement sur des périphériques compatibles avec le matériel. Pour utiliser les fonctionnalités disponibles dans OMIMSSC sur les appareils gérés, ceux-ci doivent disposer des versions minimales requises de firmware d'iDRAC, de Lifecycle Controller (LC) et du BIOS. Les périphériques dotés des versions de firmware requises sont compatibles avec le matériel.

Sujets :

- À propos des groupes de mise à jour
- À propos des sources de mise à jour
- Intégration avec Dell EMC Repository Manager (DRM)
- Définir la fréquence d'interrogation
- Afficher et actualiser l'inventaire d'appareils
- Appliquer les filtres
- Mettre à niveau et rétrograder les versions de firmware à l'aide de la méthode d'exécution de mise à jour

À propos des groupes de mise à jour

Les groupes de mise à jour sont un groupe de périphériques qui requièrent la même gestion de la mise à jour. Il existe deux types de groupes de mise à jour qui sont pris en charge dans OMIMSSC :

- Groupes de mise à jour prédéfinis : vous ne pouvez pas créer, modifier ou supprimer manuellement les groupes de mise à jour prédéfinis.
- Groupes de mise à jour personnalisée : vous pouvez créer, modifier et supprimer des périphériques de ces groupes.

REMARQUE : Tous les groupes de serveurs qui existent dans SCVMM sont répertoriés dans OMIMSSC. Cependant, la liste des serveurs dans OMIMSSC n'est pas propre à l'utilisateur. Par conséquent, assurez-vous que vous êtes en mesure d'effectuer des opérations sur ces périphériques.

Groupes de mise à jour prédéfinis

Après la découverte d'un périphérique, le périphérique découvert est ajouté à l'un des groupes prédéfinis suivants.

- **Groupes d'hôtes par défaut** : ce groupe est constitué de serveurs qui sont déployés avec le système d'exploitation Windows ou synchronisés avec une console Microsoft inscrite.
- **Groupes non attribués par défaut** : ce groupe est constitué de serveurs découverts non attribués ou sans système d'exploitation.
- **Groupes d'hôtes non-Windows par défaut** : ce groupe est constitué de serveurs qui sont déployés avec des systèmes d'exploitation non-Windows.
- **Groupes de mise à jour de châssis** : ce groupe est constitué de châssis et de serveurs modulaires ou de systèmes modulaires. Les serveurs de 12e génération et de générations supérieures sont découverts, ainsi que leurs informations de châssis. Par défaut, un groupe est créé avec le format de nom suivant : `Chassis-Service-tag-of-Chassis-Group`. Par exemple, `Chassis-GJDC4BS-Group`. Si un serveur modulaire est supprimé d'un groupe de mise à jour de cluster, le serveur est ajouté au groupe de mise à jour de châssis, avec ses informations CMC. Même s'il n'y a aucun serveur modulaire dans le groupe de mise à jour de châssis correspondant, étant donné que tous les serveurs modulaires dans le châssis sont dans un groupe de mise à jour de cluster, le groupe de mise à jour de cluster continue d'exister, mais affiche uniquement les informations CMC.
- **Groupes de mise à jour de cluster** : ce groupe est constitué de **clusters de basculement Windows Server**. Si un serveur modulaire de 12e génération et de génération supérieure fait partie d'un cluster, les informations CMC sont également ajoutées à l'inventaire dans la page **Centre de maintenance**.

Groupes de mise à jour personnalisée

Créez un groupe de mise à jour personnalisée de type **Groupes de mise à jour générique** en ajoutant les périphériques découverts dans des groupes qui nécessitent une gestion similaire. Cependant, vous pouvez ajouter un périphérique à un groupe de mise à jour personnalisée uniquement à partir de **groupes de mise à jour non attribués par défaut** et de **groupes de mise à jour d'hôte par défaut**. Pour ajouter les serveurs dans le groupe de mise à jour personnalisée, recherchez le périphérique requis à l'aide de son numéro de série. Après que vous avez ajouté un périphérique dans un groupe de mise à jour personnalisée, le périphérique est supprimé du groupe de mise à jour prédéfini et est disponible, uniquement dans le groupe de mise à jour personnalisée.

Afficher des groupes de mise à jour

Pour afficher les groupes de mise à jour :

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**.
   Tous les groupes personnalisés créés s'affichent avec leur nom, leur type de groupe et le nombre de serveurs qu'ils contiennent.

Créer des groupes de 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 firmware** 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**.

   REMARQUE : Le groupe de mise à jour personnalisé est spécifique à System Center ; est visible pour les autres utilisateurs du même System Center.

Modifier des groupes de mise à jour personnalisée

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 :
  1. Retirer le serveur d'un groupe de mise à jour personnalisé existant. Il est alors automatiquement ajouté au groupe de mise à jour prédéfini.
  2. Modifier le groupe personnalisé pour y ajouter le serveur, puis rechercher ce dernier en utilisant le numéro de service.

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.

Retirer des groupes de mise à jour personnalisée

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 appareil 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, l'appareil est supprimé du groupe de mise à jour personnalisée et déplacé dans le groupe prédéfini approprié.

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 firmware des appareils 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 firmware à l'aide des sources de mise à jour suivantes :

- **Référentiel DRM** : référentiel hors ligne. Exportez les informations d'inventaire des appareils 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 appareils appropriés, et exécutez une mise à jour sur les appareils. Pour en savoir plus sur DRM, consultez les documents relatifs à Dell Repository Manager à l'adresse `dell.com\support`.
- **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 HTTPS. Dell EMC prépare un référentiel tous les deux mois et publie les mises à jour suivantes via les catalogues PDK :
  - BIOS et firmware 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 firmware sont téléchargées et appliquées sur les périphériques gérés. Par conséquent, les versions de firmware peuvent varier entre le périphérique de référence et le périphérique déployé.
- **Inventaire de firmware 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 firmware 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 appareils 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 la source de mise à jour prédéfinie qui est disponible après une nouvelle installation ou une mise à niveau. **CATALOGUE DELL EMC ENTERPRISE** 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 HCI de serveurs Windows

OMIMSSC prend en charge la mise à jour des clusters HCI de serveurs Windows 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 firmware les plus récentes et

recommandées des composants pour les clusters HCI de serveurs Windows. Elles sont répertoriées uniquement sur la page **Centre de maintenance**.

CATALOGUE DE MISES À JOUR POUR LES SOLUTIONS HCI MICROSOFT est une source de mise à jour prédéfinie par défaut de type HTTPS, qui fait partie de **CATALOGUE DELL EMC ENTERPRISE**.

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 firmware les plus récentes et recommandées des composants pour les systèmes modulaires. Elles sont répertoriées uniquement sur la page **Centre de maintenance**.

CATALOGUE DE SOLUTIONS DELL EMC MX est une source de mise à jour prédéfinie par défaut de type HTTPS, qui fait partie de **CATALOGUE DELL EMC ENTERPRISE**.

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.

Configurer un HTTPS local

Pour configurer le HTTPS local :

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 de l'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`.

Afficher 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.

Créer une source de mise à jour

- Selon le type de la source de mise à jour, assurez-vous qu'un profil de référence Windows 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.

1. Dans la console OMIMSSC, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.
2. Cliquez sur **Source de mise à jour**.
3. 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.
4. Sélectionnez l'un des types suivants de sources de mise à jour à partir du menu déroulant **Type de source** :
   - 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 firmware 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.

5. Dans **Emplacement**, indiquez l'URL de la source de mise à jour d'une source HTTPS et l'emplacement partagé Windows pour DRM.
6. Pour accéder à la source de mise à jour, sélectionnez le profil de référence requis dans **Informations d'identification**.
7. Dans **Informations d'identification de proxy**, sélectionnez les informations d'identification de proxy appropriées si un proxy est requis pour accéder à la source HTTPS.
8. (Facultatif) Pour désigner la source de mise à jour créée comme source de mise à jour par défaut, sélectionnez **Désigner comme source par défaut**.
9. 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.

Modifier la source de mise à jour

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

- Pour modifier la source de mise à jour **CATALOGUE DE MISES À JOUR POUR LES SOLUTIONS HCI MICROSOFT**, modifiez la source de mise à jour prédéfinie respective, puis enregistrez les modifications. Cette mise à jour est reflétée dans la source de mise à jour **CATALOGUE DE MISES À JOUR POUR LES SOLUTIONS HCI MICROSOFT**.
- 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.

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

Modifier la source de mise à jour

Tenez compte des points suivants avant la suppression d'une source de mise à jour :

- Vous ne pouvez pas supprimer une source de mise à jour prédéfinie.
- Vous ne pouvez pas supprimer une source de mise à jour si elle est utilisée dans une tâche en cours ou une tâche planifiée.
- Vous ne pouvez pas supprimer une source de mise à jour s'il s'agit d'une source de mise à jour par défaut.

Sélectionnez la source de mise à jour à supprimer, puis cliquez sur **Supprimer**.

Intégration avec Dell EMC Repository Manager (DRM)

OMIMSSC OMIMSSC est intégré à DRM pour créer des sources de mise à jour personnalisée dans OMIMSSC. L'intégration est disponible à partir de la version 2.2 de DRM et versions supérieures. Fournissez les informations de périphérique découvert à partir de l'appliance OMIMSSC dans DRM, et à l'aide des informations d'inventaire disponibles, vous pouvez créer un référentiel personnalisé dans DRM et définir ce dernier en tant que source de mise à jour dans OMIMSSC pour effectuer les mises à jour du firmware et créer des clusters sur les périphériques gérés. Pour plus d'informations sur la création d'un référentiel dans DRM, consultez les documents Dell EMC Repository Manager disponibles à l'adresse `Dell.com/support/home`.

Intégration de DRM à OMIMSSC

Cette section décrit le processus de création d'un référentiel avec intégration.

REMARQUE : Pour préparer les mises à jour requises, tenez compte des facteurs tels que le test dans un environnement de test, les mises à jour de sécurité, les recommandations pour les applications et les conseils de Dell EMC.

REMARQUE : Pour afficher les informations d'inventaire les plus récentes sur les périphériques découverts, après la mise à niveau d'OMIMSSC, réintégrez DRM à l'appliance OMIMSSC.

1. Sur la page d'accueil, cliquez sur **Ajouter un nouveau référentiel**. La fenêtre **Ajouter un nouveau référentiel** s'affiche.
2. Sélectionnez l'onglet **Intégration**, saisissez le **Nom du référentiel** et la **Description**.
3. Sélectionnez **Personnalisé**, puis cliquez sur **Choisir les systèmes** pour sélectionner un système spécifique.
4. Dans le menu déroulant **Type d'intégration**, sélectionnez le produit que vous souhaitez intégrer. En fonction du produit sélectionné, les options suivantes s'affichent. Les options disponibles sont les suivantes :
   a. Dell OpenManage Integration pour Microsoft System Center : renseignez le nom de l'hôte ou l'adresse IP, le nom d'utilisateur, le mot de passe et le serveur proxy.

      REMARQUE : Assurez-vous que le mot de passe ne contient pas de caractères spéciaux, tels que `<, >, ',", &.`

   b. Dell Console Integration : renseignez l'URL https://<IP>/genericconsolerepository, l'administrateur comme nom d'utilisateur, le mot de passe et le serveur proxy.

   REMARQUE : L'option Dell Console Integration s'applique aux consoles qui ont intégré les services Web tels que OpenManage Integration pour System Center Virtual Machine Manager (SCVMM).
5. Après avoir sélectionné l'option requise, cliquez sur **Connecter**. Le système et le modèle disponibles s'affichent dans la section **Type d'intégration**.
6. Sélectionnez **Ajouter** pour créer le référentiel. Le référentiel s'affiche dans le tableau de bord des référentiels disponible sur la page d'accueil.

   REMARQUE : Lorsque vous sélectionnez les types de lot ou les formats DUP, assurez-vous de sélectionner Windows 64 bits et un système d'exploitation indépendant, si le châssis Dell PowerEdge MX7000 fait partie de l'inventaire dans OMIMSSC.

Après l'intégration de DRM à OMIMSSC, consultez la section *Obtenir un catalogue de firmwares pour les solutions HCI pour les nœuds Ready Microsoft Windows Server utilisant Dell Repository Manager* dans le document *Guide des opérations de Dell EMC Microsoft HCI Solutions pour les nœuds Ready Microsoft Windows Server pour la gestion et la surveillance du cycle de vie des nœuds Ready* à l'adresse `dell.com/support`

Définir la fréquence d'interrogation

Configurez l'interrogation et les notifications afin de recevoir des alertes lorsqu'un nouveau fichier de catalogue est disponible dans la source de mise à jour qui est sélectionnée par défaut. L'appliance OMIMSSC enregistre un cache local de la source de mise à jour. La couleur de la cloche de notification change et devient orange lorsqu'un nouveau fichier de catalogue est disponible dans la source de mise à jour. Pour remplacer le catalogue mis en cache localement disponible dans l'appliance OMIMSSC, cliquez sur l'icône de cloche. Après avoir remplacé l'ancien fichier de catalogue par le dernier fichier de catalogue, la couleur de la cloche passe au vert.

Pour définir la fréquence d'interrogation :

1. Dans OMIMSSC, cliquez sur **Centre de maintenance**, puis cliquez sur **Interrogation et notification**.
2. Cliquez sur **Interrogation et notification**.
3. Sélectionnez la fréquence d'interrogation :
   - **Jamais** : cette option est sélectionnée par défaut. Sélectionnez cette option pour ne jamais recevoir les mises à jour.
   - **Une fois par semaine** : sélectionnez cette option pour recevoir des mises à jour sur les nouveaux catalogues disponibles dans la source de mise à jour toutes les semaines.
   - **Une fois toutes les 2 semaines** : sélectionnez cette option pour recevoir des mises à jour sur les nouveaux catalogues disponibles dans la source de mise à jour une fois toutes les deux semaines.
   - **Une fois par mois** : sélectionnez cette option pour recevoir tous les mois des mises à jour sur les nouveaux catalogues disponibles dans la source de mise à jour.

