

Mise à niveau vers VMware Identity Manager 2.8

VMware Identity Manager 2.8

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

Copyright © 2016 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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 vers VMware Identity Manager 2.8	5
1 À propos de la mise à niveau vers VMware Identity Manager 2.8	7
Mise à niveau d'un cluster	8
Préparation du serveur RabbitMQ avant la mise à niveau	8
2 Mise à niveau en ligne de VMware Identity Manager	11
Conditions préalables pour la mise à niveau en ligne	11
Vérifier la disponibilité d'une mise à niveau de VMware Identity Manager en ligne	12
Configurer les paramètres du serveur proxy pour le dispositif VMware Identity Manager	12
Effectuer une mise à niveau en ligne	13
3 Mise à niveau hors ligne de VMware Identity Manager	15
Conditions préalables pour la mise à niveau hors ligne	15
Préparer un serveur Web local pour une mise à niveau hors ligne	15
Configurer le dispositif et effectuer une mise à niveau hors ligne	16
4 Configurer des paramètres après la mise à niveau	19
5 Résolution des erreurs de mise à niveau	21
Examen des journaux d'erreur de mise à niveau	21
Restauration de snapshots d' VMware Identity Manager	22
Collecter un bundle de fichiers journaux	22
6 Dépannage des problèmes de RabbitMQ	23
Index	25

Mise à niveau vers VMware Identity Manager 2.8

Mise à niveau vers VMware Identity Manager 2.8 décrit comment effectuer la mise à niveau vers VMware Identity Manager 2.8 à partir de la version 2.6.

Si vous préférez faire une nouvelle installation de la version 2.8, consultez *Installation et configuration de VMware Identity Manager*. Rappelons qu'une nouvelle installation ne conserve pas vos configurations existantes.

Pour plus d'informations sur l'utilisation de votre instance de VMware Identity Manager mise à niveau, 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. Les informations sont rédigées à l'intention d'administrateurs système Windows ou Linux expérimentés déjà familiarisés avec la technologie des machines virtuelles.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web <http://www.vmware.com/support/pubs>.

À propos de la mise à niveau vers VMware Identity Manager 2.8

1

Les chemins et les scénarios de mise à niveau suivants sont pris en charge.

Chemins de mise à niveau pris en charge

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

- Version 2.6 ou ultérieure vers 2.8

Connectivité Internet

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

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

Si votre dispositif virtuel n'est pas connecté 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 sur My VMware et configurez un serveur Web local pour qu'il héberge le fichier de mise à niveau.

Scénarios de mise à niveau

- Si vous avez déployé un seul dispositif VMware Identity Manager, mettez-le à niveau en ligne ou hors ligne tel que décrit dans [Chapitre 2, « Mise à niveau en ligne de VMware Identity Manager »](#), page 11 ou [Chapitre 3, « Mise à niveau hors ligne de VMware Identity Manager »](#), page 15.

REMARQUE Un temps d'arrêt est à prévoir, car tous les services sont arrêtés lors de la mise à niveau. Prévoyez l'heure de votre mise à niveau en conséquence.

- Si vous avez déployé plusieurs dispositifs virtuels VMware Identity Manager dans un cluster à des fins de basculement ou de haute disponibilité, reportez-vous à la section [« Mise à niveau d'un cluster »](#), page 8.
- Pour mettre à niveau VMware Identity Manager sans temps d'arrêt dans un scénario de déploiement de plusieurs centres de données, consultez [« Mise à niveau de VMware Identity Manager sans temps d'arrêt »](#) dans *Installation et configuration de VMware Identity Manager*.

Ce chapitre aborde les rubriques suivantes :

- [« Mise à niveau d'un cluster »](#), page 8
- [« Préparation du serveur RabbitMQ avant la mise à niveau »](#), page 8

Mise à niveau d'un cluster

Si vous avez déployé plusieurs dispositifs virtuels VMware Identity Manager dans un cluster à des fins de basculement ou de haute disponibilité, vous pouvez mettre les nœuds à niveau un par un. Un temps d'arrêt est à prévoir lors de la mise à niveau. Planifiez-la donc en conséquence.

Reportez-vous également à la section « [Préparation du serveur RabbitMQ avant la mise à niveau](#) », page 8.

Procédure

- 1 Prenez des snapshots de la base de données et des nœuds VMware Identity Manager.
- 2 Supprimez tous les nœuds, sauf celui de l'équilibrage de charge.
- 3 Mettez à niveau le nœud qui est toujours connecté à l'équilibrage de charge.

