Aktualisieren auf VMware Identity Manager 2.8

VMware Identity Manager 2.8

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Aktualisieren auf VMware Identity Manager 2.8

Unter *Aktualisieren auf VMware Identity Manager 2.8* wird beschrieben, wie Sie das Upgrade auf VMware Identity Manager 2.8 von Version 2.6 vornehmen.

Wenn Sie lieber eine Neuinstallation von Version 2.8 durchführen möchten, finden Sie dazu Informationen unter *VMware Identity ManagerInstallation und Konfiguration von* . Beachten Sie, dass bei einer Neuinstallation bereits vorhandene Konfigurationen verloren gehen.

Informationen zur Verwendung Ihrer aktualisierten VMware Identity Manager-Instanz finden Sie im *Administratorhandbuch für VMware Identity Manager*.

Angesprochene Zielgruppe

Diese Informationen sind für alle Personen bestimmt, die Installationen, Upgrades und Konfigurationen von VMware Identity Manager durchführen. Die Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der VM-Technologie vertraut sind.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Informationen zum Upgrade auf VMware Identity Manager 2.8

1

Die folgenden Upgrade-Pfade und -Szenarien werden unterstützt:

Unterstützte Upgrade-Pfade

Die folgenden Upgrade-Pfade werden unterstützt:

- Version 2.6 oder höher auf 2.8

Internet-Konnektivität

Sie können Online- oder Offline-Upgrades für VMware Identity Manager durchführen.

Standardmäßig verwendet die VMware Identity Manager-Appliance die VMware-Website für das Upgrade-Verfahren. Hierfür muss die Appliance über eine Verbindungsmöglichkeit zum Internet verfügen. Sie müssen ggf. auch Proxy-Server-Einstellungen für die Appliance konfigurieren.

Wenn Ihre virtuelle Appliance nicht über eine Internetverbindung verfügt, können Sie das Upgrade offline durchführen. Für ein Offline-Upgrade laden Sie das Upgrade-Paket von My VMware herunter und richten einen lokalen Webserver ein, auf dem die Upgrade-Datei gehostet werden soll.

Upgrade-Szenarien

- Wenn Sie eine einzelne VMware Identity Manager-Appliance bereitgestellt haben, können Sie diese online oder offline aufrüsten, wie in Kapitel 2, „Durchführen eines Online-Upgrades von VMware Identity Manager“, auf Seite 11 oder Kapitel 3, „Durchführen eines Offline-Upgrades für VMware Identity Manager“, auf Seite 15 beschrieben.

  Hinweis Sie müssen mit einer Ausfallzeit rechnen, weil beim Upgrade alle Dienste angehalten werden. Daher sollten Sie das Upgrade entsprechend planen.

- Wenn Sie mehrere virtuelle VMware Identity Manager-Appliances in einem Cluster für Failover oder Hochverfügbarkeit bereitgestellt haben, siehe „Durchführen eines Upgrades für einen Cluster“, auf Seite 8.

- Für ein Upgrade von VMware Identity Manager ohne Ausfallzeit in einem Bereitstellungsszenario mit mehreren Rechenzentren finden Sie Informationen unter „Upgrade von VMware Identity Manager ohne Ausfallzeit“ in *Installieren und Konfigurieren von VMware Identity Manager*.

Dieses Kapitel behandelt die folgenden Themen:

Durchführen eines Upgrades für einen Cluster

Wenn Sie mehrere virtuelle VMware Identity Manager-Appliances in einem Cluster für Failover oder Hochverfügbarkeit bereitgestellt haben, können Sie ein Upgrade der Knoten, jeweils einzeln, vornehmen. Aufgrund der Ausfallzeit beim Upgrade sollten Sie den Zeitpunkt für das Upgrade entsprechend planen.

Siehe auch „Vorbereiten des RabbitMQ-Servers für ein Upgrade“, auf Seite 8.