Afficher et actualiser l'inventaire d'appareils

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 firmware existant au firmware 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.

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 `downloads.dell.com` échoue, la source de mise à jour Dell CATALOGUE DELL EMC ENTERPRISE en ligne par défaut 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 CATALOGUE DELL EMC ENTERPRISE (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 MECM, 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 MECM 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 firmware des périphériques détectés :

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 firmware 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 firmware 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 firmware existant vers cette version.
   - Aucune action requise : le firmware 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 firmware sont inclus.

Appliquer les filtres

Appliquez des filtres pour afficher les informations sélectionnées dans le rapport de comparaison.

Filtrez le rapport de comparaison en fonction des composants de serveur disponibles. OMIMSSC prend en charge trois catégories de filtres :

- **Nature de la mise à jour** : sélectionnez cette option pour filtrer et afficher uniquement le type sélectionné de mise à jour sur les serveurs.
- **Type de composant** : sélectionnez cette option pour filtrer et afficher uniquement les composants sélectionnés sur les serveurs.
- **Modèle de serveur** : sélectionnez cette option pour filtrer et afficher uniquement les modèles de serveurs sélectionnés.

REMARQUE : Vous ne pouvez pas exporter et importer des profils de serveur si les filtres sont appliqués.

Pour appliquer les filtres :

Dans OMIMSSC, cliquez sur **Centre de maintenance** et sur le menu déroulant des filtres, puis sélectionnez les filtres.

Supprimer des filtres

Pour supprimer des filtres :

Dans OMIMSSC, cliquez sur **Centre de maintenance** et sur **Effacer des filtres** ou désactivez les cases cochées.

Mettre à niveau et rétrograder les versions de firmware à l'aide de la méthode d'exécution de mise à jour

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 la source de mise à jour CATALOGUE DE MISES À JOUR POUR LES SOLUTIONS MICROSOFT HCI ou les sources de mise à jour CATALOGUE DE MISES À JOURS DELL EMC MX pour appliquer les mises à jour de firmwares sur des clusters HCI de serveurs Windows ou des systèmes modulaires MX7000, ces sources de mise à jour présentent une référence modifiée vers le catalogue qui contient les versions de firmware recommandées pour les clusters HCI de serveurs Windows 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.

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 firmware 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 firmware :

- 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 firmware 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 firmware sur les périphériques n'entraîne aucune action sur les périphériques.
- Pour plus d'informations sur la mise à jour du châssis, consultez la section Mise à jour de firmware CMC du document Guide de l'utilisateur du firmware Dell PowerEdge M1000e Chassis Management Controller.
  - Pour plus d'informations sur la mise à jour de firmware du châssis dans VRTX, consultez la section Mise à jour de firmware du document Guide d'utilisation de Dell Chassis Management Controller pour Dell PowerEdge VRTX.

- Pour plus d'informations sur la mise à jour de firmware du châssis dans FX2, consultez la section Mise à jour de firmware du document Guide d'utilisation de Dell Chassis Management Controller pour Dell PowerEdge X2.

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 une 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 une mise à jour**.
3. Dans la zone **Détails de la mise à jour**, entrez le nom et la description de la tâche de mise à jour de firmware.
4. Pour activer la rétrogradation des versions de firmware, 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 firmware.
5. 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 firmware à l'avenir.
6. 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.
   - **Mises à jour sans agent** : les mises à jour sont appliquées et le système redémarre immédiatement.

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

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 firmware 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.

Mises à jour via CAU

Les mises à jour sur les serveurs (qui font partie du cluster) se produisent via le coordinateur de mise à jour de cluster qui est présent sur le même système où le serveur SCVMM est installé. Les mises à jour sont appliquées immédiatement et non en plusieurs étapes. À l'aide de la mise à jour adaptée aux clusters, vous pouvez réduire toute interruption ou tout temps d'inactivité du serveur en permettant la disponibilité continue de la charge applicative. Par conséquent, il n'y a aucun impact sur le service fourni par le groupe de clusters. Pour plus d'informations sur la mise à jour adaptée aux clusters, reportez-vous à la section Présentation de la mise à jour adaptée aux clusters à l'adresse `technet.microsoft.com`.

Avant d'appliquer les mises à jour sur les groupes de mise à jour de cluster, vérifiez les éléments suivants :

- Assurez-vous que l'utilisateur inscrit dispose de privilèges d'administrateur pour la mise à jour via la fonction de mise à jour adaptée aux clusters.
- Connectivité à une source de mise à jour sélectionnée.
- Disponibilité des clusters de basculement.
- Vérifiez la préparation de la mise à jour de cluster et assurez-vous qu'il n'existe aucune erreur ni aucun avertissement important dans le rapport de préparation du cluster pour l'application de la méthode de mise à jour adaptée aux clusters. Pour plus d'informations sur la fonctionnalité de mise à jour adaptée aux clusters, reportez-vous à la section Requirements and Best Practices for Cluster—aware Updating (Exigences et pratiques d'excellence relatives à la mise à jour adaptée aux clusters) à l'adresse `Technet.microsoft.com`.
- Assurez-vous que le système d'exploitation Windows Server 2012 R2, Windows 2016 ou Windows 2019 est installé sur tous les nœuds de cluster de basculement pour prendre en charge la fonctionnalité de mise à jour adaptée aux clusters.
- La configuration des mises à jour automatiques n'est pas activée pour installer automatiquement les mises à jour sur un nœud du cluster de basculement.
- Activez la règle de pare-feu qui permet l'arrêt à distance sur chaque nœud du cluster de basculement.
- Assurez-vous que le groupe de clusters possède au moins deux nœuds.

REMARQUE :

- Pour en savoir plus sur l'application de mises à jour, reportez-vous à Mise à niveau et rétrogradation des versions de firmware à l'aide de la méthode d'exécution de mise à jour. Pour plus d'informations sur Dell EMC Repository Manager pour télécharger les mises à jour des firmwares et des pilotes, rendez-vous sur la page Catalogue des mises à jour des firmwares et des pilotes pour Dell EMC Solutions pour Microsoft Azure Stack HCI dans `dell.com\support` et téléchargez le fichier de catalogue.

19

Gérer les appareils avec OMIMSSC

Conservez les serveurs et les systèmes modulaires à jour en planifiant les tâches pour la mise à niveau des firmwares des composants du serveur et des systèmes modulaires. Gérez les serveurs en restaurant les serveurs à un état précédent en exportant leur configuration antérieure, en appliquant les configurations de l'ancien composant sur le composant remplacé, et en exportant les journaux LC à des fins de résolution des problèmes.

Sujets :

- Restauration de serveur
- Appliquer les paramètres de firmware et de configuration sur un composant remplacé
- Collecter des journaux LC pour les serveurs
- Exporter l'inventaire
- Gérer des tâches

Restauration de serveur

Enregistrez les configurations d'un serveur dans l'archive sécurisée en exportant les configurations du serveur dans un profil et en important le profil sur le même serveur pour le restaurer à un état antérieur.

Archive sécurisée (Protection vault)

L'archive sécurisée est un emplacement sécurisé où vous pouvez enregistrer les profils de serveur. Exportez le profil de serveur à partir d'un serveur ou d'un groupe de serveurs et importez-le sur le même serveur ou groupe de serveurs. Vous pouvez enregistrer ce profil de serveur sur un emplacement partagé dans le réseau en créant une archive externe ou sur une carte vFlash Secure Digital (SD) interne en créant une archive interne. Vous pouvez associer un serveur ou un groupe de serveurs à une seule archive sécurisée. Cependant, vous pouvez associer une archive sécurisée à de nombreux serveurs ou un groupe de serveurs. Vous pouvez enregistrer un profil de serveur sur une seule archive sécurisée. Cependant, vous pouvez enregistrer n'importe quel nombre de profils de serveur sur une seule archive sécurisée.

Créer une archive sécurisée

Assurez-vous que l'emplacement de l'archive est accessible.

1. Dans **OMIMSSC**, cliquez sur **Centre de maintenance**, puis sur **Paramètres de maintenance**.
2. Dans **Centre de maintenance**, cliquez sur **Archive sécurisée** puis sur **Créer**.
3. Sélectionnez un type d'archive sécurisée à utiliser et fournissez les détails.
   - Si vous créez une archive sécurisée de type **Partage réseau**, indiquez un emplacement pour enregistrer les profils, les informations d'identification pour accéder à cet emplacement et une phrase secrète pour sécuriser le profil.
     REMARQUE : Ce type d'archive sécurisée assure la prise en charge du partage de fichiers de type CIFS (Common Internet File System).
   - Si vous créez une archive sécurisée de type **vFlash**, fournissez la phrase secrète pour protéger le profil.

Modifier une archive sécurisée

vous ne pouvez pas modifier le nom, la description, le type d'archive sécurisée et la phrase secrète.

1. Dans **OMIMSSC**, cliquez sur **Centre de maintenance** > **Paramètres de maintenance** > **Archive sécurisée**.
2. Pour modifier l'archive sécurisée, sélectionnez-la, puis cliquez sur **Modifier**.

REMARQUE : Si l'archive sécurisée est modifiée pendant que les tâches d'exportation ou d'importation du profil du serveur sont en cours, les informations modifiées sont prises en compte pour les sous-tâches en attente dans la tâche.

Supprimer une archive sécurisée

Vous ne pouvez pas supprimer une archive sécurisée dans les cas suivants :

- L'archive sécurisée est associée à un serveur ou un groupe de serveurs.

  Pour supprimer une archive sécurisée, supprimez le serveur ou le groupe de serveurs, puis supprimez l'archive sécurisée.

- Une tâche planifiée est associée à cette archive sécurisée. Cependant, pour supprimer cette archive sécurisée, supprimez la tâche planifiée, puis supprimez l'archive sécurisée.

1. Dans **OMIMSSC**, cliquez sur **Centre de maintenance** > **Paramètres de maintenance** > **Archive sécurisée**.
2. Sélectionnez l'archive à supprimer, puis cliquez sur **Supprimer**.

Exporter des profils de serveur

Exportez un profil de serveur, y compris les images de firmware installées sur divers composants, tels que le BIOS, RAID, la carte NIC, l'iDRAC, Lifecycle Controller et la configuration de ces composants. L'appliance OMIMSSC crée un fichier contenant toutes les configurations, que vous pouvez enregistrer sur une carte SD vFlash ou un partage réseau. Sélectionnez une archive sécurisée de votre choix pour enregistrer ce fichier. Vous pouvez exporter les profils de configuration d'un serveur ou d'un groupe de serveurs immédiatement ou les planifier pour plus tard. En outre, vous pouvez sélectionner une option de récurrence pertinente pour la fréquence d'exportation des profils de serveur.

Désactivez l'option **Invite F1/F2 en cas d'erreur** dans **Paramètres du BIOS**.

Tenez compte des points suivants avant d'exporter des profils de serveur :

- Au niveau d'une instance, vous pouvez planifier une seule tâche de configuration d'exportation pour un groupe de serveurs.
- Vous ne pouvez pas effectuer d'autres activités sur ce serveur ou groupe de serveurs dont les profils de configuration sont en cours d'exportation.
- Assurez-vous que la tâche **Procédure de sauvegarde automatique** dans l'iDRAC n'est pas planifiée pour la même heure.
- Vous ne pouvez pas exporter des profils de serveur si les filtres sont appliqués. Pour exporter des profils de serveur, désactivez tous les filtres appliqués.
- Pour exporter des profils de serveur, assurez-vous que vous disposez de la licence iDRAC Enterprise.
- Avant l'exportation du profil de serveur, assurez-vous que l'adresse IP du serveur n'est pas modifiée. Si l'adresse IP du serveur a changé en raison d'une opération quelconque, redécouvrez ce serveur dans OMIMSSC, puis planifiez la tâche d'exportation de profil de 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.
3. Dans **Exporter le profil du serveur**, fournissez les détails de la tâche, puis sélectionnez une archive sécurisée.

   Pour plus d'informations sur les archives sécurisées, reportez-vous à la section Création d'une archive sécurisée.

   Sous **Planifier l'exportation du profil du serveur**, sélectionnez l'une des options suivantes :
   - **Exécuter maintenant** : exporte immédiatement la configuration de serveur ou du groupe de serveurs sélectionnés.
   - Planification : fournit un calendrier pour l'exportation de la configuration de serveur du groupe de serveurs sélectionné.
     - **Jamais** : exporte le profil de serveur une seule fois au cours de l'heure planifiée.
     - **Une fois par semaine** : exporte le profil de serveur toutes les semaines.
     - **Une fois toutes les 2 semaines** : exporte le profil de serveur une fois toutes les deux semaines.
     - **Une fois toutes les 4 semaines** : exporte le profil de serveur une fois toutes les quatre semaines.

Importer le profil du serveur

Vous pouvez importer un profil de serveur qui a été exporté précédemment pour ce même serveur, ou un groupe de serveurs. L'importation du profil du serveur aide à restaurer la configuration et le firmware d'un serveur à un état stocké dans le profil.

Vous pouvez importer des profils de serveur de deux manières :

- Importation rapide de profil de serveur : permet d'importer automatiquement le dernier profil de serveur exporté pour ce serveur. Vous n'avez pas besoin de sélectionner chacun des profils de serveur de chacun des serveurs pour cette opération.
- Importation personnalisée de profil de serveur : importe les profils de serveur de chacun des serveurs sélectionnés individuellement. Par exemple, si l'exportation du profil de serveur est planifiée et que le profil de serveur est exporté tous les jours, cette fonction permet de sélectionner un profil de serveur spécifique qui est importé depuis la liste des profils de serveur disponibles dans l'archive sécurisée du serveur.