Suivez le processus d'une mise à niveau en ligne ou hors ligne, comme décrit dans [Chapitre 2, « Mise à niveau en ligne de VMware Identity Manager »](#), page 11 ou [Chapitre 3, « Mise à niveau hors ligne de VMware Identity Manager »](#), page 15.

IMPORTANT Un temps d'arrêt est à prévoir lors du processus de mise à niveau.

- 4 Une fois le nœud mis à niveau, laissez-le connecté à l'équilibrage de charge.
Cela garantit que le service VMware Identity Manager est disponible lorsque vous mettez à niveau les autres nœuds.
- 5 Mettez à niveau les autres nœuds un par un.
- 6 Une fois tous les nœuds mis à niveau, rajoutez-les à l'équilibrage de charge.

Préparation du serveur RabbitMQ avant la mise à niveau

Si vous avez déployé plusieurs dispositifs virtuels VMware Identity Manager dans un cluster, vous devez arrêter le cluster RabbitMQ sur tous les nœuds avant d'effectuer la mise à niveau du dispositif VMware Identity Manager.

Les nœuds RabbitMQ doivent être arrêtés dans l'ordre inverse de leur démarrage. Cela conserve l'ordre du nœud master. Pour déterminer l'ordre de démarrage, affichez le fichier `/db/rabbitmq/data/*/nodes_running_at_shutdown` sur chaque serveur. Commencez par arrêter le nœud RabbitMQ qui répertorie tous les nœuds. Par exemple, si vous disposez de trois nœuds démarrés dans l'ordre `node1, node2, node3`, le fichier `nodes_running_at_shutdown` sur le nœud 3 indique `node1,node2,node3`. Le nœud 2 indique `node1,node2`. Le nœud 1 indique `node1`. Arrêtez le nœud 3, le nœud 2, puis le nœud 1.

Procédure

- 1 Arrêtez les nœuds RabbitMQ sur chaque dispositif VMware Identity Manager du cluster. Tapez `rabbitmqctl stop`.
Faites cela pour chaque nœud RabbitMQ du cluster avant de continuer.
- 2 Vérifiez que RabbitMQ est détaché du cluster. Tapez `rabbitmqctl cluster_status`.
- 3 Mettez à niveau le premier nœud. Consultez les procédures de mise à niveau dans [Chapitre 2, « Mise à niveau en ligne de VMware Identity Manager »](#), page 11 ou [Chapitre 3, « Mise à niveau hors ligne de VMware Identity Manager »](#), page 15.

Le dispositif VMware Identity Manager est démarré.

- 4 Suivez les étapes 2 à 4 pour chaque nœud.

Lorsque chaque nœud est mis à niveau, exécutez la commande `rabbitmqctl cluster_status` sur le nœud mis à niveau afin de vérifier que tous les nœuds mis à niveau jusqu'à présent sont répertoriés dans la section `running_nodes` de la sortie. Après la mise à niveau du nœud 1, la section `running_nodes` indique uniquement `node1`. Après la mise à niveau du nœud 2, exécutez la commande `rabbitmqctl cluster_status` sur les deux nœuds et la section `running_nodes` doit indiquer `node1` et `node2`. Cela indique que les nœuds RabbitMQ sont regroupés correctement.

Lorsque tous les nœuds sont mis à niveau, RabbitMQ forme un cluster avec les nœuds dans le bon ordre.

Mise à niveau en ligne de VMware Identity Manager

2

Vous pouvez mettre à niveau le dispositif virtuel VMware Identity Manager en ligne. Le dispositif virtuel doit pouvoir se connecter à Internet pour une mise à niveau en ligne.

Ce chapitre aborde les rubriques suivantes :

- [« Conditions préalables pour la mise à niveau en ligne », page 11](#)
- [« Vérifier la disponibilité d'une mise à niveau de VMware Identity Manager en ligne », page 12](#)
- [« Configurer les paramètres du serveur proxy pour le dispositif VMware Identity Manager », page 12](#)
- [« Effectuer une mise à niveau en ligne », page 13](#)

Conditions préalables pour la mise à niveau en ligne

Avant de mettre à niveau le dispositif virtuel VMware Identity Manager en ligne, exécutez ces tâches préalables.