Vorgehensweise

1 Führen Sie einen Snapshot der Datenbank und der VMware Identity Manager-Knoten durch.

2 Entfernen Sie alle Knoten mit Ausnahme des Knotens am Lastausgleichsdienst.

3 Nehmen Sie ein Upgrade des Knotens vor, der noch an den Lastausgleichsdienst angeschlossen ist.

   Führen Sie die Schritte für ein Online- oder Offline-Upgrade wie in Kapitel 2, „Durchführen eines Online-Upgrades von VMware Identity Manager“, auf Seite 11 und Kapitel 3, „Durchführen eines Offline-Upgrades für VMware Identity Manager“, auf Seite 15 beschrieben durch.

   Wichtig Rechnen Sie mit Ausfallzeit beim Upgrade-Vorgang.

4 Nach dem Upgrade lassen Sie den Knoten an den Lastausgleichsdienst angeschlossen.

   Dadurch ist gewährleistet, dass der VMware Identity Manager-Dienst beim Upgrade der anderen Knoten zur Verfügung steht.

5 Nehmen Sie ein Upgrade der anderen Knoten vor, jeweils einzeln.

6 Nach dem Upgrade können Sie alle Knoten wieder zum Lastausgleichsdienst hinzufügen.

Vorbereiten des RabbitMQ-Servers für ein Upgrade

Wenn Sie mehrere virtuelle VMware Identity Manager-Appliances in einem Cluster bereitgestellt haben, müssen Sie den RabbitMQ-Cluster auf allen Knoten anhalten, bevor Sie das Upgrade der VMware Identity Manager-Appliance vornehmen.

Die RabbitMQ-Knoten müssen in umgekehrter Startreihenfolge angehalten werden. Dadurch bleibt die Reihenfolge des Master-Knotens erhalten. Zur Ermittlung der Startreihenfolge zeigen Sie die `/db/rabbitmq/data/*/nodes_running_at_shutdown`-Dateien auf jedem Server an. Fahren Sie den RabbitMQ-Knoten herunter, in dem alle Knoten zuerst angezeigt werden. Wenn Sie beispielsweise drei Knoten haben, die als Knoten 1 (node1), dann Knoten 2 (node2), dann Knoten 3 (node3) gestartet wurden, wird in der Datei „nodes_running_at_shutdown“ bei Knoten 3 „node1,node2,node3“ angezeigt. Knoten 2 zeigt node1,node2 an. Knoten 1 zeigt node1 an. Sie fahren also zuerst Knoten 3, dann Knoten 2 und schließlich Knoten 1 herunter.

Vorgehensweise

1 Stoppen Sie RabbitMQ-Knoten auf jeder VMware Identity Manager-Appliance im Cluster. Geben Sie Folgendes ein: `rabbitmqctl stop`.

   Führen Sie dies für jeden RabbitMQ-Knoten im Cluster durch, bevor Sie fortfahren.

2 Vergewissern Sie sich, ob RabbitMQ vom Cluster getrennt ist. Geben Sie Folgendes ein: `rabbitmqctl cluster_status`.

3 Aktualisieren Sie den ersten Knoten. Erläuterungen finden Sie in der Darstellung des Upgrade-Vorgangs in Kapitel 2, „Durchführen eines Online-Upgrades von VMware Identity Manager“, auf Seite 11 oder Kapitel 3, „Durchführen eines Offline-Upgrades für VMware Identity Manager“, auf Seite 15.

   Die VMware Identity Manager-Appliance wird gestartet.

4 Führen Sie die Schritte 2 bis 4 für jeden Knoten durch.

   Beim Upgrade jedes Knotens führen Sie den Befehl `rabbitmgctl cluster_status` auf dem aufgerüsteten Knoten aus, um zu prüfen, ob alle bislang aufgerüsteten Knoten im Abschnitt `running_nodes` der Ausgabe aufgeführt sind. Nach dem Upgrade von Knoten 1 ist in Abschnitt `running_nodes` nur node1 (Knoten 1) aufgeführt. Nach dem Upgrade von Knoten 2 führen Sie den Befehl `rabbitmqctl cluster_status` auf beiden Knoten aus; im Abschnitt `running_nodes` sollten Knoten 1 (node1) und Knoten 2 (node2) aufgeführt sein. Das ist ein Hinweis dafür, dass das Clustern der RabbitMQ-Knoten einwandfrei erfolgt ist.