Remarques sur l'importation des profils de serveur :

- Vous pouvez importer un profil de serveur à partir d'une liste de profils de serveur exportés pour ce serveur uniquement. Vous ne pouvez pas importer les mêmes profils de serveur pour les différents serveurs ou groupes de serveurs. Si vous essayez d'importer le profil de serveur d'un autre serveur ou groupe de serveurs, la tâche d'importation de profil de serveur échoue.
- Si une image de profil de serveur n'est plus disponible pour un serveur ou groupe de serveurs et qu'une tâche d'importation de profil de serveur est tentée pour le serveur ou le groupe de serveurs, la tâche d'importation du profil de serveur échoue pour les serveurs ayant ce profil de serveur. Un message de journal est ajouté dans les journaux d'activité avec les détails de l'échec.
- Après l'exportation d'un profil de serveur, si un composant est supprimé du serveur, puis qu'une tâche d'importation de profil est démarrée, toutes les informations sur les composants sont restaurées à l'exception des informations sur les composants manquants. Ces informations ne sont pas disponibles dans le journal d'activité d'OMIMSSC. Pour en savoir plus sur les composants manquants, consultez le **journal Lifecycle** d'iDRAC.
- Vous ne pouvez pas importer un profil de serveur après l'application des filtres. Pour importer des profils de serveur, désactivez tous les filtres appliqués.
- Pour importer des profils de serveur, vous devez disposer de la licence iDRAC Enterprise.

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.
3. Fournissez les détails, sélectionnez le **type d'importation de profil de serveur** souhaité.

   REMARQUE : Un profil de serveur est exporté en même temps que la configuration RAID existante. Cependant, vous pouvez importer le profil de serveur en incluant ou en excluant la configuration RAID sur le serveur ou groupe de serveurs. L'option **Conserver les données** est sélectionnée par défaut et conserve la configuration RAID existante dans le serveur. Désactivez cette case si vous souhaitez appliquer les paramètres RAID stockés dans le profil de serveur.

4. Pour importer le profil de serveur, cliquez sur **Terminer**.

Appliquer les paramètres de firmware et de configuration sur un composant remplacé

La fonction de remplacement de pièce met automatiquement à jour un composant de serveur remplacé à la version de firmware requise, à la configuration de l'ancien composant, ou les deux. La mise à jour est effectuée automatiquement lorsque vous redémarrez le serveur après avoir remplacé le composant.

Afin de définir les configurations pour le remplacement d'une 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.

3. Vous pouvez définir **CSIOR**, **Mise à jour de firmware de pièce** et **Mise à jour de la configuration de pièce** sur l'une des options suivantes, puis cliquer sur **Terminer** :
   - CSIOR (collecte de l'inventaire du système au redémarrage) : collecte toutes les informations relatives au composant à chaque redémarrage du système.
     - **Activé** : les informations d'inventaire des logiciels et du matériel des composants du serveur sont mises à jour automatiquement à chaque redémarrage du système.
     - **Désactivé** : les informations d'inventaire des logiciels et du matériel des composants de serveur ne sont pas mises à jour.
     - **Ne pas modifier la valeur sur le serveur** : la configuration de serveur existante est conservée.
   - Mise à jour de firmware de pièce : restaure, met à niveau ou rétrograde la version du firmware du composant en fonction de la sélection effectuée.
     - **Désactivé** : la mise à jour de firmware de pièce est désactivée et la même configuration est appliquée au composant remplacé.
     - **Autoriser uniquement la mise à niveau de version** : les versions de firmware mises à niveau sont appliquées au composant remplacé, si la version de firmware du nouveau composant est antérieure à la version existante.
     - **Faire correspondre le firmware de la pièce remplacée** : la version du firmware du nouveau composant est mise en correspondance avec la version de firmware du composant d'origine.
     - **Ne pas modifier la valeur sur le serveur** : la configuration existante du composant est conservée.
   - Mise à jour de la configuration de pièce : restaure ou met à niveau la configuration des composants en fonction de la sélection effectuée.
     - **Désactivé** : la mise à jour de la configuration de pièce est désactivée et la configuration enregistrée de l'ancien composant n'est pas appliquée au composant remplacé.
     - **Toujours appliquer** : la mise à jour de la configuration de pièce est activée et la configuration enregistrée de l'ancien composant est appliquée au composant remplacé.
     - **Appliquer uniquement si le firmware correspond** : la configuration enregistrée de l'ancien composant est appliquée au composant remplacé uniquement si les versions de leurs firmwares correspondent.
     - **Ne pas modifier la valeur sur le serveur** : la configuration existante est conservée.

Collecter des journaux LC pour les serveurs

Les journaux LC fournissent un historique des activités déroulées sur un système géré. Ces fichiers journaux sont utiles pour les administrateurs du serveur, car ils fournissent des informations détaillées sur les actions recommandées et d'autres informations techniques utiles à des fins de dépannage. Les différents types d'informations disponibles dans les journaux LC sont relatifs aux alertes, aux modifications de configuration sur les composants matériels du système, aux modifications de firmwares en raison d'une mise à niveau ou d'une rétrogradation, aux pièces remplacées, aux avertissements de température, aux horodatages détaillés correspondant au démarrage des activités, à la gravité des activités, etc. Le fichier journal LC exporté est enregistré dans un dossier et le dossier est nommé d'après le numéro de série du serveur. Les journaux LC sont enregistrés au format `<YYYYMMDDHHMMSSSSS>.<file format>`. Par exemple, 201607201030010597.xml.gz est le nom de fichier LC, ce qui inclut la date et l'heure de création du fichier. Il existe deux options pour recueillir les journaux LC :

- Journaux LC complets : exporte les fichiers journaux actifs et archivés. Ils sont de grande taille, et de ce fait, compressés au format `.gz` et exportés vers l'emplacement spécifié sur un partage réseau CIFS.
- Journaux LC actifs : exporte les fichiers journaux récents immédiatement ou planifie une tâche pour exporter les fichiers journaux à intervalles réguliers. Affichez, recherchez et exportez ces fichiers journaux vers l'appliance OMIMSSC. De plus, vous pouvez enregistrer une sauvegarde de fichiers journaux dans un partage réseau.

Pour installer les journaux LC, procédez comme suit :

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**.
3. Dans **Collecte des journaux LC**, sélectionnez l'une des options suivantes et cliquez sur **Terminer** :
   - **Exporter l'intégralité des journaux LC (.gz)** : sélectionnez cette option pour exporter l'intégralité des journaux LC vers un partage réseau CIFS en fournissant les informations d'identification Windows.
   - **Exporter les journaux actifs (Exécuter maintenant)** : sélectionnez cette option pour exporter immédiatement les journaux actifs vers l'appliance OMIMSSC.
     - (Facultatif) Cochez la case **Sauvegarder les journaux LC sur le partage réseau** pour enregistrer une sauvegarde des journaux LC sur le partage réseau CIFS en fournissant les informations d'identification Windows.
   - **Planifier la collecte des journaux LC** : sélectionnez cette option pour exporter les journaux actifs à intervalles réguliers.

     Dans **Planifier la collecte des journaux LC**, sélectionnez une date et une heure pour exporter les fichiers journaux.

Sélectionnez un bouton radio en fonction de la fréquence d'exportation souhaitée des fichiers. Les options de planification de fréquence disponibles afin de déterminer la fréquence à laquelle vous souhaitez collecter les journaux LC sont les suivantes :

- **Jamais** : cette option est sélectionnée par défaut. Sélectionnez cette option pour exporter les journaux LC une seule fois à un moment planifié.
- **Tous les jours** : sélectionnez cette option pour exporter les journaux LC tous les jours à l'heure planifiée.
- **Une fois par semaine** : sélectionnez cette option pour exporter les journaux LC une fois par semaine à l'heure planifiée.
- **Une fois toutes les 4 semaines** : sélectionnez cette option pour exporter les journaux LC une fois toutes les quatre semaines à l'heure planifiée.
- (Facultatif) Cochez la case **Sauvegarder les journaux LC sur le partage réseau** pour enregistrer une sauvegarde des journaux LC sur le partage réseau CIFS en fournissant les informations d'identification Windows.

REMARQUE : Indiquez un dossier de partage avec suffisamment d'espace de stockage, étant donné que les fichiers exportés sont de grande taille.

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

Afficher des journaux LC

Affichez tous les journaux LC actifs, recherchez une description détaillée et téléchargez les journaux au format CSV.

Ajoutez l'appliance OMIMSSC dans le **site Intranet local**.

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**.
3. Tous les serveurs dans le groupe sélectionné et les serveurs pour lesquels des journaux LC sont collectés sont répertoriés avec leurs fichiers journaux LC. Cliquez sur le nom de fichier pour afficher toutes les entrées de journal dans le fichier journal LC spécifique de ce serveur. Pour plus d'informations, reportez-vous à la section Description de fichier.
4. (Facultatif) Utilisez la zone de recherche pour effectuer une recherche dans les descriptions de tous les fichiers journaux, et exportez le fichier au format CSV.

   Il existe deux méthodes pour rechercher une description de message dans un fichier LC :
   - Cliquez sur un nom de fichier pour ouvrir le fichier journal LC et recherchez une description dans la zone de recherche.
   - Saisissez une description dans la zone de recherche, puis affichez tous les fichiers LC avec ces instances de texte.

   REMARQUE : Si le message de description du journal LC est long, le message est tronqué à 80 caractères.

   REMARQUE : L'heure affichée en regard des messages du journal LC correspond au fuseau horaire de l'iDRAC.

Description de fichier

Utilisez cette page pour afficher les informations détaillées sur certaines actions recommandées et d'autres informations techniques qui sont utiles à des fins d'alerte ou de suivi d'un serveur particulier.

Pour afficher le contenu d'un fichier, cliquez sur un nom de fichier :

- Vous pouvez rechercher des descriptions de message spécifiques.
- Vous pouvez consulter les fichiers journaux dans la fenêtre ou télécharger le fichier pour afficher des messages de journal supplémentaires.
- Vous pouvez afficher les commentaires d'un utilisateur pour une activité.

REMARQUE : Lors de l'utilisation de l'option de recherche, seuls les résultats de la recherche sont exportés vers un fichier CSV.

REMARQUE : Si le message est long, le message est tronqué à 80 caractères.

REMARQUE : Cliquez sur **ID de message** pour afficher plus d'informations sur le message.

Exporter 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.

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

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.

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 de l’hôte ou l’adresse IP, le modèle de périphérique, le nom de composant, la version de firmware en cours sur ce composant, la version de firmware de la source de mise à jour et l’action de mise à jour sur ce composant.

Gérer des tâches

Assurez-vous que la tâche présente l'état **Planifiée**.

1. Dans OMIMSSC, effectuez l’une des opérations suivantes :
   - Dans le volet de navigation, cliquez sur **Centre de maintenance**, puis cliquez sur **Gérer les tâches**.
   - Dans le volet de navigation, cliquez sur **Centre des tâches et des journaux**, puis cliquez sur l'onglet **Planifiée**.
2. Sélectionnez les tâches à annuler, puis cliquez sur **Annuler** et sur **Oui** pour confirmer.

20

Déployer le cluster Azure Stack HCI

Vous trouverez ci-dessous les étapes à suivre pour déployer le cluster Azure Stack HCI :

1. Créez les profils d'informations d'identification de périphérique et de Windows requis.
2. Créer une image WinPE
   a. Installez la fonctionnalité WDS sur le SCVMM, puis configurez-la.
   b. Ajoutez un serveur PXE dans le serveur SCVMM en utilisant des ressources supplémentaires et spécifiez le même nom de serveur (nom de l'hôte SCVVM) Serveur PXE.
   c. Créez le dossier partagé dans le serveur SCVMM, puis copiez le fichier Boot.wim à partir de *C:\RemoteInstall\DCMgr\Boot\Windows\Images* vers un dossier de partage.
   d. Extrayez les pilotes depuis le pack de pilotes Dell EMC OpenManage.
   e. Créez une image WinPE.
   f. Assurez-vous que l'image WinPE est placée dans un dossier partagé dans SCVMM.
3. Ajoutez le modèle de machine virtuelle du serveur Windows 2016 et 2019 à la bibliothèque SCVMM. Pour plus d'informations, reportez-vous à la documentation Windows.
   a. Modifiez les propriétés suivantes :
   - Système d'exploitation : Datacenter Windows Server 2016 et 2019
   - Plate-forme de virtualisation : Microsoft Hyper-V

   REMARQUE : Pour créer un disque virtuel Windows Server 2019 (.vhdx) à l'aide du fichier .iso pour le déploiement du système d'exploitation, reportez-vous à https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f
4. Créez un profil d'ordinateur physique (PCP) dans SCVMM. Dans Configuration matérielle > Disque et partitions, sélectionnez le schéma de partition en tant que **Tableau de partition GUID**. Pour plus d'informations, reportez-vous à la section de création d'un profil d'ordinateur physique dans la section des conditions préalables de la documentation Microsoft sur le provisionnement d'un hôte ou d'un cluster Hyper-V à partir d'ordinateurs sans système d'exploitation.
5. Créez un groupe d'hôtes dans SCVMM pour héberger le cluster Azure Stack HCI. Pour en savoir plus sur la création de groupes d'hôtes dans la console SCVMM, consultez la documentation de Microsoft.
6. Créez un profil d'hyperviseur.
7. Découvrez les serveurs dans l'extension Dell EMC OpenManage.
8. Configurez à l'aide d'un modèle opérationnel prédéfini.
9. (Facultatif) Vérifiez la conformité (Configuration et déploiement > Vue Serveur > sélectionnez le serveur et attribuez un modèle opérationnel).
10. Créer un commutateur logique
11. Déployez le cluster Azure Stack HCI.
    Pour vérifier le succès du déploiement du cluster, accédez à **Vue Cluster** pour vérifier si le cluster est répertorié avec la catégorie correspondante.

