Mise à niveau de VMware Identity Manager Connector

VMware Identity Manager 2.8
VMware Identity Manager 2.9.1

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

https://docs.vmware.com/fr/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

Mise à niveau de VMware Identity Manager Connector

Mise à niveau de VMware Identity Manager Connector décrit comment mettre à niveau votre instance de VMware Identity Manager Connector. Si vous préférez faire une nouvelle installation, reportez-vous à la section *Installation et configuration de VMware Identity Manager Connector*. Rappelons qu'une nouvelle installation ne conserve pas vos configurations existantes.

Les chemins de mise à niveau suivants sont pris en charge :

- De la version 2.3, 2.4, 2015.10.1 ou supérieure à la dernière version disponible

Pour plus d'informations sur l'utilisation de votre instance du connecteur mis à jour, consultez le *Guide de l'administrateur de VMware Identity Manager*.

Public concerné

Ces informations sont conçues pour toute personne qui installe, met à niveau et configure VMware Identity Manager Connector. Les informations sont rédigées à l'intention d'administrateurs système Windows ou Linux expérimentés déjà familiarisés avec la technologie des machines virtuelles.

À propos de la mise à niveau de VMware Identity Manager Connector

1

Vous pouvez mettre à niveau VMware Identity Manager Connector en ligne ou hors ligne.

Par défaut, le connecteur utilise le site Web VMware pour la procédure de mise à niveau, qui requiert que le dispositif du connecteur soit connecté à Internet. Vous devez également configurer les paramètres du serveur proxy pour le dispositif du connecteur, si applicable.

Si votre instance du connecteur n'est pas connectée à Internet, vous pouvez effectuer la mise à niveau hors ligne. Pour une mise à niveau hors ligne, vous téléchargez le package de mise à niveau et configurez un serveur Web local pour qu'il héberge le fichier de mise à niveau.

Les chemins de mise à niveau suivants sont pris en charge :

- De la version 2.3, 2.4, 2015.10.1 ou supérieure à la dernière version disponible

Préparation de la mise à niveau de VMware Identity Manager Connector 2

Pour préparer la mise à niveau du connecteur, vous devez exécuter plusieurs tâches préalables, comme rechercher les mises à niveau disponibles et configurer les paramètres du serveur proxy pour le dispositif, si applicable.

Ce chapitre aborde les rubriques suivantes :

Conditions préalables pour la mise à niveau

Avant de mettre à niveau le connecteur, exécutez ces tâches préalables.

Conditions préalables pour la mise à niveau en ligne

- Vérifiez que le dispositif du connecteur peut résoudre et atteindre l'adresse vapp-updates.vmware.com sur le port 80 via HTTP.
- Confirmez qu'une mise à niveau de connecteur existe. Exécutez la commande appropriée pour rechercher des mises à niveau. Voir « Vérifier la disponibilité d'une mise à niveau de VMware Identity Manager Connector en ligne », page 10.
- Vérifiez qu'au moins 2 Go d'espace disque sont disponibles sur la partition racine principale du dispositif.
- Vérifiez que le connecteur est correctement configuré.
- Prenez un snapshot de votre dispositif du connecteur pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Si un serveur proxy HTTP est requis pour l'accès HTTP sortant, configurez les paramètres du serveur proxy pour le dispositif du connecteur. Voir « Configurer les paramètres du serveur proxy pour le dispositif VMware Identity Manager Connector », page 10.

Conditions préalables pour la mise à niveau hors ligne

- Confirmez qu'une mise à niveau de connecteur existe. Rendez-vous sur le site Téléchargements My VMware à l'adresse my.vmware.com pour voir s'il existe des mises à niveau.
- Vérifiez qu'au moins 2 Go d'espace disque sont disponibles sur la partition racine principale du dispositif.

- Vérifiez que le connecteur est correctement configuré.
- Prenez un snapshot de votre dispositif du connecteur pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Configurez le dispositif du connecteur afin qu'il utilise un serveur Web local pour héberger le fichier de mise à niveau. Voir Chapitre 4, « Effectuer une mise à niveau hors ligne de VMware Identity Manager Connector », page 13.

Vérifier la disponibilité d'une mise à niveau de VMware Identity Manager Connector en ligne

Si votre dispositif du connecteur est connecté à Internet, vous pouvez vérifier la disponibilité des mises à niveau en ligne à partir du dispositif.

Procédure

1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.