Bei einem Upgrade aller Knoten bildet RabbitMQ einen Cluster, in dem die Knoten in der richtigen Reihenfolge angeordnet sind.

Durchführen eines Online-Upgrades von VMware Identity Manager 2

Sie können das Upgrade für die virtuelle VMware Identity Manager-Appliance auch online ausführen. Für ein Online-Upgrade muss die virtuelle Appliance eine Verbindung zum Internet herstellen können.

Dieses Kapitel behandelt die folgenden Themen:

Voraussetzungen für ein Online-Upgrade

Führen Sie die folgenden Aufgaben vor einem Online-Upgrade der virtuellen VMware Identity Manager-Appliance durch.

- Vergewissern Sie sich, dass mindestens 2,5 GB Festplattenspeicher auf der primären Root-Partition der virtuellen Appliance verfügbar sind.
- Erstellen Sie einen Snapshot Ihrer virtuellen Appliance als Backup. Informationen zum Erstellen von Snapshots finden Sie in der vSphere-Dokumentation.
- Wenn Sie eine externe Datenbank verwenden, erstellen Sie einen Snapshot oder ein Backup der Datenbank.
- Stellen Sie sicher, dass VMware Identity Manager korrekt konfiguriert ist.
- Vergewissern Sie sich, dass die virtuelle Appliance vapp-updates.vmware.com an Port 80 über HTTP auflösen und erreichen kann.
- Wenn für den ausgehenden HTTP-Zugriff ein HTTP-Proxy-Server erforderlich ist, konfigurieren Sie die Proxy-Server-Einstellungen für die virtuelle Appliance. Siehe „Konfigurieren von Proxy-Server-Einstellungen für die VMware Identity Manager-Appliance“, auf Seite 12.
- Vergewissern Sie sich, dass ein VMware Identity Manager-Upgrade vorhanden ist. Führen Sie den entsprechenden Befehl aus, um zu überprüfen, ob Upgrades vorhanden sind. Siehe „Überprüfen, ob ein Upgrade des VMware Identity Manager online verfügbar ist“, auf Seite 12.

Überprüfen, ob ein Upgrade des VMware Identity Manager online verfügbar ist

Wenn Ihre virtuelle VMware Identity Manager-Appliance eine Verbindung zum Internet herstellen kann, haben Sie die Möglichkeit, die Verfügbarkeit von Online-Upgrades aus der Appliance zu prüfen.

Vorgehensweise

1 Melden Sie sich bei der virtuellen Appliance als Root-Anwender an.

2 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein Online-Upgrade vorhanden ist.

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

Konfigurieren von Proxy-Server-Einstellungen für die VMware Identity Manager -Appliance

Die virtuelle VMware Identity Manager-Appliance greift über das Internet auf die VMware-Update-Server zu. Wenn Ihre Netzwerkkonfiguration Internetzugriff über einen HTTP-Proxy bereitstellt, müssen Sie die Proxy-Einstellungen für die -Appliance anpassen.

Aktivieren Sie den Proxy, damit dieser nur den Internetdatenverkehr verarbeitet. Um sicherzustellen, dass der Proxy korrekt eingerichtet ist, legen Sie den Parameter für internen Datenverkehr innerhalb der Domäne auf `no–proxy` fest.

Hinweis Proxy-Server, die eine Authentifizierung erfordern, werden nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Root-Kennwort für die virtuelle Appliance verfügen.
- Stellen Sie sicher, dass Sie über die Informationen für den Proxy-Server verfügen. Beachten Sie, dass Proxy-Server, die eine Authentifizierung erfordern, nicht unterstützt werden.

Vorgehensweise

1 Melden Sie sich bei der virtuellen VMware Identity Manager-Appliance als Root-Benutzer an.

2 Geben Sie in die Befehlszeile `YaST` ein, um das Hilfsprogramm `YaST` auszuführen.

3 Wählen Sie im linken Fensterbereich **Netzwerkdienste** und dann **Proxy** aus.

4 Geben Sie die URLs der Proxy-Server in die Felder **URL für HTTP-Proxy** und **URL für HTTPS-Proxy** ein.

5 Wählen Sie **Fertig stellen** aus und beenden Sie das Hilfsprogramm `YaST`.

6 Führen Sie in der virtuellen VMware Identity Manager-Appliance einen Neustart des Tomcat-Servers aus, um die neuen Proxy-Einstellungen anzuwenden.

```
service horizon–workspace restart
```

Die VMware-Update-Server sind jetzt für die virtuelle VMware Identity Manager-Appliance verfügbar.