21

Dépannage

Sujets :

- Ressources nécessaires à la gestion OMIMSSC
- Vérification des autorisations d'utilisation de l'extension de console OMIMSSC pour MECM
- Vérification des autorisations PowerShell d'utilisation de l'extension de console OMIMSSC pour SCVMM
- Installation et mise à niveau de scénarios dans OMIMSSC
- OMIMSSC Scénarios du portail d'administration
- Scénarios de découverte, synchronisation et inventaire dans OMIMSSC
- Scénarios génériques dans OMIMSSC
- Scénarios de mise à jour de firmware dans OMIMSSC
- Scénarios de déploiement de système d'exploitation dans OMIMSSC
- Scénarios de profil de serveur dans OMIMSSC
- Scénarios de journaux LC dans OMIMSSC

Ressources nécessaires à la gestion OMIMSSC

Utilisez ce guide pour rechercher les privilèges requis et résoudre les problèmes rencontrés dans OMIMSSC.

Pour résoudre tous les problèmes rencontrés dans OMIMSSC, vérifiez que vous avez bien les ressources suivantes :

- Les détails du compte d'utilisateur en lecture seule pour vous connecter à l'appliance OMIMSSC et effectuer diverses opérations.

  Pour vous connecter en tant qu'utilisateur en lecture seule à partir de la machine virtuelle de l'appliance OMIMSSC, saisissez le nom d'utilisateur `readonly` avec le même mot de passe utilisé pour vous connecter à la machine virtuelle de l'appliance OMIMSSC.

- Fichiers journaux ayant un niveau élevé et tous les détails sur les erreurs :
  - Journaux d'activité : contient des informations spécifiques à l'utilisateur et de niveau élevé sur les tâches lancées dans OMIMSSC, ainsi que le statut des tâches exécutées dans OMIMSSC. Pour afficher les journaux d'activité, accédez à la page **Tâches et journaux** dans l'extension de console OMIMSSC.
  - Journaux complets : contient les journaux associés à l'administrateur et plusieurs journaux détaillés spécifiques aux scénarios dans OMIMSSC. Pour afficher l'intégralité des journaux, rendez-vous sur la page **Tâches et journaux** dans **Portail d'administration d'OMIMSSC**, **Paramètres**, puis **Journaux**.
  - Journaux LC : contiennent des informations au niveau du serveur, des messages d'erreur détaillés sur les opérations exécutées dans OMIMSSC. Pour télécharger et afficher les journaux LC, reportez-vous au *Guide de l'utilisateur de Dell EMC OpenManage Integration pour Microsoft System Center pour System Center Virtual Machine Manager*.

    REMARQUE : Pour le dépannage des périphériques individuels à partir de la page d'iDRAC ou d'OpenManage Enterprise Module (OME-modulaire), lancez OMIMSSC, cliquez sur la page **Configuration et déploiement**, lancez les vues respectives, puis cliquez sur l'URL de l'adresse IP du périphérique.

REMARQUE : L'utilisateur Admin du serveur SCVMM ne doit pas correspondre à un compte de service SCVMM.

REMARQUE : Si vous effectuez une mise à niveau de SP1 VMM SC2012 à R2 VMM SC2012, effectuez une mise à niveau à Windows PowerShell 4.0.

Vérification des autorisations d'utilisation de l'extension de console OMIMSSC pour MECM

Après avoir installé OMIMSSC, vérifiez que l'utilisateur possède les droits suivants :

1. Sur le système où OMIMSSC est installé, fournissez les autorisations d'**écriture** pour le dossier *<Configuration Manager Admin Console Install Dir>\XmlStorage\Extensions\DLCPlugin* à l'aide des commandes PowerShell.

Remplissez les conditions préalables suivantes sur le serveur de site et le serveur de fournisseur SMS avant d'installer le composant OMIMSSC :

a. Dans PowerShell, exécutez la commande : `PSRemoting`.

   Si la commande `PSRemoting` est désactivée, exécutez la commande `PSRemoting` à l'aide des commandes suivantes.

   i. Exécutez la commande : `Enable-PSRemoting`
   ii. Dans le message de confirmation, tapez `Y`.

b. Dans PowerShell, exécutez la commande : `Get-ExecutionPolicy`.

   Si la stratégie n'est pas définie sur `RemoteSigned`, alors définissez-la sur `RemoteSigned` à l'aide des commandes suivantes.

   i. Exécutez la commande : `Set-ExecutionPolicy RemoteSigned`.
   ii. Dans le message de confirmation, tapez `Y`.

2. Configurez l'accès utilisateur à WMI (infrastructure de gestion Windows). Pour plus d'informations, reportez-vous à la section Configuration de l'accès utilisateur à WMI.
3. Accordez les autorisations du dossier et du partage afin de pouvoir écrire des fichiers sur le dossier des boîtes de réception.

   Pour accorder les autorisations du dossier et du partage afin de pouvoir écrire des fichiers sur la boîte de réception DDR :

   a. Depuis la console Configuration Manager, sous **Administration**, accordez à l'utilisateur l'autorisation d'écrire sur le partage **SMS_<codesite>**.
   b. À l'aide de l'**Explorateur de fichiers**, accédez à l'emplacement du partage **SMS_<codesite>**, puis au dossier `ddm.box`. Accordez un contrôle total à l'utilisateur du domaine pour les dossiers suivants :
      - **SMS_<codesite>**
      - Boîtes de réception
      - `ddm.box`

Configuration de l'accès utilisateur à WMI

Pour configurer l'accès utilisateur distant à WMI :

REMARQUE : Assurez-vous que le pare-feu de votre système ne bloque pas la connexion WMI.

1. Pour accéder au modèle DCOM (Distributed Component Object Model) à distance, fournissez les autorisations à l'utilisateur MECM inscrit.

   Pour octroyer des droits d'utilisateur DCOM :

   a. Exécutez `dcomcnfg.exe`.
   b. Depuis le volet gauche, dans la console **Services de composants**, développez **Ordinateurs**, effectuez un clic droit sur **Poste de travail**, puis sélectionnez **Propriétés**.
   c. Sur **Sécurité COM** :
      - Depuis **Droits d'accès**, cliquez sur **Modifier les limites**, puis sélectionnez **Accès distant**.
      - Depuis **Droit de lancement et d'activation**, cliquez sur **Modifier les limites**, puis sélectionnez **Lancement local**, **Lancement à distance** et **Activation à distance**.

2. Pour accéder aux composants DCOM Config Windows Management and Instrumentation (WMI), fournissez les droits d'utilisateur à l'utilisateur inscrit.

   Pour octroyer des droits d'utilisateur DCOM Config WMI :

   a. Exécutez `dcomcnfg.exe`.
   b. Développez **Poste de travail** > **Configuration DCOM**.
   c. Effectuez un clic droit sur **Gestion et instrumentation Windows**, puis sélectionnez **Propriétés.**
   d. Dans l'onglet **Sécurité**, depuis **Droit de lancement et d'activation**, cliquez sur **Modifier**, puis sélectionnez les **Droits de Lancement à distance** et **Activation à distance**.

3. Définissez la sécurité de l'espace de nommage et octroyez les autorisations.

   Pour configurer les paramètres de sécurité de l'espace de nommage et octroyer des droits :

   a. Lancer `wmimgmt.msc`
   b. Dans le panneau **Contrôle WMI**, effectuez un clic droit sur **Contrôle WMI**, sélectionnez **Propriétés**, puis sélectionnez **Sécurité**.
   c. Accédez à `ROOT\SMS Namespace`.
   d. Sélectionnez les droits **Exécuter les méthodes**, **Fournir une écriture**, **Activer le compte** et **Droits d'activation à distance**.
   e. Accédez à `Root\cimv2\OMIMSSC`.
   f. Sélectionnez les droits **Exécuter les méthodes**, **Fournir une écriture**, **Activer le compte** et **Droits d'activation à distance**.

Une autre méthode consiste pour l'utilisateur Configuration Manager à devenir un membre du groupe **SMS_Admin** et vous pouvez alors ajouter **Activation à distance** aux droits du groupe.

Vérification des autorisations PowerShell d'utilisation de l'extension de console OMIMSSC pour SCVMM

Vérifiez si le statut **`PSRemoting`** est activé et **`ExecutionPolicy`** est défini sur **`RemoteSigned`**. Si le statut est différent, exécutez les étapes ci-dessous dans PowerShell :

a. Dans PowerShell, exécutez la commande : `PSRemoting`.

   Si la commande `PSRemoting` est désactivée, exécutez la commande `PSRemoting` à l'aide des commandes suivantes.

   i. Exécutez la commande : `Enable-PSRemoting`

   ii. Dans le message de confirmation, tapez `Y`.

b. Dans PowerShell, exécutez la commande : `Get-ExecutionPolicy`.

   Si la stratégie n'est pas définie sur `RemoteSigned`, alors définissez-la sur `RemoteSigned` à l'aide des commandes suivantes.

   i. Exécutez la commande : `Set-ExecutionPolicy RemoteSigned`.

   ii. Dans le message de confirmation, tapez `Y`.

Installation et mise à niveau de scénarios dans OMIMSSC

Cette section contient toutes les informations de dépannage liées à l'installation et à la mise à niveau d'OMIMSSC

Vérification de la configuration de la machine virtuelle d'OMIMSSC

Pour vérifier que la machine virtuelle de l'appliance OMIMSSC est correctement configurée, sélectionnez-la, puis cliquez avec le bouton droit sur la machine virtuelle de l'appliance OMIMSSC, cliquez sur **Paramètres**, puis effectuez les tâches suivantes :

1. Vérifiez si l'allocation de mémoire pour l'appliance OMIMSSC est conforme à la configuration requise mentionnée dans la section Configuration matérielle pour OMIMSSC. Sinon, indiquez la mémoire dans **RAM de démarrage**, puis cliquez sur **Appliquer**.
2. Vérifiez si le nombre de processeurs est conforme à la configuration requise mentionnée dans la section Configuration matérielle pour OMIMSSC. Vous pouvez également indiquer le nombre de processeurs dans **Nombre de processeurs virtuels** sous **Processeurs**.
3. Vérifiez, dans le champ **Disque dur virtuel** sous Contrôleur IDE : **Contrôleur IDE 0** > **Disque dur**, si le **Disque dur virtuel** fait référence au fichier **OMIMSSC—v7**. Sinon, cliquez sur **Parcourir** et naviguez jusqu'à l'emplacement où le fichier VHD est décompressé et sélectionnez le fichier **OMIMSSC—v7**, puis cliquez sur **Appliquer**.
4. Vérifiez si **Adaptateur réseau** > **Commutateur virtuel** est connecté à une carte réseau (NIC) physique ; si ce n'est pas le cas, configurez la carte réseau, sélectionnez la carte réseau appropriée dans le menu déroulant **Commutateur virtuel** et cliquez sur **Appliquer**.

Si la machine virtuelle nouvellement créée avec le disque dur virtuel sélectionné pour l'appliance OMIMSSC ne parvient pas à s'amorcer avec une exception de panique du noyau, modifiez les paramètres de la machine virtuelle et activez l'option de mémoire dynamique sur cette machine virtuelle, en procédant comme suit :

1. Cliquez avec le bouton droit sur la machine virtuelle de l'appliance OMIMSSC, cliquez sur **Paramètres**, puis cliquez sur **Mémoire**.
2. Sous **Mémoire dynamique**, cochez la case **Activer la mémoire dynamique**, puis fournissez les détails.

Échec de l'inscription

Si le test de connexion ou l'inscription échoue, alors vous recevez un message d'erreur.

Pour résoudre ce problème, procédez comme suit :

- Envoyez un ping à partir de l'appliance OMIMSSC vers le FQDN de serveur MECM ou SCVMM inscrit par le biais d'une connexion à la machine virtuelle de l'appliance OMIMSSC en tant qu'utilisateur en lecture seule. Si vous obtenez une réponse, patientez un certain temps et passez ensuite à l'inscription.

Pour lancer la machine virtuelle de l'appliance OMIMSSC en tant qu'utilisateur en lecture seule, saisissez le nom d'utilisateur `readonly` avec le même mot de passe que celui utilisé pour vous connecter à la machine virtuelle de l'appliance OMIMSSC.

- Assurez-vous que le serveur MECM ou SCVMM est en cours d'exécution.
- Le compte Microsoft utilisé pour inscrire la console devrait être un admin délégué ou un administrateur dans System Center, et un administrateur local pour le serveur System Center.
- Spécifique aux utilisateurs de SCVMM :
  - Assurez-vous que le serveur SCVMM n'est pas enregistré sur n'importe quelle autre appliance OMIMSSC. Si vous souhaitez enregistrer le même serveur SCVMM avec l'appliance OMIMSSC, supprimez le profil d'application **Profil d'enregistrement OMIMSSC** du serveur SCVMM.
  - Si vous avez appliqué la mise à jour Rollup SCVMM, vérifiez le numéro de port TCP Indigo de la console SCVMM dans le registre `(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings)`. Utilisez le même numéro de port que celui utilisé pour enregistrer la console SCVMM. 8100 par défaut.

Échec du test de connexion

Si les noms d'utilisateur sont identiques mais que les mots de passe sont différents pour le compte d'utilisateur de domaine et le compte d'utilisateur local, alors le test de la connexion entre la console Microsoft et l'appliance OMIMSSC échoue.

Par exemple, le compte d'utilisateur de domaine est `domain\user1` et le mot de passe est `pwd1`. Et compte d'utilisateur local est `user1` et le mot de passe est `Pwd2`. Lorsque vous essayez de vous inscrire avec le compte d'utilisateur de domaine ci-dessus, le test de connexion échoue.

Pour contourner ce problème, utilisez des noms d'utilisateurs différents pour les comptes d'utilisateur de domaine et local, ou utilisez un compte d'utilisateur unique en tant qu'utilisateur local et lors de l'inscription à la console Microsoft dans l'appliance OMIMSSC.

Échec du lancement d'OMIMSSC après l'installation de l'extension de console MECM

À partir des configurations installées MECM 2103, le point de lancement de la console OMIMSSC n'est pas disponible par défaut dans la console MECM.