- Vérifiez qu'au moins 2,5 Go d'espace disque sont disponibles sur la partition racine principale du dispositif virtuel.
- Prenez un snapshot de votre dispositif virtuel pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Si vous utilisez une base de données externe, prenez un snapshot ou une sauvegarde de la base de données.
- Vérifiez que VMware Identity Manager est correctement configuré.
- Vérifiez que le dispositif virtuel peut résoudre et atteindre l'adresse `vapp-updates.vmware.com` sur le port 80 via HTTP.
- Si un serveur proxy HTTP est requis pour l'accès HTTP sortant, configurez les paramètres du serveur proxy pour le dispositif virtuel. Voir [« Configurer les paramètres du serveur proxy pour le dispositif VMware Identity Manager », page 12](#).
- Confirmez qu'une mise à niveau de VMware Identity Manager existe. Exécutez la commande appropriée pour rechercher des mises à niveau. Voir [« Vérifier la disponibilité d'une mise à niveau de VMware Identity Manager en ligne », page 12](#).

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

Si votre dispositif virtuel VMware Identity Manager peut se connecter à Internet, vous pouvez vérifier la disponibilité des mises à niveau en ligne depuis le dispositif.

Procédure

- 1 Connectez-vous au dispositif virtuel en tant qu'utilisateur root.
- 2 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

Le dispositif virtuel VMware Identity Manager 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 virtuel.
- Vérifiez que vous disposez des informations du serveur proxy. Notez que les serveurs proxy qui requièrent l'authentification ne sont pas pris en charge.

Procédure

- 1 Connectez-vous au dispositif virtuel VMware Identity Manager 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 VMware Identity Manager pour utiliser les nouveaux paramètres de proxy.

```
service horizon-workspace restart
```

Les serveurs de mise à jour VMware sont maintenant disponibles pour le dispositif virtuel VMware Identity Manager.

Effectuer une mise à niveau en ligne

Si votre dispositif virtuel VMware Identity Manager est connecté à Internet, vous pouvez effectuer la mise à niveau du dispositif en ligne.

Prérequis

- Vérifiez que vous respectez les conditions préalables répertoriées dans la section « [Conditions préalables pour la mise à niveau en ligne](#) », page 11.
- Vérifiez que le dispositif virtuel est sous tension et qu'il fonctionne.

Procédure

- 1 Connectez-vous au dispositif virtuel VMware Identity Manager en tant qu'utilisateur root.
- 2 Exécutez la commande `updatemgr.hzn` suivante.
`/usr/local/horizon/update/updatemgr.hzn updateinstall`
- 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.
`vami-cli version --appliance`
La nouvelle version est affichée.
- 7 Redémarrez le dispositif virtuel.
`reboot`

La mise à niveau est terminée.

Notez que les fonctionnalités de recherche et de saisie semi-automatique dans la console d'administration ne seront pas disponibles pendant 15 à 20 minutes après le démarrage du dispositif virtuel. Dans la version 2.7, les indexes de recherche ont été déplacés dans Elasticsearch, un moteur de recherche et d'analyse intégré au dispositif VMware Identity Manager. Le processus de migration peut durer 15 à 20 minutes au maximum après le démarrage du dispositif virtuel.

Notez également que, pour que la recherche et la saisie semi-automatique fonctionnent, l'audit ne doit pas être désactivé. Vous pouvez vérifier le paramètre d'audit sur la page **Catalogue > Paramètre > Audit**.

Mise à niveau hors ligne de VMware Identity Manager

3

Si votre dispositif virtuel VMware Identity Manager 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 afin qu'il utilise le serveur Web local pour la mise à niveau.

Ce chapitre aborde les rubriques suivantes :

- « Conditions préalables pour la mise à niveau hors ligne », page 15
- « Préparer un serveur Web local pour une mise à niveau hors ligne », page 15
- « Configurer le dispositif et effectuer une mise à niveau hors ligne », page 16

Conditions préalables pour la mise à niveau hors ligne

Avant de mettre à niveau le dispositif virtuel VMware Identity Manager hors ligne, exécutez ces tâches préalables.

- Vérifiez qu'au moins 2,5 Go d'espace disque sont disponibles sur la partition racine principale du dispositif virtuel.
- Prenez un snapshot de votre dispositif virtuel pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Si vous utilisez une base de données externe, prenez un snapshot ou une sauvegarde de la base de données.
- Vérifiez que VMware Identity Manager est correctement configuré.
- Confirmez qu'une mise à niveau de VMware Identity Manager existe. Rendez-vous sur le site My VMware à l'adresse my.vmware.com pour voir s'il existe des mises à niveau.
- Préparez un serveur Web local pour héberger le fichier de mise à niveau. Voir « Préparer un serveur Web local pour une mise à niveau hors ligne », page 15.