Durchführen eines Online-Upgrades

Wenn Ihre virtuelle VMware Identity Manager-Appliance über eine Internetverbindung verfügt, können Sie das Upgrade für die Appliance online durchführen.

Voraussetzungen

- Stellen Sie sicher, dass die Voraussetzungen, die unter „Voraussetzungen für ein Online-Upgrade“, auf Seite 11 aufgeführt sind, erfüllt sind.
- Stellen Sie sicher, dass die virtuelle Appliance eingeschaltet ist und funktioniert.

Vorgehensweise

1 Melden Sie sich bei der virtuellen VMware Identity Manager-Appliance als Root-Benutzer an.

2 Führen Sie folgenden `updatemgr.hzn`-Befehl aus.

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

3 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein Online-Upgrade vorhanden ist.

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

4 Aktualisieren Sie mit dem folgenden Befehl die Appliance.

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

Während des Upgrades ausgegebene Meldungen werden in der Datei `update.log` unter dem Pfad `/opt/vmware/var/log/update.log` gespeichert.

5 Führen Sie erneut den `updatemgr.hzn check`-Befehl aus, um sich zu vergewissern, dass kein neueres Update vorhanden ist.

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

6 Überprüfen Sie die Version der Appliance nach dem Upgrade.

```
vamicli version ––appliance
```

Die neue Version wird angezeigt.

7 Starten Sie die Appliance neu.

```
reboot
```

Damit ist die Aktualisierung abgeschlossen.

Beachten Sie, dass die Funktionen Suche und automatische Vervollständigung in der Verwaltungskonsole für die Dauer von 15–20 Minuten nach dem Starten der virtuellen Appliance nicht zur Verfügung stehen. In Version 2.7 wurden die Suchindexe nach Elasticsearch, einem Such- und Analysemodul in der VMware Identity Manager-Appliance, verschoben. Der Migrationsvorgang kann bis zu 15–20 Minuten nach dem Starten der virtuellen Appliance dauern.

Beachten Sie auch, dass Prüfung nicht deaktiviert sein darf, damit die Suche und automatische Vervollständigung einwandfrei funktionieren. Sie können die Prüfeinstellungen auf der Seite **Katalog > Einstellungen > Prüfung** überprüfen.

Durchführen eines Offline-Upgrades für VMware Identity Manager 3

Wenn Ihre virtuelle VMware Identity Manager-Appliance keine Verbindung zum Internet herstellen kann, können Sie das Upgrade auch offline ausführen. Sie müssen ein Upgrade-Repository auf einem lokalen Webserver einrichten und die Appliance konfigurieren, um den lokalen Webserver für Upgrades zu verwenden.

Dieses Kapitel behandelt die folgenden Themen:

Voraussetzungen für ein Offline-Upgrade

Führen Sie die folgenden Aufgaben vor einem Offline-Upgrade der virtuellen VMware Identity Manager-Appliance durch.

- Vergewissern Sie sich, dass mindestens 2,5 GB Festplattenspeicher auf der primären Root-Partition der virtuellen Appliance verfügbar sind.
- Erstellen Sie einen Snapshot Ihrer virtuellen Appliance als Backup. Informationen zum Erstellen von Snapshots finden Sie in der vSphere-Dokumentation.
- Wenn Sie eine externe Datenbank verwenden, erstellen Sie einen Snapshot oder ein Backup der Datenbank.
- Stellen Sie sicher, dass VMware Identity Manager korrekt konfiguriert ist.
- Vergewissern Sie sich, dass ein VMware Identity Manager-Upgrade vorhanden ist. Prüfen Sie, ob auf der My VMware-Website unter my.vmware.com Upgrades vorhanden sind.
- Bereiten Sie einen lokalen Webserver für das Hosten der Upgrade-Datei vor. Siehe „Vorbereiten eines lokalen Webservers für ein Offline-Upgrade“, auf Seite 15.