Pour contourner ce problème, désactivez **Seules les extensions de console approuvées pour la hiérarchie** dans les propriétés de **paramètres de hiérarchie**. *Pour plus d'informations, reportez-vous à la section de la console Configuration Manager dans la* documentation Microsoft.

Échec de la connexion à l'extension de console OMIMSSC pour SCVMM

Une fois l'extension de console OMIMSSC inscrite et installée dans un environnement SCVMM, lorsque vous tentez de lancer OMIMSSC, l'erreur suivante s'affiche : `Connection to server failed`.

Pour résoudre ce problème, procédez comme suit :

1. Ajoutez l'adresse IP de l'appliance OMIMSSC et le FQDN dans l'intranet local de la console SCVMM, lorsque vous lancez OMIMSSC.
2. Ajoutez l'adresse IP de l'appliance OMIMSSC et le FQDN dans **Zones de recherche directe** et **Zones de recherche indirecte** dans DNS.
3. Pour plus de détails, vérifiez s'il y a des messages d'erreur dans le fichier `C:\ProgramData\VMMLogs\AdminConsole`.

Erreur d'accès à l'extension de console après la mise à jour de SCVMM R2

Après l'application de la mise à jour Rollup pour SC2012 R2 VMM, si vous essayez d'ouvrir la console OMIMSSC déjà installée, SCVMM affiche un message d'erreur pour des raisons de sécurité, et vous ne pouvez pas accéder à la console OMIMSSC.

Pour résoudre le problème, procédez comme suit :

1. Supprimez le dossier se trouvant dans le chemin par défaut : `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Redémarrez SCVMM.
3. Supprimez l'extension de console, puis importez l'extension de console comme mentionné dans la section *Importation de l'extension de console OMIMSSC pour SCVMM* du *Guide d'installation de Dell EMC OpenManage Integration pour Microsoft System Center pour System Center Configuration Manager et System Center Virtual Machine Manager*.

Adresse IP non attribuée à l'appliance OMIMSSC

Après la création et le démarrage de la machine virtuelle de l'appliance OMIMSSC, l'adresse IP de l'appliance OMIMSSC n'est pas attribuée ni affichée.

Pour contourner ce problème, vérifiez si le commutateur virtuel est mappé à un commutateur physique, si ce dernier est configuré correctement, puis connectez-vous à l'appliance OMIMSSC.

Blocage de SCVMM lors de l'importation de l'extension de console OMIMSSC

La console d'administrateur SC2016 VMM RTM build 4.0.1662.0 peut se bloquer lors de l'importation de l'extension de console OMIMSSC.

Pour résoudre ce problème, mettez à niveau SCVMM à l'aide de l'article 4094925 de la base de connaissance disponible à `support.microsoft.com/kb/4094925`, puis importez l'extension de console OMIMSSC.

Échec de la connexion aux extensions de console OMIMSSC

La connexion de l'extension de console OMIMSSC échoue avec le message d'erreur suivant : `Failed to login. Ensure to use correct credentials or check if account is locked in Active Directory.`

Pour contourner ce problème, assurez-vous d'utiliser les informations d'identification correctes et que le compte n'est pas verrouillé dans Active Directory. En cas de verrouillage du compte dans Active Directory, réessayez de vous connecter au bout de quelques minutes en fonction de la stratégie de verrouillage du compte Active Directory. Pour plus d'informations sur les stratégies de verrouillage de compte Active Directory, reportez-vous à la documentation de Microsoft.

Blocage de SC2012 VMM SP1 pendant la mise à jour

Après la mise à niveau vers VMM SC2012 SP1, lors de l'importation de l'extension de console OMIMSSC vers SC2012 VMM UR5 ou version ultérieure, la console SCVMM peut cesser de fonctionner.

Pour plus d'informations sur ce problème et afin de résoudre le problème, consultez le problème n° 5 dans l'URL de la base de connaissances : `support.microsoft.com/kb/2785682`.

Pour contourner ce problème, mettez à jour SCVMM, quelle que soit la version de la mise à jour cumulative installée.

OMIMSSC Scénarios du portail d'administration

Cette section contient toutes les informations de dépannage liées au portail d'administration d'OMIMSSC

Message d'erreur lors de l'accès au portail d'administration d'OMIMSSC via le navigateur Mozilla Firefox

Lorsque vous accédez au portail d'administration d'OMIMSSC à l'aide du navigateur Mozilla Firefox, vous recevez le message d'avertissement suivant : "`Secure Connection Failed`".

Pour contourner ce problème, supprimez le certificat créé à partir d'une entrée précédente du portail d'administration dans le navigateur. Pour en savoir plus sur la suppression de certificat depuis le navigateur Mozilla Firefox, reportez-vous à `support.mozilla.org`

Échec de l'affichage du logo Dell EMC dans le portail d'administration d'OMIMSSC

Lorsque le portail d'administration d'OMIMSSC est lancé dans un navigateur IE Windows 2016 par défaut, le portail d'administration ne s'affiche pas avec le logo Dell EMC.

Pour contourner le problème, effectuez l'une des opérations suivantes :

- Faites une mise à niveau du navigateur IE vers la version la plus récente.
- Supprimez l'historique de navigation, puis ajoutez l'URL du portail d'administration d'OMIMSSC à la liste de favoris du navigateur.

Scénarios de découverte, synchronisation et inventaire dans OMIMSSC

Cette section contient toutes les informations de dépannage relatives aux problèmes de références, de découverte de serveurs, de regroupement de serveurs et de synchronisation de console Microsoft inscrite avec OMIMSSC lors de l'utilisation d'OMIMSSC.

Échec de la découverte des serveurs

Lorsque plusieurs consoles Microsoft sont inscrites dans une appliance OMIMSSC et que vous tentez de découvrir un serveur, si même une des consoles MECM n'est pas accessible, la tâche de détection des serveurs échoue.

Pour contourner ce problème, annulez l'inscription de la console MECM inaccessible ou corrigez les erreurs, puis assurez-vous que la console MECM est accessible à partir de l'appliance OMIMSSC.

Échec de la découverte automatique des serveurs iDRAC

La détection automatique des serveurs iDRAC échoue, dans le cas où le mot de passe défini pour le profil d'informations d'identification de l'appareil par défaut n'est pas suffisamment fiable.

Pour contourner ce problème, veillez à définir un mot de passe sécurisé. Pour plus d'informations sur les exigences en matière de la stratégie de mots de passe, reportez-vous au Guide de l'utilisateur de l'iDRAC.

Serveurs découverts non ajoutés à la collecte Tous les serveurs Dell Lifecycle Controller

Après avoir découvert les serveurs dans OMIMSSC pour l'extension de console MECM, le serveur risque de ne pas être ajouté dans la collecte **Tous les serveurs Dell Lifecycle Controller**.

Pour résoudre ce problème, supprimez la collecte **Tous les serveurs Dell Lifecycle Controller**, puis découvrez le serveur. La collecte est automatiquement créée dans MECM et le serveur est ajouté à ce groupe.

Échec de la découverte des serveurs en raison d'informations d'identification incorrectes

Si vous fournissez des références incorrectes lors de la découverte, en fonction de la version d'iDRAC utilisée, les solutions suivantes sont disponibles :

- ○ Lors de la découverte d'un serveur PowerEdge de 12e génération avec iDRAC de version 2.10.10.10 ou ultérieure, la détection de serveur échoue si des détails incorrects sont fournis dans le profil de référence, avec le comportement suivant :
  - À la première tentative, l'adresse IP du serveur n'est pas bloquée.
  - À la deuxième tentative, l'adresse IP du serveur est bloquée pendant 30 secondes.
  - À partir de la troisième tentative, l'adresse IP du serveur est bloquée pendant 60 secondes.

  Vous pouvez retenter la découverte des serveurs avec les détails de profil de référence corrects une fois que l'adresse IP est débloquée.

- Si le profil de référence iDRAC par défaut est modifié après la découverte d'un serveur et ajouté dans l'appliance, alors aucune activité ne peut être réalisée sur le serveur. Pour utiliser le serveur, redécouvrez le serveur avec le nouveau profil d'identification.

Création de groupe de châssis VRTX incorrect après la découverte des serveurs

Lorsque les serveurs modulaires précédemment installés dans un autre châssis sont ajoutés à un châssis VRTX et découverts dans OMIMSSC, les serveurs modulaires portent le numéro de série du châssis précédent. Par conséquent, un groupe de châssis VRTX avec les anciennes informations sur le châssis est créé dans l'appliance au lieu des informations les plus récentes sur le châssis.

Pour résoudre le problème, procédez comme suit :

1. Activez la fonction CSIOR et réinitialisez iDRAC sur le serveur modulaire qui vient d'être ajouté.
2. Supprimez manuellement tous les serveurs du groupe de châssis VRTX, puis effectuez une nouvelle découverte de ces serveurs.

Impossible de synchroniser les serveurs hôtes avec la console MECM inscrite

Lors de la synchronisation de l'extension de la console OMIMSSC avec la console MECM inscrite, les serveurs ne sont pas répertoriés en tant que sous-tâches dans la tâche de synchronisation et ne sont donc pas synchronisés.

Pour contourner ce problème, lancez la console MECM avec « Exécuter en tant que privilège d'administration » et mettez à jour la configuration hors bande pour un serveur. Puis, synchronisez l'extension de console OMIMSSC avec l'instance MECM inscrite.

Pour plus d'informations, reportez-vous à la section Synchronisation avec la console Microsoft inscrite dans *Guide unifié de l'utilisateur d'OpenManage Integration pour Microsoft System Center Version 7.3 pour Endpoint Configuration Manager et System Center Virtual Machine Manager*.

Impossible de supprimer un groupe de mise à jour de cluster vide pendant la découverte automatique ou la synchronisation

Lorsqu'un cluster est découvert dans OMIMSSC, un groupe de mise à jour de cluster est créé dans le **Centre de maintenance** avec tous les serveurs répertoriés dans le groupe de mise à jour de cluster. Plus tard, si tous les serveurs sont supprimés de ce cluster via SCVMM, et qu'une découverte automatique ou une synchronisation avec l'opération SCVMM est effectuée, le groupe de mise à jour de cluster vide n'est pas supprimé dans le **Centre de maintenance**.

Pour contourner ce problème, pour supprimer le groupe de serveurs vide, effectuez une nouvelle découverte des serveurs.

Impossible de créer un cluster lors de l'application des fonctionnalités de cluster

En cas d'échec de la création du cluster sur les nœuds lors de l'application des fonctionnalités de cluster, et le déploiement du système d'exploitation réussit. Lors de la création du cluster, un message d'erreur `Failed to install the features on hosts that are required for creating clusters` s'affiche et les journaux s'affichent, `Failed to run Pre Cluster Creation Scripts on Host Create Cluster`.

Pour contourner ce problème, assurez-vous que les **informations d'identification d'accès à l'ordinateur**, sélectionnées dans le **Profil d'ordinateur physique** utilisé pour la création du cluster, sont identiques à celles de l'utilisateur inscrit. L'utilisateur inscrit doit être un administrateur de domaine ou un utilisateur de domaine disposant des privilèges nécessaires pour ajouter le système au domaine.

Impossible de récupérer l'état de la tâche de mise à jour compatible adaptée au cluster

Lorsque l'état de la tâche de mise à jour adaptée est postérieur à l'achèvement de la tâche de mise à jour.

Pour contourner ce problème, vérifiez l'état de la tâche à l'aide de l'outil Microsoft Failover Cluster Manager et assurez-vous de supprimer les fichiers OMIMSSC créés dans le serveur SCVMM après la réalisation de la tâche.

Manquement à effectuer les tâches de maintenance sur les serveurs redécouverts

Lorsque vous supprimez un serveur ou tous les serveurs dans un groupe de mises à jour depuis OMIMSSC, et que vous les redécouvrez, vous ne pouvez pas effectuer d'autres opérations sur ces serveurs, comme la mise à jour de micrologiciel, l'exportation et l'importation de journaux LC, l'exportation et l'importation de profils de serveur.

Pour contourner ce problème, après avoir redécouvert le ou les serveurs supprimés, réalisez les mises à jour de firmware en utilisant la fonctionnalité **Déployer Modèle opérationnel** dans **Vue du serveur** et pour les autres scénarios de maintenance, utilisez iDRAC.

Scénarios génériques dans OMIMSSC

Cette section contient des informations de dépannage qui sont indépendantes des workflow dans OMIMSSC.

Échec d'accès au partage CIFS à l'aide du nom d'hôte

Les serveurs modulaires ne sont pas en mesure d'accéder au partage CIFS à l'aide du nom d'hôte pour effectuer une tâche dans OMIMSSC.

Pour contourner ce problème, spécifiez l'adresse IP du serveur possédant CIFS au lieu du nom d'hôte.

Erreur d'affichage de la page Tâches et journaux dans l'extension de console

La page **Centre des tâches et des journaux** ne s'affiche pas dans les extensions de console OMIMSSC.

Pour contourner ce problème, ré-inscrivez la console, puis lancez la page **Tâches et journaux**.

Échec des opérations sur les systèmes gérés

Toutes les fonctionnalités d'OMIMSSC n'agissent pas comme prévu sur les systèmes gérés, en raison d'une version de TLS (Transport Layer Security).

Si vous utilisez la version 2.40.40.40 du micrologiciel de l'iDRAC, ou ultérieure, alors la version 1.1 du protocole TLS (Transport Layer Security), ou ultérieure, est activée par défaut. Avant d'installer l'extension de la console, installez la mise à jour pour activer TLS 1.1 et versions ultérieures, comme mentionné dans l'article de la base de connaissances suivant : `Support.microsoft.com/en-us/kb/3140245`. Il est recommandé d'activer la prise en charge de TLS 1.1 ou versions ultérieures sur votre serveur et votre console SCVMM pour vous assurer qu'OMIMSSC fonctionne comme prévu. Pour de plus amples informations concernant iDRAC, consultez Dell.com/idracmanuals.