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

Avant de démarrer la mise à niveau hors ligne, configurez le serveur Web local en créant une structure de répertoire incluant un sous-répertoire pour le dispositif virtuel VMware Identity Manager.

Prérequis

- Obtenez le fichier `identity-manager-2.8.x.x-bui ldNumber-updaterepo.zip`. Rendez-vous sur my.vmware.com et accédez à la page de téléchargement de produits VMware Identity Manager pour télécharger le fichier.

- 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/updatesLocal.hzn checkurl http://YourWebServer/VM
```

Configurer le dispositif et effectuer une mise à niveau hors ligne

Configurez le dispositif VMware Identity Manager 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 15.

Procédure

- 1 Connectez-vous au dispositif VMware Identity Manager 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/updatesLocal.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/updatesLocal.hzn setdefault
```

- 3 Effectuez la mise à niveau.
 - a Exécutez la commande `updateMgr.hzn` suivante.

```
/usr/local/horizon/update/updatesMgr.hzn updateinstaller
```
 - b Exécutez la commande suivante.

```
/usr/local/horizon/update/updatesMgr.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`.
 - c Exécutez de nouveau la commande `updateMgr.hzn check` pour vérifier qu'une mise à jour plus récente n'existe pas.

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


- d Vérifiez la version du dispositif mis à niveau.

```
vami cli version --appliance
```

La commande doit afficher la nouvelle version.

- e Redémarrez le dispositif virtuel.

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