Vorbereiten eines lokalen Webservers für ein Offline-Upgrade

Bevor Sie mit dem Offline-Upgrade beginnen, richten Sie den lokalen Webserver ein, indem Sie eine Verzeichnisstruktur erstellen, die ein Unterverzeichnis für die virtuelle VMware Identity Manager-Appliance enthält.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Datei `identity-manager-2.8.x.x-buildNumber-updaterepo.zip` verfügen. Wechseln Sie zu my.vmware.com und dann zur Produkt-Download-Seite von VMware Identity Manager, um die Datei herunterzuladen.

- Wenn Sie einen IIS-Webserver verwenden, konfigurieren Sie den Webserver für die Verwendung von Sonderzeichen in Dateinamen. Diese Konfiguration erfolgt im Abschnitt **Filter anfordern** durch Auswahl der Option **Doppeltes Escape-Zeichen zulassen**.

Vorgehensweise

1 Erstellen Sie ein Verzeichnis auf dem Webserver unter http://*YourWebServer*/*VM*/ und kopieren Sie die heruntergeladene ZIP-Datei hinein.

2 Stellen Sie sicher, dass Ihr Webserver MIME-Typen für `.sig` (text/plain) und `.sha256` (text/plain) enthält.

Ohne diese MIME-Typen kann Ihr Server nicht nach Updates suchen.

3 Entpacken Sie die ZIP-Datei.

Server für den Inhalt der extrahierten ZIP-Datei ist http://*YourWebServer*/*VM*/.

Der extrahierte Inhalt der Datei enthält die folgenden Unterverzeichnisse: `/manifest` und `/package-pool`.

4 Führen Sie den folgenden `updatelocal.hzn`-Befehl aus, um zu prüfen, ob die URL gültige Aktualisierungsinhalte aufweist.

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

Konfigurieren der Appliance und Durchführen von Offline-Upgrades

Konfigurieren Sie die VMware Identity Manager-Appliance so, dass sie auf den lokalen Webserver zeigt, um ein Offline-Upgrade durchzuführen. Führen Sie dann ein Upgrade für die Appliance durch.

Voraussetzungen

„Vorbereiten eines lokalen Webservers für ein Offline-Upgrade“, auf Seite 15.

Vorgehensweise

1 Melden Sie sich bei der VMware Identity Manager-Appliance als Root-Anwender an.

2 Führen Sie den folgenden Befehl aus, um ein Upgrade-Repository zu konfigurieren, das einen lokalen Webserver verwendet.

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

Hinweis Um die Konfiguration rückgängig zu machen und die Möglichkeit wiederherzustellen, ein Online-Upgrade durchzuführen, können Sie den folgenden Befehl ausführen.

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

---

3 Führen Sie das Upgrade durch.

a Führen Sie folgenden `updatemgr.hzn`-Befehl aus.

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

b Führen Sie folgenden Befehl aus.

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

Während des Upgrades ausgegebene Meldungen werden in der Datei `update.log` unter dem Pfad `/opt/vmware/var/log/update.log` gespeichert.

c Führen Sie erneut den `updatemgr.hzn check`-Befehl aus, um sich zu vergewissern, dass kein neueres Update vorhanden ist.

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

d Überprüfen Sie die Version der Appliance nach dem Upgrade.

```
vamicli version --appliance
```

Der Befehl sollte die neue Version anzeigen.

e Starten Sie die Appliance neu.

Führen Sie beispielsweise an der Befehlszeile den folgenden Befehl aus.

```
reboot
```

Damit ist die Aktualisierung abgeschlossen.

Beachten Sie, dass die Funktionen Suche und automatische Vervollständigung in der Verwaltungskonsole für die Dauer von 15–20 Minuten nach dem Starten der virtuellen Appliance nicht zur Verfügung stehen. In Version 2.7 wurden die Suchindexe nach Elasticsearch, einem Such- und Analysemodul in der VMware Identity Manager-Appliance, verschoben. Der Migrationsvorgang kann bis zu 15–20 Minuten nach dem Starten der virtuellen Appliance dauern.