Échec du lancement de l'aide en ligne pour OMIMSSC

Lorsque vous utilisez le système d'exploitation Windows 2012 R2, le contenu de l'aide contextuelle en ligne est lancé et affiche un message d'erreur.

Pour résoudre ce problème, mettez à jour le système d'exploitation en utilisant les derniers articles de la base de connaissance, puis affichez le contenu de l'aide en ligne.

OMIMSSC Échec de tâches en raison d'un mot de passe de partage réseau non pris en charge

Certaines tâches OMIMSSC échouent car certains caractères spéciaux du mot de passe du partage réseau ne sont pas pris en charge par l'iDRAC.

Vous trouverez ci-dessous la liste des échecs de tâches et des messages d'erreur associés aux échecs de tâches respectifs :

- Échec de l'export de journaux LC - `Failed to Export Complete LC Logs from iDRAC IP <IP address> Cannot access network share`
- Impossible de déployer le système d'exploitation RHEL et ESXi - `Inaccessible network share`
- Échec de mise à jour du firmware à l'aide de DRM - `Firmware update failed on server with iDRAC IP <IP address> for <Component>`
- Échec du déploiement du système d'exploitation Windows - `Inaccessible network share for iDRAC <IP address>`
- Échec de l'exportation et de l'importation du profil du serveur - `Failed to invoke Export Server Profile on iDRAC IP: <iDRAC_IP> with error Cannot Access Network Share`

Pour contourner ce problème, assurez-vous d'utiliser le mot de passe de l'IDRAC recommandé pour le partage réseau. Pour plus d'informations, consultez la documentation d'iDRAC.

Scénarios de mise à jour de firmware dans OMIMSSC

Cette section contient toutes les informations de dépannage relatives aux sources de mise à jour, aux groupes de mise à jour, aux référentiels et à l'inventaire après les mises à jour.

Échec du test de connexion pour la source de mise à jour locale

Après avoir fourni les détails d'une source de mise à jour locale, le test de connexion risque d'échouer car les fichiers requis peuvent ne pas être accessibles.

Pour contourner ce problème, assurez-vous que le fichier `catalog.gz` est présent dans la structure de dossiers suivante :

- Pour la source de mise à jour DRM locale : `\\IP address\\catalog\<catalogfile>.gz`

Échec de la création d'une source de mise à jour DRM

La création d'une source de mise à jour DRM sur le serveur de gestion s'exécutant sur Windows 10 risque d'échouer, affichant le message d'erreur suivant : `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Reportez-vous au journal **omimsscappliance_main** du portail d'administration d'OMIMSSC, si le message d'erreur affiché est le suivant : *`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

Pour contourner ce problème, reportez-vous à l'article de la base de connaissance suivant : *support.microsoft.com/en-us/help/4034314*

Impossible de créer un référentiel au cours d'une mise à jour du micrologiciel

La création d'un référentiel peut échouer pendant une mise à jour du micrologiciel en raison de références incorrectes fournies lors de la création d'une source de mise à jour, ou lorsque l'appliance OMIMSSC ne parvient pas à accéder à la source de mise à jour.

Pour contourner ce problème, assurez-vous que la source de la mise à jour est accessible depuis l'emplacement dans lequel l'appliance OMIMSSC est hébergée, et fournissez les références correctes lors de la création d'une source de mise à jour.

Échec de mise à jour de firmware de clusters

Après la soumission d'une tâche dans OMIMSSC pour mettre à jour le firmware de clusters, les clusters ne sont pas mis à jour pour certaines raisons affichant les messages d'erreur suivants dans les **Journaux d'activité**.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

REMARQUE : Les actions de mise à jour adaptée aux clusters sont journalisées aux emplacements suivants : dossier \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports dans lequel le rapport de mise à jour adaptée aux clusters sera stocké. Le dossier \\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log contiendra en plus les journaux du plug-in Dell EMC System Update (DSU) pour chaque nœud. Les journaux de script étendus sont disponibles à l'emplacement C:\Window\Temp, qui comprend les fichiers precau.log et postcau.log dans chaque nœud du cluster pour le cluster HCI de serveur Windows.

Motifs d'échec de la mise à jour de firmware sur des clusters avec la solution suivante :

- Si les fichiers de catalogue et les DUP requis ne sont pas présents dans la source de mise à jour locale sélectionnée.

  Pour contourner ce problème, assurez-vous que tous les fichiers de catalogue et DUP requis sont disponibles dans les référentiels, puis mettez à jour le firmware des clusters.

- Le groupe cluster ne répond plus ou la tâche de mise à jour de firmware est annulée dans CAU en raison d'une tâche en cours, les DUP sont alors téléchargés et placés dans chaque nœud de cluster de serveur appartenant au groupe de cluster.

  Pour résoudre ce problème, supprimez tous les fichiers qui figurent dans le dossier Dell, puis planifiez une tâche de mise à jour de firmware de clusters.

- Si le Lifecycle Controller (LC) est occupé avec d'autres opérations, la tâche de mise à jour de firmware sur un nœud de cluster échoue. Pour vérifier si la mise à jour a échoué parce que de LC est occupé, recherchez le message d'erreur dans chaque nœud du cluster au chemin suivant : `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then
  reboot the system.
  ```

  Pour contourner ce problème, arrêtez le serveur, retirez les câbles d'alimentation, puis redémarrez le serveur. Après le redémarrage, mettez à jour le firmware sur les clusters.

REMARQUE : Pour plus d'informations sur l'échec de la CAU, vérifiez l'état de la tâche de CAU dans l'outil du gestionnaire de cluster de basculement de Microsoft et reportez-vous à la section des pratiques d'excellence sur la mise à jour adaptée aux clusters de la documentation Microsoft.

Impossible de mettre à jour le micrologiciel car la file d'attente des tâches est pleine

La tâche de mise à jour de micrologiciel envoyée à partir d'OMIMSSC vers iDRAC échoue, et le journal OMIMSSC principal affiche l'erreur suivante : `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

Pour contourner ce problème, supprimez manuellement les tâches terminées dans iDRAC, puis relancez la tâche de mise à jour de micrologiciel. Pour plus d'informations sur la suppression de tâches dans iDRAC, reportez-vous à la documentation iDRAC à l'adresse **dell.com/support/home**.

Échec de mise à jour de firmware en utilisant une source de mise à jour DRM

La tâche de mise à jour de firmware peut échouer si vous utilisez la source de mise à jour DRM avec un accès insuffisant aux dossiers de partage. Si le profil de référence Windows fourni lors de la création de source de mise à jour DRM ne fait pas partie du groupe d'administrateur de domaine ou du groupe d'administrateur local, le message d'erreur suivant s'affiche : `Local cache creation failure`.

Pour résoudre le problème, procédez comme suit :

1. Après la création du référentiel dans DRM, effectuez un clic-droit sur le dossier, cliquez sur l'onglet **Sécurité**, puis cliquez sur **Avancé**.
2. Cliquez sur **Activer l'héritage** et sélectionnez l'option **Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet**, puis partager le dossier avec **Tout le monde** avec une autorisation de lecture/en écriture.

Mise à jour de firmware de quelques composants, quelle que soit la sélection

Les mêmes composants sur des serveurs identiques sont mis à jour lors de la mise à jour d'un firmware, quelle que soit la sélection des composants sur ces serveurs individuels. Ce comportement est observé pour la 12e et la 13e génération de serveurs PowerEdge avec une licence Enterprise d'iDRAC.

Pour contourner le problème, effectuez l'une des opérations suivantes :

- Commencez par appliquer les mises à jour pour les composants communs sur des serveurs identiques, puis appliquez-les aux composants spécifiques sur des serveurs individuels.
- Effectuez des mises à jour préparées avec heure de coupure planifiée pour gérer la mise à jour de firmware requise.

Échec de la suppression d'un groupe de mise à jour personnalisée

Après avoir planifié une tâche sur un serveur appartenant à un groupe de mise à jour personnalisée, si le serveur est supprimé de la console Microsoft et que vous synchronisez la console Microsoft enregistrée avec OMIMSSC, le serveur est retiré du groupe de mise à jour personnalisée et est déplacé vers un groupe de mise à jour prédéfini. Vous ne pouvez pas supprimer un tel groupe de mise à jour personnalisée, car il est associé à une tâche planifiée.

Pour résoudre ce problème, supprimez la tâche planifiée de la page **Tâches et journaux**, puis supprimez le groupe de mise à jour personnalisée.

Échec de mise à jour de l'image WinPE

Lorsque vous essayez de mettre à jour l'image WinPE, la tâche de mise à jour peut échouer avec le message d'erreur suivant : `Remote connection to console failed.`

Pour éviter cet incident, exécutez la commande **DISM** pour nettoyer toutes les images montées précédemment dans la console Microsoft, puis réessayez de mettre à jour l'image WinPE.

Modification de la couleur de cloche d'interrogation et de notification après mise à jour de la fréquence

Si un serveur géré n'est pas découvert dans OMIMSSC, et que vous modifiez la fréquence de l'option d'interrogation et de notification, la cloche devient jaune au bout d'un moment, même s'il n'y a pas de modifications dans le catalogue.

Pour contourner ce problème, découvrez les serveurs gérés, puis modifiez la fréquence de l'option d'interrogation et de notification.

Scénarios de déploiement de système d'exploitation dans OMIMSSC

Cette section contient toutes les informations de dépannage relatives au déploiement du système d'exploitation ou de l'hyperviseur (pour SCVMM) en utilisant le modèle opérationnel dans OMIMSSC.

Scénarios génériques de déploiement du système d'exploitation

Cette section contient toutes les informations sur le dépannage générique liées au déploiement du système d'exploitation.

Échec du déploiement du modèle opérationnel

Après le déploiement du modèle opérationnel sur les serveurs sélectionnés, les attributs ou les valeurs d'attribut sélectionnés ne sont pas appropriés pour le fichier .CSV sélectionné, ou l'adresse IP iDRAC ou les références d'iDRAC sont modifiées en raison des configurations dans le modèle. La tâche dans iDRAC est réussie, cependant elle affiche l'état de réussite ou d'échec dans OMIMSSC à cause d'un fichier .CSV non valide, ou la tâche ne peut pas être suivie en raison de modifications apportées à iDRAC sur le serveur cible.

Pour contourner ce problème, assurez-vous que le fichier .CSV sélectionné dispose des attributs et valeurs d'attributs correctes, et que les références ou l'adresse IP iDRAC ne changent pas en raison des configurations dans le modèle.

Échec de l'enregistrement d'un modèle opérationnel

Lorsque vous créez un modèle opérationnel, si vous cochez et décochez une case d'attribut indépendant possédant une valeur de pool, vous ne pouvez pas enregistrer le modèle opérationnel avec le message d'erreur suivant :