2 Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 Exécutez la commande suivante pour rechercher une mise à niveau en ligne.

```
/usr/local/horizon/update/updatemgr.hzn check
```

Configurer les paramètres du serveur proxy pour le dispositif VMware Identity Manager Connector

Le dispositif du connecteur accède aux serveurs de mise à jour VMware par Internet. Si votre configuration réseau fournit un accès à Internet via un proxy HTTP, vous devez régler les paramètres de proxy pour le dispositif.

Autorisez uniquement la gestion du trafic Internet sur votre serveur proxy. Pour vous assurer que le serveur proxy est correctement configuré, définissez le paramètre du trafic interne sur no-proxy dans le domaine.

Remarque Les serveurs proxy qui requièrent l'authentification ne sont pas pris en charge.

Prérequis

- Vérifiez que vous disposez du mot de passe racine pour le dispositif du connecteur.
- Vérifiez que vous disposez des informations du serveur proxy.

Procédure

1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.

2 Entrez `YaST` sur la ligne de commande pour exécuter l'utilitaire `YaST`.

3 Sélectionnez **Services réseau** dans le volet de gauche, puis sélectionnez **Proxy**.

4 Entrez les URL du serveur proxy dans les champs **URL de proxy HTTP** et **URL de proxy HTTPS**.

5 Sélectionnez **Terminer** et quittez l'utilitaire `YaST`.

6 Redémarrez le serveur Tomcat sur le dispositif virtuel du connecteur pour utiliser les nouveaux paramètres de proxy.

```
service horizon-workspace restart
```

Les serveurs de mise à jour VMware sont maintenant disponibles pour le dispositif du connecteur.

Effectuer une mise à niveau en ligne de VMware Identity Manager Connector

3

Vous pouvez mettre à niveau votre instance de VMware Identity Manager Connector en ligne.

Prérequis

- Vous respectez les conditions préalables répertoriées dans la section Chapitre 2, « Préparation de la mise à niveau de VMware Identity Manager Connector », page 9.
- Vérifiez que le dispositif du connecteur est sous tension et qu'il fonctionne.

Procédure

1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.

2 Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 Exécutez la commande suivante pour vérifier qu'une mise à niveau en ligne existe.

```
/usr/local/horizon/update/updatemgr.hzn check
```

4 Exécutez la commande suivante pour mettre à jour le dispositif.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Les messages générés pendant la mise à niveau sont enregistrés dans le fichier `update.log` à l'emplacement `/opt/vmware/var/log/update.log`.

5 Exécutez de nouveau la commande `updatemgr.hzn check` pour vérifier qu'une mise à jour plus récente n'existe pas.

```
/usr/local/horizon/update/updatemgr.hzn check
```

6 Vérifiez la version du dispositif mis à niveau.

```
vamicli version --appliance
```

La nouvelle version est affichée.

7 Redémarrez le dispositif du connecteur.

```
reboot
```

8 Répétez les étapes précédentes pour chaque dispositif du connecteur dans votre déploiement de VMware Identity Manager.

La mise à niveau du connecteur est terminée.

Effectuer une mise à niveau hors ligne de VMware Identity Manager Connector

4

Si votre dispositif VMware Identity Manager Connector ne peut pas se connecter à Internet pour la mise à niveau, vous pouvez effectuer une mise à niveau hors ligne. Vous devez installer un référentiel de mise à niveau sur un serveur Web local et configurer le dispositif du connecteur afin qu'il utilise le serveur Web local pour la mise à niveau.

Ce chapitre aborde les rubriques suivantes :

Préparer un serveur Web local pour une mise à niveau hors ligne

Avant de démarrer la mise à niveau hors ligne du connecteur, préparez le serveur Web local en créant une structure de répertoire incluant un sous-répertoire pour le dispositif du connecteur.

Prérequis

- Téléchargez le fichier `identity-manager-connector-`*`versionNumber-buildNumber`*`-updaterepo.zip` sur My VMware. Allez sur le site my.vmware.com, accédez à la page Téléchargement VMware Identity Manager et téléchargez le fichier répertorié sous **Package de mise à niveau hors ligne VMware Identity Manager Connector**.
- Si vous utilisez un serveur Web IIS, configurez le serveur Web pour qu'il autorise les caractères spéciaux dans les noms de fichier. Vous configurez cela dans la section **Filtrage des demandes** en sélectionnant l'option **Autoriser le double-échappement**.