Beachten Sie auch, dass Prüfung nicht deaktiviert sein darf, damit die Suche und automatische Vervollständigung einwandfrei funktionieren. Sie können die Prüfeinstellungen auf der Seite **Katalog > Einstellungen > Prüfung** überprüfen.

Konfigurieren von Einstellungen nach dem Upgrade

4

Konfigurieren Sie nach dem Upgrade auf VMware Identity Manager 2.8 diese Einstellungen.

- Wenn Sie ein VMware Identity Manager Cluster für Failover eingerichtet haben, empfiehlt es sich, dieses auf drei Knoten zu aktualisieren. Grund dafür ist eine Einschränkung von Elasticsearch, einem Such- und Analysemodul, das in die VMware Identity Manager-Appliance integriert ist. Sie können auch weiterhin zwei Knoten verwenden, sollten sich jedoch darüber im Klaren sein, dass es in Bezug auf Elasticsearch einige Einschränkungen gibt. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Failover und Redundanz“ unter *Installieren und Konfigurieren von VMware Identity Manager*.
- Aktivieren Sie die neue Benutzeroberfläche des Portals.
  a Klicken Sie in der Verwaltungskonsole auf den Pfeil in der Registerkarte **Katalog** und wählen Sie **Einstellungen** aus.

  b Wählen Sie im linken Bereich **Neue Benutzeroberfläche des Endbenutzerportals** aus und klicken Sie auf **Neue Benutzeroberfläche des Portals aktivieren**.
- Standardmäßig ist das TLS-Protokoll 1.0 (Transport Layer Security) in VMware Identity Manager 2.8 deaktiviert. TLS 1.1 und 1.2 werden unterstützt.

  Wenn TLS 1.0 deaktiviert ist, können bekanntermaßen Probleme bei externen Produkten auftreten. Daher empfiehlt es sich, die Konfiguration anderer Produkte auf die Verwendung von TLS 1.1 oder 1.2 zu aktualisieren. Doch wenn Ihre Version von Produkten wie Horizon, Horizon Air, Citrix oder Lastausgleichsdienste von TLS 1.0 abhängen, können Sie TLS 1.0 in VMware Identity Managernach dem Upgrade aktivieren, indem Sie die im Knowledgebase-Artikel 2144805 enthaltenen Anweisungen befolgen.

Behebung von Upgrade-Problemen 5

Sie können Upgrade-Probleme beheben, indem Sie die Fehlerprotokolleinträge prüfen. Wenn VMware Identity Manager nicht gestartet wird, können Sie eine frühere Instanz per Rollback auf einen Snapshot wiederherstellen.

Dieses Kapitel behandelt die folgenden Themen:

Überprüfen der Upgrade-Fehlerprotokolle

Um Fehler zu beheben, die während des Upgrades auftreten, überprüfen Sie die Fehlerprotokolle. Upgrade-Protokolldateien befinden sich im Verzeichnis `/opt/vmware/var/log`.

Problem

Nach Abschluss des Upgrades wird VMware Identity Manager nicht gestartet und die Fehlerprotokolle enthalten Fehler.

Ursache

Während des Upgrades treten Fehler auf.

Lösung

1 Melden Sie sich bei der virtuellen VMware Identity Manager-Appliance an.

2 Rufen Sie das Verzeichnis unter dem Pfad `/opt/vmware/var/log` auf.

3 Öffnen Sie die Datei `update.log` und überprüfen Sie die Fehlermeldungen.

4 Beheben Sie die Fehler und führen Sie den Upgrade-Befehl erneut aus. Der Upgrade-Befehl wird an dem Punkt fortgesetzt, an dem er angehalten wurde.

Hinweis Alternativ können Sie auch einen Snapshot wiederherstellen und das Upgrade erneut ausführen.

Rollback auf Snapshots von VMware Identity Manager

Wenn VMware Identity Manager nach einem Upgrade nicht ordnungsgemäß gestartet wird, können Sie ein Rollback auf eine frühere Instanz durchführen.

Problem

Nach dem Upgrade wird VMware Identity Manager nicht korrekt gestartet. Sie haben die Upgrade-Fehlerprotokolle überprüft und den Upgrade-Befehl erneut durchgeführt, aber dies hat das Problem nicht gelöst.