```
Select atleast one attribte, under the selected components, before creating the Operational Template.
```

Pour contourner ce problème, procédez de l'une des manières suivantes :

- Sélectionnez un autre attribut dépendant ayant une valeur de pool ou le même attribut dépendant et enregistrez le modèle opérationnel.
- Créez un nouveau modèle opérationnel.

Échec du déploiement du système d'exploitation de Windows Server 2016 sur les serveurs AMD

Le déploiement du système d'exploitation de Windows Server 2016 sur les plates-formes AMD ne prend pas en charge x2apic. Par conséquent, le déploiement du système d'exploitation échoue.

Pour contourner ce problème, modifiez le modèle opérationnel utilisé pour le déploiement, sélectionnez le composant BIOS, puis désactivez les paramètres du BIOS x2apic et du processeur logique. Recommencez ensuite le déploiement à l'aide de ce modèle. Pour plus d'informations, reportez-vous à l'article de la base de connaissances Le serveur AMD Dell EMC se bloque sur le logo Windows lors de l'installation de Windows Server 2016.

Scénarios de déploiement de système d'exploitation pour les utilisateurs MECM

Cette section contient toutes les informations de dépannage relatives au déploiement de système d'exploitation à l'aide d'OMIMSSC dans la console MECM.

Option de déploiement non visible dans la séquence de tâches

L'option **Déployer** ne s'affiche pas dans une séquence de tâches existante après la désinstallation et la réinstallation de l'extension de console OMIMSSC pour MECM.

Pour contourner ce problème, ouvrez la séquence de tâches pour la modifier, réactivez l'option **Appliquer**, puis cliquez sur **OK**. L'option **Déployer** s'affiche à nouveau.

Pour réactiver l'option **Appliquer** :

1. Cliquez avec le bouton droit sur la séquence de tâches et sélectionnez **Modifier**.
2. Sélectionnez **Redémarrer dans Windows PE**. Dans la section **Description**, tapez un caractère quelconque et supprimez-le pour que la modification ne soit pas enregistrée.
3. Cliquez sur **OK**.

   L'option **Appliquer** est alors réactivée.

Échec de l'ajout de serveurs dans la collecte Managed Lifecycle Controller Lifecycle Controller ESXi dans MECM

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

Pour résoudre ce problème, installez le serveur client MECM, puis effectuez une synchronisation pour ajouter les serveurs dans la collecte Managed Lifecycle Controller Lifecycle Controller (ESXi).

Échec du déploiement du système d'exploitation Windows sur les serveurs PowerEdge basés sur l'iDRAC 9

Le déploiement du système d'exploitation Windows échoue sur les serveurs PowerEdge basés sur l'iDRAC 9, qui sont en mode de démarrage UEFI.

Pour contourner ce problème, ajoutez un retard dans le fichier Winpeshl. ini, qui se trouve dans C:\Program Files\Microsoft Configuration Manager\OSD\bin\x64. Pour plus d'informations, reportez-vous à la section suivante de la communauté Microsoft : *OS Deployment - Unable to read task sequence, Wpelnit.exe does not start automatically* (Déploiement SE - Impossible de lire la séquence de tâches, Wpelnit.exe ne démarre pas automatiquement).

Scénarios de déploiement de système d'exploitation pour les utilisateurs SCVMM

Cette section contient toutes les informations de dépannage relatives au déploiement de l'hyperviseur à l'aide d'OMIMSSC dans la console SCVMM.

Échec de déploiement d'hyperviseur en raison de LC ou de protection de pare-feu

Le déploiement de l'hyperviseur ne parvient pas à afficher le message d'erreur suivant dans le journal d'activités : `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

Cette erreur peut survenir pour l'une des raisons suivantes :

- Le Dell Lifecycle Controller est défectueux.

  Pour résoudre le problème, connectez-vous à l'interface utilisateur de l'iDRAC et réinitialisez le Lifecycle Controller.

  Si le problème persiste une fois le Lifecycle Controller réinitialisé, essayez l'une des alternatives suivantes :

- Il est possible que vous ne puissiez pas exécuter correctement la commande `WINRM` en raison d'un antivirus ou d'un pare-feu.

  Reportez-vous à l'article de la base de connaissances suivant pour contourner le problème : `support.microsoft.com/kb/961804`

Échec du déploiement de l'hyperviseur car il reste des fichiers de pilote dans le partage de bibliothèque

Le déploiement de l'hyperviseur ne parvient pas à afficher le message d'erreur suivant dans le journal d'activités :

- **Error** : `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information** : `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
- **Error** : `Deleting staging share (drivers) for <server uuid> failed.`

Ces erreurs peuvent se produire en raison d'une exception émise par la commande VMM `GET-SCJOB status` et les fichiers de pilote se trouvant dans le partage de bibliothèque. Avant de retenter l'opération ou d'effectuer un autre déploiement de l'hyperviseur, vous devez supprimer ces fichiers du partage de bibliothèque.

Pour supprimer des fichiers du partage de bibliothèque : vous pouvez ensuite déployer les hyperviseurs.

1. Dans la console SCVMM, sélectionnez **Bibliothèque** > **Serveurs de bibliothèque**, puis cliquez sur le serveur IG qui a été ajouté en tant que serveur de bibliothèque.
2. Dans le serveur de bibliothèque, sélectionnez et supprimez le partage de bibliothèque.
3. Une fois le partage de bibliothèque supprimé, connectez-vous au partage IG en utilisant `\\<Integration Gateway server>\LCDriver\`.
4. Supprimez le dossier contenant les fichiers de pilote.

Erreur SCVMM numéro 21119 pendant l'ajout de serveurs à Active Directory

Lors de l'ajout de serveurs à Active Directory, l'erreur 21119 SCVMM s'affiche. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

Pour résoudre le problème, procédez comme suit :

1. Patientez quelques instants pour voir si le serveur est ajouté à Active Directory.
2. Si le serveur n'est pas ajouté à Active Directory, puis ajouter-le manuellement.
3. Ajoutez le serveur à SCVMM.
4. Une fois le serveur ajouté à SCVMM, effectuez une nouvelle découverte du serveur dans OMIMSSC.

   Le serveur est désormais répertorié dans l'onglet **Hôte**.

Scénarios de création de clusters HCI de serveurs Windows pour les utilisateurs SCVMM

Cette section contient toutes les informations de dépannage associées à la création de clusters HCI de serveurs Windows à l'aide d'OMIMSSC dans la console SCVMM.

L'état d'intégrité du cluster HCI de serveurs Windows est inconnu

Lorsque vous créez un cluster HCI de serveurs Windows sur les nœuds qui faisaient partie d'un cluster existant, alors les configurations du disque et du pool de stockage correspondent à celles du cluster existant. Par conséquent, le pool de stockage du cluster peut ne pas être créé et, si le pool de stockage du cluster est créé, l'état d'intégrité peut s'afficher comme inconnu.

Pour contourner ce problème, effacez la configuration du disque et du pool de stockage possédant les détails du cluster existant, puis créez le cluster HCI de serveurs Windows. Pour plus d'informations sur la suppression du contenu du pool de stockage, reportez-vous à la section *Troubleshoot Windows server HCI health and operational states (Dépannage des problèmes liés aux états opérationnels et à l'intégrité du cluster HCI de serveurs Windows)* de la documentation Microsoft.

Scénarios de profil de serveur dans OMIMSSC

Cette section contient toutes les informations de dépannage liées à l'exportation et l'importation des profils de serveur dans OMIMSSC.

Échec de l'exportation des profils de serveur

Après la planification d'une tâche d'exportation de profil de serveur, le profil de serveur n'est pas exporté et le message d'erreur suivant s'affiche : `The selectors for the resource are not valid.`

Pour contourner ce problème, réinitialisez iDRAC, puis planifiez la tâche d'exportation de profil de serveur. Pour plus d'informations, consultez la documentation d'iDRAC disponible sur `dell.com/support`.

L'importation d'une tâche de profil de serveur expire au bout de deux heures

Après la soumission de la tâche d'importation du profil du serveur dans OMIMSSC, cette tâche peut expirer au bout de deux heures.

Pour résoudre ce problème, procédez comme suit :

1. Démarrez le serveur, appuyez sur F2, puis entrez les **Paramètres du BIOS**.
2. Cliquez sur **Configuration du système** et sélectionnez **Paramètres divers**.
3. Désactivez **Invite F1/F2 en cas d'erreur**.

Après avoir effectué les étapes suivantes, exportez à nouveau le profil de serveur et utilisez le même profil de serveur pour l'importer sur ce serveur.

Scénarios de journaux LC dans OMIMSSC

Cette section contient toutes les informations de dépannage liées à l'exportation et l'affichage des journaux LC.

Échec de l'exportation des journaux LC au format .CSV

Lorsque vous essayez de télécharger les fichiers journaux LC au format . CSV, l'opération de téléchargement échoue.

Pour contourner ce problème, ajoutez le FQDN de l'appliance OMIMSSC dans le navigateur sous le site intranet local. Pour plus d'informations sur l'ajout de l'appliance OMIMSSC dans l'intranet local, reportez-vous à la section *Affichage des journaux LC* dans *Guide unifié de l'utilisateur de Dell EMC OpenManage Integration pour Microsoft System Center Version 7.3 pour Microsoft Endpoint Configuration Manager et System Center Virtual Machine Manager*.

Échec de l'ouverture de fichiers journaux LC

Après avoir collecté les journaux LC, lorsque vous essayez d'afficher le fichier journal LC pour un serveur, le message d'erreur suivant s'affiche : `"Failed to perform the requested action. For more information see the activity log"`.

Pour contourner ce problème, réinitialisez iDRAC, puis collectez et affichez les journaux LC. Pour plus d'informations sur la réinitialisation d'iDRAC, reportez-vous à la documentation iDRAC disponible à l'adresse `Dell.com/support`.

Échec du test de connexion

Si les noms d'utilisateur sont identiques mais que les mots de passe sont différents pour le compte d'utilisateur de domaine et le compte d'utilisateur local, alors le test de la connexion entre la console Microsoft et l'appliance OMIMSSC échoue.

Par exemple, le compte d'utilisateur de domaine est `domain\user1` et le mot de passe est `pwd1`. Et compte d'utilisateur local est `user1` et le mot de passe est `Pwd2`. Lorsque vous essayez de vous inscrire avec le compte d'utilisateur de domaine ci-dessus, le test de connexion échoue.

Pour contourner ce problème, utilisez des noms d'utilisateurs différents pour les comptes d'utilisateur de domaine et local, ou utilisez un compte d'utilisateur unique en tant qu'utilisateur local et lors de l'inscription à la console Microsoft dans l'appliance OMIMSSC.

22

Annexe I : valeurs des attributs de fuseau horaire

Fournissez les valeurs d'attribut de fuseau horaire manuellement dans les périphériques Mx7000 en vous reportant au tableau ci-dessous :

Tableau 12. Détails des fuseaux horaires

ID de fuseau horaire	Différence du fuseau horaire
TZ_ID_1	(GMT-12h00) Ligne de date internationale Ouest
TZ_ID_2	(GMT+14h00) Samoa
TZ_ID_3	(GMT-10h00) Hawaï
TZ_ID_4	(GMT-09h00) Alaska
TZ_ID_5	(GMT-08h00) Heure du Pacifique (États-Unis et Canada)
TZ_ID_6	(GMT-08h00) Basse-Californie
TZ_ID_7	(GMT-07h00) Arizona
TZ_ID_8	(GMT-07h00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07h00) Heure des Rocheuses (États-Unis et Canada)
TZ_ID_10	(GMT-06h00) Amérique centrale
TZ_ID_11	(GMT-06h00) Heure du Centre (États-Unis et Canada)
TZ_ID_12	(GMT-06h00) Guadalajara, Mexico, Monterrey
TZ_ID_13	(GMT-06h00) Saskatchewan
TZ_ID_14	(GMT-05h00) Bogota, Lima, Quito
TZ_ID_15	(GMT-05h00) Heure de l'Est (États-Unis et Canada)
TZ_ID_16	(GMT-05h00) Indiana (Est)
TZ_ID_17	(GMT-04h30) Caracas
TZ_ID_18	(GMT-04h00) Asuncion
TZ_ID_19	(GMT-04h00) Heure de l'Atlantique (Canada)
TZ_ID_20	(GMT-04h00) Cuiaba
TZ_ID_21	(GMT-04h00) Georgetown, La Paz, Manaus, San Juan
TZ_ID_22	(GMT-04h00) Santiago
TZ_ID_23	(GMT-03h30) Terre-Neuve
TZ_ID_24	(GMT-03h00) Brasilia
TZ_ID_25	(GMT-03h00) Buenos Aires
TZ_ID_26	(GMT-03h00) Cayenne, Fortaleza
TZ_ID_27	(GMT-03h00) Groenland
TZ_ID_28	(GMT-03h00) Montevideo
TZ_ID_29	(GMT-02h00) Centre du littoral atlantique

Tableau 12. Détails des fuseaux horaires (suite)

ID de fuseau horaire	Différence du fuseau horaire
TZ_ID_30	(GMT-01h00) Açores
TZ_ID_31	(GMT-01h00) Cap-Vert
TZ_ID_32	(GMT+00h00) Casablanca
TZ_ID_33	(GMT+00h00) Temps universel coordonné
TZ_ID_34	(GMT+00h00) Dublin, Édimbourg, Lisbonne, Londres
TZ_ID_35	(GMT+00h00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01h00) Amsterdam, Berlin, Berne, Rome, Stockholm, Vienne
TZ_ID_37	(GMT+01h00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
TZ_ID_38	(GMT+01h00) Bruxelles, Copenhague, Madrid, Paris
TZ_ID_39	(GMT+01h00) Sarajevo, Skopje, Varsovie, Zagreb
TZ_ID_40	(GMT+01h00) Afrique centrale occidentale
TZ_ID_41	(GMT+02h00) Windhoek
TZ_ID_42	(GMT+02h00) Amman
TZ_ID_43	(GMT+03h00) Istanbul
TZ_ID_44	(GMT+02h00) Beyrouth
TZ_ID_45	(GMT+02h00) Le Caire