Procédure

1. Créez un répertoire sur le serveur Web à l'adresse http://*YourWebServer/VM/* et copiez le fichier zip téléchargé dessus.
2. Vérifiez que votre serveur Web inclut des types mime pour `.sig` (texte/brut) et `.sha256` (texte/brut).

   Sans ces types mime, votre serveur Web ne parvient pas à rechercher les mises à jour.
3. Décompressez le fichier.

   Le contenu du fichier ZIP extrait est servi par http://*YourWebServer/VM/*.

   Le fichier extrait contient les sous-répertoires suivants : `/manifest` et `/package-pool`.
4. Exécutez la commande `updatelocal.hzn` suivante pour vérifier que l'URL dispose d'un contenu de mise à jour valide.

   ```
   /usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM
   ```

Configurer le connecteur et effectuer une mise à niveau hors ligne

Configurez le dispositif du connecteur pour qu'il pointe vers le serveur Web local afin d'effectuer une mise à niveau hors ligne. Puis mettez le dispositif à niveau.

Prérequis

« Préparer un serveur Web local pour une mise à niveau hors ligne », page 13.

Procédure

1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.

2 Exécutez la commande suivante pour configurer un référentiel de mise à niveau qui utilise un serveur Web local.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://YourWebServer/VM/
```

Remarque Pour annuler la configuration et pouvoir de nouveau effectuer une mise à niveau en ligne, vous pouvez exécuter la commande suivante.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

---

3 Effectuez la mise à niveau.

a Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

b Exécutez la commande suivante pour vérifier la version de la mise à niveau disponible.

```
/usr/local/horizon/update/updatemgr.hzn check
```

c Exécutez la commande suivante pour mettre à jour le connecteur.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Les messages générés pendant la mise à niveau sont enregistrés dans le fichier `update.log` à l'emplacement `/opt/vmware/var/log/update.log`.

d Exécutez de nouveau la commande `updatemgr.hzn check`.

```
/usr/local/horizon/update/updatemgr.hzn check
```

e Vérifiez la version du dispositif mis à niveau.

```
vamicli version --appliance
```

La commande doit afficher la nouvelle version.

f Redémarrez le dispositif du connecteur.

Par exemple, à partir de la ligne de commande, exécutez la commande suivante.