```
reboot
```

La mise à niveau est terminée.

Notez que les fonctionnalités de recherche et de saisie semi-automatique dans la console d'administration ne seront pas disponibles pendant 15 à 20 minutes après le démarrage du dispositif virtuel. Dans la version 2.7, les indexes de recherche ont été déplacés dans Elasticsearch, un moteur de recherche et d'analyse intégré au dispositif VMware Identity Manager. Le processus de migration peut durer 15 à 20 minutes au maximum après le démarrage du dispositif virtuel.

Notez également que, pour que la recherche et la saisie semi-automatique fonctionnent, l'audit ne doit pas être désactivé. Vous pouvez vérifier le paramètre d'audit sur la page **Catalogue > Paramètre > Audit**.

Configurer des paramètres après la mise à niveau

4

Après avoir effectué la mise à niveau vers VMware Identity Manager 2.8, configurez ces paramètres.

- Si vous avez configuré le basculement d'un cluster VMware Identity Manager, il est recommandé de mettre ce dernier à jour vers trois nœuds. Cela est dû à une limite d'Elasticsearch, un moteur de recherche et d'analyse intégré au dispositif VMware Identity Manager. Vous pouvez continuer à utiliser deux nœuds, mais vous devez connaître quelques-unes des limites liées à Elasticsearch. Pour plus d'informations, consultez « Configuration du basculement et de la redondance » dans *Installation et configuration de VMware Identity Manager*.
- Activez la nouvelle interface utilisateur du portail.
 - a Dans la console d'administration, cliquez sur la flèche dans l'onglet **Catalogue** et sélectionnez **Paramètres**.
 - b Sélectionnez **Nouvelle interface utilisateur du portail de l'utilisateur final** dans le volet de gauche et cliquez sur **Activer la nouvelle interface utilisateur du portail**.
- Le protocole Transport Layer Security 1.0 (TLS) est désactivé par défaut dans VMware Identity Manager 2.8. TLS 1.1 et 1.2 sont pris en charge.

Les problèmes avec les produits externes lorsque TLS 1.0 est désactivé sont connus. Il est recommandé d'effectuer la mise à jour de vos autres configurations de produit pour utiliser TLS 1.1 ou 1.2. Toutefois, si votre version de produits tels qu'Horizon, Horizon Air, Citrix ou des équilibres de charge ont une dépendance à TLS 1.0, vous pouvez activer TLS 1.0 dans VMware Identity Manager en suivant les instructions dans l'[article 2144805 de la base de connaissances](#).

Résolution des erreurs de mise à niveau

5

Vous pouvez résoudre les problèmes de mise à niveau en consultant les journaux d'erreur. Si VMware Identity Manager ne démarre pas, 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 »](#), page 21
- [« Restauration de snapshots d'VMware Identity Manager »](#), page 22
- [« Collecter un bundle de fichiers journaux »](#), page 22

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, VMware Identity Manager 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 virtuel VMware Identity Manager.
- 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 niveau.

Restauration de snapshots d' VMware Identity Manager

Si VMware Identity Manager ne démarre pas correctement après une mise à niveau, vous pouvez restaurer une instance précédente.

Problème

Une fois mis à niveau, VMware Identity Manager 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 créés comme sauvegarde de votre instance de VMware Identity Manager et de votre base de données externe initiales, le cas échéant. Pour plus d'informations, consultez la documentation de vSphere.

Collecter un bundle de fichiers journaux

Vous pouvez collecter un bundle de fichiers journaux. Vous obtenez le bundle sur la page de configuration du dispositif VMware Identity Manager.

Les fichiers journaux suivants sont collectés dans le bundle.

Tableau 5-1. 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.
Journaux de service (horizon.log)	/opt/vmware/horizon/workspace/logs/horizon.log	Le journal de service enregistre l'activité qui a lieu sur le dispositif VMware Identity Manager, telle que l'activité liée aux droits d'accès, aux utilisateurs et aux groupes.
Journaux de catalogue unifié (greenbox_web.log)	/opt/vmware/horizon/workspace/logs/greenbox_web.log	Enregistre l'activité liée au catalogue unifié.

Procédure

- 1 Connectez-vous à la page de configuration du dispositif VMware Identity Manager à l'adresse <https://identitymanagerURL:8443/cfg/logs>.
- 2 Cliquez sur **Préparer le bundle de journaux**.
- 3 Téléchargez le bundle.

Dépannage des problèmes de RabbitMQ

6

Le service RabbitMQ cesse de fonctionner après la mise à niveau.

Problème

RabbitMQ ne répond pas correctement dans l'environnement de cluster mis à niveau.

Solution

Les nœuds RabbitMQ doivent être arrêtés dans l'ordre inverse de leur démarrage. Cela conserve l'ordre du nœud master. Pour déterminer l'ordre de démarrage, affichez le fichier `/db/rabbitmq/data/*/nodes_running_at_shutdown` sur chaque serveur. Commencez par arrêter le nœud qui répertorie tous les nœuds. Par exemple, si vous disposez de trois nœuds démarrés dans l'ordre `node1, node2, node3`, le fichier `nodes_running_at_shutdown` sur le nœud 3 indique `node1,node2,node3`. Le nœud 2 indique `node1,node2`. Le nœud 1 indique `node1`. Vous arrêtez dans l'ordre 3, 2, 1.

Procédure

- 1 Arrêtez les nœuds RabbitMQ sur chaque dispositif VMware Identity Manager du cluster.
Tapez `rabbitmqctl stop`.
Faites cela pour chaque nœud RabbitMQ du cluster avant de continuer.
- 2 Démarrez le nœud RabbitMQ sur le dernier nœud arrêté.
Tapez `rabbitmq-server -detached`.
- 3 Vérifiez que le nœud a démarré.
Tapez `rabbitmqctl status`.
- 4 Suivez les étapes 2 et 3 pour démarrer les autres nœuds RabbitMQ dans le cluster dans le bon ordre.
- 5 Vérifiez que RabbitMQ est détaché du cluster.
Tapez `rabbitmqctl cluster_status`.
- 6 Redémarrez le service VMware Identity Manager.
Tapez `service horizon-workspace restart`.

Index

B

bundle de journaux **22**

snapshots **22**

C

cluster, mise à niveau **8**

collecter un bundle de journaux **22**

conditions préalables pour la mise à niveau en ligne **11**

conditions préalables pour la mise à niveau hors ligne **15**

configurer les paramètres **19**

E

erreurs **21**

erreurs de mise à niveau **21**

G

glossaire **5**

J

journaux d'erreurs **21**

M

mise à niveau **7**

mise à niveau en ligne **11, 13**

mise à niveau hors ligne **15**

N

nouvelle interface utilisateur du portail **19**

P

pointer vers le serveur Web local **16**

préparer un serveur Web local **15**

proxy HTTP **12**

public concerné **5**

R

rabbitMQ **8**

RabbitMQ, dépannage **23**

rechercher une mise à niveau en ligne **12**

résolution des problèmes **21**

restaurer un snapshot **22**

S

serveur proxy **12**

serveur Web local **16**