TZ_ID_46	(GMT+02h00) Damas
TZ_ID_47	(GMT+02h00) Harare, Pretoria
TZ_ID_48	(GMT+02h00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
TZ_ID_49	(GMT+02h00) Jérusalem
TZ_ID_50	(GMT+02h00) Minsk
TZ_ID_51	(GMT+03h00) Bagdad
TZ_ID_52	(GMT+03h00) Koweït, Riyad
TZ_ID_53	(GMT+03h00) Moscou, Saint- Pétersbourg, Volgograd
TZ_ID_54	(GMT+03h00) Nairobi
TZ_ID_55	(GMT+03h30) Téhéran
TZ_ID_56	(GMT+04h00) Abou Dabi, Muscat
TZ_ID_57	(GMT+04h00) Bakou
TZ_ID_58	(GMT+04h00) Port-Louis
TZ_ID_59	(GMT+04h00) Tbilissi
TZ_ID_60	(GMT+04h00) Erevan
TZ_ID_61	(GMT+04h30) Kaboul
TZ_ID_62	(GMT+05h00) Iekaterinbourg
TZ_ID_63	(GMT+05h00) Islamabad, Karachi
TZ_ID_64	(GMT+05h00) Tachkent
TZ_ID_65	(GMT+05h30) Chennai, Calcutta, Mumbai, New Delhi
TZ_ID_66	(GMT+05h30) Sri Jayawardenapura

Tableau 12. Détails des fuseaux horaires (suite)

ID de fuseau horaire	Différence du fuseau horaire
TZ_ID_67	(GMT+05h45) Katmandou
TZ_ID_68	(GMT+06h00) Astana
TZ_ID_69	(GMT+06h00) Dhaka
TZ_ID_70	(GMT+06h00) Novosibirsk
TZ_ID_71	(GMT+06h30) Yangon (Rangoun)
TZ_ID_72	(GMT+07h00) Bangkok, Hanoï, Jakarta
TZ_ID_73	(GMT+07h00) Krasnoïarsk
TZ_ID_74	(GMT+08h00) Pékin, Chongqing, Hong Kong, Ürümqi
TZ_ID_75	(GMT+08h00) Irkoutsk
TZ_ID_76	(GMT+08h00) Kuala Lumpur, Singapour
TZ_ID_77	(GMT+08h00) Perth
TZ_ID_78	(GMT+08h00) Taipei
TZ_ID_79	(GMT+08h00) Oulan-Bator
TZ_ID_80	(GMT+08h30) Pyongyang
TZ_ID_81	(GMT+09h00) Osaka, Sapporo, Tokyo
TZ_ID_82	(GMT+09h00) Séoul
TZ_ID_83	(GMT+09h00) Iakoutsk
TZ_ID_84	(GMT+09h30) Adélaïde
TZ_ID_85	(GMT+09h30) Darwin
TZ_ID_86	(GMT+10h00) Brisbane
TZ_ID_87	(GMT+10h00) Canberra, Melbourne, Sydney
TZ_ID_88	(GMT+10h00) Guam, Port Moresby
TZ_ID_89	(GMT+10h00) Hobart
TZ_ID_90	(GMT+10h00) Vladivostok
TZ_ID_91	(GMT+11h00) Magadan, Îles Salomon, Nouvelle-Calédonie
TZ_ID_92	(GMT+12h00) Auckland, Wellington
TZ_ID_93	(GMT+12h00) Fidji
TZ_ID_94	(GMT+13h00) Nuku'alofa
TZ_ID_95	(GMT+14h00) Kiritimati
TZ_ID_96	(GMT+02h00) Athènes, Bucarest

23

Annexe II : renseigner les valeurs de pool

Remplissez le fichier CSV de la valeur du pool.

Tableau 13. Format du fichier de valeur du pool

serviceTag(renseigné automatiquement)	FQDD(renseigné automatiquement)	poolAttributeName	poolAtrributeValue
Numéro de série du ou des périphériques à partir desquels les attributs spécifiques du système sont exportés	Identifie le composant associé à l'attribut spécifique du système	Identifie l'attribut spécifique du système à configurer	Définir la valeur de l'attribut spécifique au système spécifié

Tableau 14. Valeurs propres au système pour le composant matériel

Composant	Nom de groupe	Nom de l'attribut
BIOS	Miscellaneous Settings (Paramètres divers)	Numéro d'inventaire
BIOS	Paramètres de la connexion 1	Passerelle de l'initiateur
BIOS	Paramètres de la connexion 1	Adresse de l'initiateur IP
BIOS	Paramètres de la connexion 1	Masque de sous-réseau de l'initiateur
BIOS	Paramètres de la connexion 1	Adresse IP cible
BIOS	Paramètres de la connexion 1	Nom de la cible
BIOS	Paramètres de la connexion 2	Passerelle de l'initiateur
BIOS	Paramètres de la connexion 2	Adresse de l'initiateur IP
BIOS	Paramètres de la connexion 2	Masque de sous-réseau de l'initiateur
BIOS	Paramètres de la connexion 2	Adresse IP cible
BIOS	Paramètres de la connexion 2	Nom de la cible
BIOS	Paramètres réseau	Nom de l'initiateur iSCSI
BIOS	Integrated Devices (Périphériques intégrés)	Carte réseau intégrée 1 liaison PCIe Link1
BIOS	Integrated Devices (Périphériques intégrés)	Carte réseau intégrée 1 liaison PCIe Link2
BIOS	Integrated Devices (Périphériques intégrés)	Carte réseau intégrée 1 liaison PCIe Link3
iDRAC	Informations NIC	Nom du RAC DNS
iDRAC	Informations NIC	Activer le VLAN
iDRAC	Informations NIC	ID du VLAN
iDRAC	Informations sur IPv4	Activation IPv4
iDRAC	Informations sur IPv4	Activer l'interruption DHCP du contrôleur IPv4
iDRAC	Informations IPv6	Activation IPV6
iDRAC	Informations IPv6	Autoconfiguration d'IPv6
iDRAC	Topologie de serveurs	Nom du datacenter
iDRAC	Topologie de serveurs	Nom de l'allée

Tableau 14. Valeurs propres au système pour le composant matériel (suite)

Composant	Nom de groupe	Nom de l'attribut
iDRAC	Topologie de serveurs	Nom du rack
iDRAC	Topologie de serveurs	Logement de rack
iDRAC	Active Directory	Nom RAC Active Directory
iDRAC	Informations statiques sur le certificat NIC	Nom de domaine DNS
iDRAC	Informations statiques sur IPv4	Adresse IPv4
iDRAC	Informations statiques sur IPv4	Masque réseau
iDRAC	Informations statiques sur IPv4	Passerelle
iDRAC	Informations statiques sur IPv4	Serveur DNS 1
iDRAC	Informations statiques sur IPv4	Serveur DNS 2
iDRAC	Informations statiques sur IPv6	Adresse IPv6 1
iDRAC	Informations statiques sur IPv6	Passerelle IPv6
iDRAC	Informations statiques sur IPv6	Longueur de préfixe local de liaison IPv6
iDRAC	Informations statiques sur IPv6	Serveur DNS IPV6 1
iDRAC	Informations statiques sur IPv6	Serveur DNS IPV6 2
iDRAC	Système d'exploitation du serveur	Nom de l'hôte du serveur
iDRAC	Topologie de serveurs	Nom de la pièce
iDRAC	Informations NIC	Nom du RAC DNS
iDRAC	Informations NIC	Nom du RAC DNS
iDRAC	Informations sur IPv4	Activer l'interruption DHCP du contrôleur IPv4
iDRAC	Informations statiques sur IPv4	Adresse IPv4
iDRAC	Informations statiques sur IPv4	Masque réseau
iDRAC	Informations statiques sur IPv4	Passerelle
iDRAC	Informations statiques sur IPv4	Serveur DNS 1
iDRAC	Informations statiques sur IPv4	Serveur DNS 2
iDRAC	Informations statiques sur IPv6	Passerelle IPv6
iDRAC	Informations statiques sur IPv6	Longueur de préfixe local de liaison IPv6
iDRAC	Informations statiques sur IPv6	Serveur DNS 1
iDRAC	Informations statiques sur IPv6	Serveur DNS 2
Réseau	Paramètres généraux iSCSI	Authentification mutuelle CHAP
Réseau	Paramètres de la première cible iSCSI	Se connecter
Réseau	Paramètres de la deuxième cible iSCSI	Se connecter
Réseau	Paramètres de la première cible iSCSI	Numéro d'unité logique d'amorçage
Réseau	Paramètres de la première cible iSCSI	ID CHAP
Réseau	Paramètres de la première cible iSCSI	CHAP Secret (Secret CHAP)
Réseau	Paramètres de la première cible iSCSI	Adresse IP
Réseau	Paramètres de la première cible iSCSI	Nom iSCSI
Réseau	Paramètres de la première cible iSCSI	Port TCP

Tableau 14. Valeurs propres au système pour le composant matériel (suite)

Composant	Nom de groupe	Nom de l'attribut
Réseau	Paramètres de l'initiateur iSCSI	ID CHAP
Réseau	Paramètres de l'initiateur iSCSI	CHAP Secret (Secret CHAP)
Réseau	Paramètres de l'initiateur iSCSI	Passerelle par défaut
Réseau	Paramètres de l'initiateur iSCSI	Adresse IP
Réseau	Paramètres de l'initiateur iSCSI	Adresse IPv4
Réseau	Paramètres de l'initiateur iSCSI	Passerelle IPv4 par défaut
Réseau	Paramètres de l'initiateur iSCSI	DNS principal IPv4
Réseau	Paramètres de l'initiateur iSCSI	DNS secondaire IPv4
Réseau	Paramètres de l'initiateur iSCSI	Adresse IPv6
Réseau	Paramètres de l'initiateur iSCSI	Passerelle IPv6 par défaut
Réseau	Paramètres de l'initiateur iSCSI	DNS principal IPv6
Réseau	Paramètres de l'initiateur iSCSI	DNS secondaire IPv6
Réseau	Paramètres de l'initiateur iSCSI	Nom iSCSI
Réseau	Paramètres de l'initiateur iSCSI	DNS principal
Réseau	Paramètres de l'initiateur iSCSI	DNS secondaire
Réseau	Paramètres de l'initiateur iSCSI	Masque de sous-réseau
Réseau	Paramètres de l'initiateur iSCSI	Préfixe du masque de sous-réseau
Réseau	Paramètres de l'unité iSCSI secondaire	Adresse MAC de l'unité secondaire
Réseau	Paramètres de la deuxième cible iSCSI	Numéro d'unité logique d'amorçage
Réseau	Paramètres de la deuxième cible iSCSI	CHAP Secret (Secret CHAP)
Réseau	Paramètres de la deuxième cible iSCSI	ID CHAP
Réseau	Paramètres de la deuxième cible iSCSI	Adresse IP
Réseau	Paramètres de la deuxième cible iSCSI	Nom iSCSI
Réseau	Paramètres de la deuxième cible iSCSI	Port TCP
Réseau	Paramètres de l'unité iSCSI secondaire	Utiliser un nom de cible indépendant
Réseau	Paramètres de l'unité iSCSI secondaire	Utiliser un portail cible indépendant
Réseau	Page principale de configuration	Adresse MAC FIP virtuelle
Réseau	Page principale de configuration	Adresse MAC du déchargement iSCSI virtuel
Réseau	Page principale de configuration	Adresse MAC virtuelle
Réseau	Configuration n Partition	Adresse MAC virtuelle
Réseau	Page principale de configuration	GUID de port virtuel
Réseau	Page principale de configuration	Nom du nœud universel virtuel
Réseau	Configuration n Partition	Nom du nœud universel virtuel
Réseau	Page principale de configuration	Nom du port universel virtuel
Réseau	Configuration n Partition	Nom du port universel virtuel
Réseau	Page principale de configuration	Nom du nœud universel
Réseau	Configuration n Partition	Nom du nœud universel

Tableau 14. Valeurs propres au système pour le composant matériel (suite)

Composant	Nom de groupe	Nom de l'attribut
FC	Configuration des cibles Fibre Channel	Sélection d'analyse du démarrage
FC	Configuration des cibles Fibre Channel	LUN de la première cible FC
FC	Configuration des cibles Fibre Channel	Nom de port universel de la première cible FC
FC	Configuration des cibles Fibre Channel	LUN de la deuxième cible FC
FC	Configuration des cibles Fibre Channel	Nom de port universel de la deuxième cible FC
FC	Page Configuration du port	Nom du nœud universel virtuel
FC	Page Configuration du port	Nom du port universel virtuel
Module de gestion pour les châssis MX	ChassisLocation	Datacenter
Module de gestion pour les châssis MX	ChassisLocation	Salle
Module de gestion pour les châssis MX	ChassisLocation	Allée
Module de gestion pour les châssis MX	ChassisLocation	Rack
Module de gestion pour les châssis MX	ChassisLocation	Logement de rack
Module de gestion pour les châssis MX	ChassisLocation	Emplacement

Tableau 15. Valeurs propres au système pour le composant Windows

serviceTag(renseigné automatiquement)	FQDD(renseigné automatiquement)	poolAttributeName	poolAtrributeValue	Détails sur l'attribut et la façon de le remplir
xxxxxxx	WINDOWS	HOSTNAME	WIN19SRVDTA	Quoi : il s'agit du nom de l'hôte à définir sur le serveur déployé/provisionné.
xxxxxxx	WINDOWS	ServerMngNIC	<MAC Adresses>	Quoi : il s'agit de l'adresse MAC du port réseau qui peut communiquer avec le centre de systèmes et l'appliance OMMISSC. Comment : récupérer l'adresse MAC de l'iDRAC en naviguant vers un port spécifique.
xxxxxxx	WINDOWS	LOGICALNETWORK	OSD UTILISANT UNE IP STATIQUE	Quoi : il s'agit du profil de réseau créé dans SCVMM qui transporte le pool d'IP statiques, le sous-réseau et d'autres détails de réseau à appliquer sur MN. Comment : créer le profil réseau logique dans SCVMM et fournir le nom du modèle créé. Pour plus d'informations, reportez-vous à la section Planifier la structure de réseau VMM de la documentation Microsoft.
xxxxxxx	WINDOWS	IPSUBNET	100.100.28.0/22	Quoi : il s'agit du masque de sous-réseau pour l'entrée statique du pool d'IP dans le profil de réseau logique ci-dessus.
xxxxxxx	WINDOWS	IPADDRESS	100.100.31.145	Quoi : il s'agit de l'IP statique à appliquer sur le nœud géré déployé/provisionné.

Tableau 16. Valeurs propres au système pour un composant non-Windows

serviceTag(renseigné automatiquement)	FQDD(renseigné automatiquement)	poolAttributeName	poolAtrributeValue	Détails sur l'attribut et la façon de le remplir
xxxxxxx	LINUX	HOSTNAME	<Nom de l'hôte>	Quoi : il s'agit du nom de l'hôte à définir sur le serveur déployé/provisionné.
xxxxxxx	LINUX	IPADDRESS	<Adresse IP statique>	Quoi : il s'agit de l'IP statique à appliquer sur le nœud géré déployé/provisionné.
xxxxxxx	LINUX	SUBNETMASK	<Masque de sous-réseau>	Quoi : le masque de sous-réseau pour le pool d'adresses IP statiques
xxxxxxx	LINUX	DEFAULTGATEWAY	<Passerelle par défaut>	Quoi : la passerelle par défaut
xxxxxxx	LINUX	PRIMARYDNSSERVER	<Serveur DNS primaire>	Quoi : serveur DNS primaire
xxxxxxx	LINUX	SECONDARYDNSSERVER	<Serveur DNS secondaire>	Quoi : serveur DNS secondaire

24

Accès au contenu de support à partir du site de support Dell EMC

Accédez au contenu de support lié à un ensemble d'outils de gestion de systèmes à l'aide de liens directs, en accédant au site de support Dell EMC, ou à l'aide d'un moteur de recherche.

- Liens directs :
  - Pour la gestion des systèmes Dell EMC Enterprise et la gestion à distance des systèmes Dell EMC Enterprise à distance :https://www.dell.com/esmmanuals
  - Pour les solutions de virtualisation Dell EMC :https://www.dell.com/SoftwareManuals
  - Pour Dell EMC OpenManage :https://www.dell.com/openmanagemanuals
  - Pour iDRAC :https://www.dell.com/idracmanuals
  - Pour la gestion des systèmes Dell EMC OpenManage Connections Enterprise :https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les outils facilitant la maintenance Dell EMC :https://www.dell.com/serviceabilitytools
- Site de support Dell EMC :
  1. Rendez-vous sur https://www.dell.com/support.
  2. Cliquez sur **Parcourir tous les produits**.
  3. Sur la page **Tous les produits**, cliquez sur **Logiciel** et cliquez sur le lien requis.
  4. Cliquez sur le produit requis, puis sur la version requise.

À l'aide des moteurs de recherche, saisissez le nom et la version du document dans la zone de recherche.