```
reboot
```

4 Répétez les étapes précédentes pour chaque dispositif du connecteur dans votre déploiement de VMware Identity Manager.

La mise à niveau du connecteur est terminée.

Configurer des paramètres après la mise à niveau du connecteur 5

Après avoir effectué la mise à niveau vers le connecteur 2016.3.1.0 ou une version ultérieure, configurez ces paramètres.

- Si vous utilisez des ThinApps, l'authentification Kerberos ou des annuaires Active Directory (authentification Windows intégrée), vous devez quitter le domaine et le rejoindre. Cela est obligatoire pour tous les dispositifs virtuels de connecteur dans votre déploiement.
  a Cliquez sur l'onglet **Identité et gestion de l'accès**.
  b Cliquez sur **Configuration**
  c Sur la page Connecteurs, pour chaque connecteur utilisé pour l'intégration des ThinApps, l'authentification Kerberos ou un annuaire Active Directory (authentification Windows intégrée), cliquez sur **Quitter le domaine**.
  d Cliquez sur **Joindre le domaine** pour rejoindre le domaine.

    Pour joindre le domaine, vous avez besoin d'informations d'identification Active Directory avec les privilèges pour joindre le domaine. Pour plus d'informations sur la jonction à un domaine, consultez la section « Intégration à Active Directory » du document *Installation et configuration de VMware Identity Manager*.
  e Si vous utilisez l'authentification Kerberos, activez de nouveau l'adaptateur d'authentification Kerberos. Pour accéder à la page Adaptateurs d'authentification, sur la page Connecteurs, cliquez sur le lien approprié dans la colonne **Employé** et sélectionnez l'onglet **Adaptateurs d'authentification**.
  f Vérifiez que les autres adaptateurs d'authentification que vous utilisez sont activés.
- Si vous utilisez Active Directory (authentification Windows intégrée), ou Active Directory sur LDAP avec l'option **Cet annuaire prend en charge l'emplacement du service DNS** activée, enregistrez la page Domaines de l'annuaire.
  a Cliquez sur l'onglet **Identité et gestion de l'accès**.
  b Sur la page Annuaires, cliquez sur l'annuaire.
  c Fournissez le mot de passe pour l'utilisateur ND Bind et cliquez sur **Enregistrer**.
  d Cliquez sur **Paramètres de synchronisation** sur la gauche de la page et sélectionnez l'onglet **Domaines**.

e Cliquez sur **Enregistrer**.

Remarque Dans le connecteur 2016.3.1.0 et versions ultérieures, un fichier `domain_krb.properties` est créé et rempli automatiquement avec des contrôleurs de domaine lorsqu'un annuaire avec l'option Emplacement du service DNS activée est créé. Lorsque vous enregistrez la page Domaines après la mise à niveau, si vous disposiez d'un fichier `domain_krb.properties` dans votre déploiement d'origine, le fichier est mis à jour avec les domaines que vous avez pu ajouter par la suite et qui n'étaient pas dans le fichier. Si vous ne disposiez pas d'un fichier `domain_krb.properties` dans votre déploiement d'origine, le fichier est créé et rempli automatiquement avec des contrôleurs de domaine. Pour plus d'informations sur le fichier `domain_krb.properties`, consultez la section « Intégration à Active Directory » du document *Installation et configuration de VMware Identity Manager*.

Résolution des erreurs de mise à niveau 6

Vous pouvez résoudre les problèmes de mise à niveau en consultant les journaux d'erreur. Si le connecteur ne démarre pas après la mise à niveau, vous pouvez rétablir une instance précédente en restaurant un snapshot.

Ce chapitre aborde les rubriques suivantes :

Examen des journaux d'erreur de mise à niveau

Résolvez les erreurs qui se produisent lors d'une mise à niveau en examinant les journaux d'erreur. Les fichiers journaux de mise à niveau se trouvent dans le répertoire `/opt/vmware/var/log`.

Problème

Lorsque la mise à niveau est terminée, le connecteur ne démarre pas et des erreurs apparaissent dans les journaux d'erreur.

Cause

Des erreurs se sont produites au cours de la mise à niveau.

Solution

1. Connectez-vous au dispositif du connecteur.
2. Accédez au répertoire `/opt/vmware/var/log`.
3. Ouvrez le fichier `update.log` et consultez les messages d'erreur.
4. Résolvez les erreurs et exécutez de nouveau la commande de mise à niveau. La commande de mise à niveau reprend au point où elle s'est arrêtée.

Remarque Vous pouvez également restaurer un snapshot et réexécuter la mise à jour.

Restauration de snapshots du connecteur

Si le connecteur ne démarre pas correctement après une mise à niveau, vous pouvez restaurer une instance précédente.

Problème

Une fois votre instance du connecteur mise à niveau, elle ne démarre pas correctement. Vous avez examiné les journaux d'erreur de mise à niveau et exécuté de nouveau la commande de mise à niveau, mais cela n'a pas résolu le problème.

Cause

Des erreurs se sont produites pendant le processus de mise à niveau.

Solution

- Restaurez l'un des snapshots que vous avez pris comme sauvegarde de votre instance du connecteur d'origine. Pour plus d'informations, consultez la documentation de vSphere.

Collecter un bundle de fichiers journaux

Vous pouvez collecter un bundle de fichiers journaux à envoyer au support VMware. Vous obtenez le bundle sur la page de configuration du connecteur.

Les fichiers journaux suivants sont collectés dans le bundle.

Tableau 6-1. Fichiers journaux

Composant	Emplacement du fichier journal	Description
Journaux Apache Tomcat (catalina.log)	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat enregistre les messages qui ne sont pas enregistrés dans d'autres fichiers journaux.
Journaux du Programme de configuration (configurator.log)	`/opt/vmware/horizon/workspace/logs/configurator.log`	Requêtes que Configurator reçoit du client REST et de l'interface Web.
Journaux Connector (connector.log)	`/opt/vmware/horizon/workspace/logs/connector.log`	Enregistrement de chaque demande reçue de l'interface Web. Chaque entrée de journal inclut également l'URL, l'horodatage et les exceptions de la requête. Aucune action de synchronisation n'est enregistrée.

Procédure

1 Connectez-vous à la page de configuration du connecteur à l'adresse https://*connectorURL*:8443/cfg/logs.

2 Cliquez sur **Préparer le bundle de journaux**.

3 Téléchargez le bundle et envoyez-le au support VMware.

Index