Ursache

Während des Upgrade-Vorgangs sind Fehler aufgetreten.

Lösung

- Stellen Sie einen als Sicherung der ursprünglichen VMware Identity Manager-Instanz und externen Datenbank angefertigten Snapshot wieder her. Weitere Informationen finden Sie in der vSphere-Dokumentation.

Erfassen eines Pakets von Protokolldateien

Sie können ein Paket von Protokolldateien zusammenstellen. Sie beziehen das Paket von der Konfigurationsseite für die VMware Identity Manager-Appliance.

Die folgenden Protokolldateien werden im Paket erfasst.

Tabelle 5-1. Protokolldateien

Komponente	Speicherort der Protokolldatei	Beschreibung
Apache Tomcat-Protokolle (catalina.log)	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat zeichnet Meldungen auf, die in den anderen Protokolldateien nicht aufgezeichnet werden.
Konfigurator-Protokolle (configurator.log)	`/opt/vmware/horizon/workspace/logs/configurator.log`	Anforderungen, die der Konfigurator vom REST-Client und der Web-Benutzeroberfläche empfängt
Connector-Protokolle (connector.log)	`/opt/vmware/horizon/workspace/logs/connector.log`	Ein Datensatz für jede von der Webschnittstelle empfangene Anforderung. Jeder Protokolleintrag enthält zudem die Anforderungs-URL, den Zeitstempel und Ausnahmen. Synchronisierungsaktionen werden nicht erfasst.
Dienstprotokolle (horizon.log)	`/opt/vmware/horizon/workspace/logs/horizon.log`	Der Dienst zeichnet die Aktivitäten auf, die in der VMware Identity Manager-Appliance durchgeführt werden, beispielsweise Aktivitäten im Zusammenhang mit Berechtigungen, Anwendern und Gruppen.
Protokolle des einheitlichen Katalogs (greenbox_web.log)	`/opt/vmware/horizon/workspace/logs/greenbox_web.log`	Zeichnet die Aktivitäten in Bezug auf den einheitlichen Katalog auf.

Vorgehensweise

1 Melden Sie sich bei der VMware Identity Manager-Appliance -Konfigurationsseite unter https://*identityManagerURL*:8443/cfg/logs an.

2 Klicken Sie auf **Protokollpaket vorbereiten**.

3 Laden Sie das Paket herunter.

RabbitMQ-Fehlerbehebung 6

Der RabbitMQ-Dienst funktioniert nach einem Upgrade nicht mehr.

Problem

RabbitMQ reagiert nach dem Upgrade in der Cluster-Umgebung nicht richtig.

Lösung

Die RabbitMQ-Knoten müssen in umgekehrter Startreihenfolge angehalten werden. Dadurch bleibt die Reihenfolge des Master-Knotens erhalten. Zur Ermittlung der Startreihenfolge zeigen Sie die `/db/rabbitmq/data/*/nodes_running_at_shutdown`-Dateien auf jedem Server an. Fahren Sie den Knoten herunter, in dem alle Knoten zuerst angezeigt werden. Wenn Sie beispielsweise drei Knoten haben, die als Knoten 1 (node1), dann Knoten 2 (node2), dann Knoten 3 (node3) gestartet wurden, wird in der Datei `nodes_running_at_shutdown` bei Knoten 3 „node1,node2,node3“ angezeigt. Knoten 2 zeigt node1,node2 an. Knoten 1 zeigt node1 an. Sie fahren 3, dann 2, dann 1 herunter.

Vorgehensweise

1 Stoppen Sie RabbitMQ-Knoten auf jeder VMware Identity Manager-Appliance im Cluster.

   Geben Sie Folgendes ein: `rabbitmqctl stop`.

   Tun Sie dies für jeden RabbitMQ-Knoten im Cluster, bevor Sie fortfahren.

2 Starten Sie den RabbitMQ-Knoten bei dem Knoten, der zuletzt gestoppt wurde.

   Geben Sie Folgendes ein: `rabbitmq-server -detached`.

3 Prüfen, ob der Knoten gestartet wurde.

   Geben Sie Folgendes ein: `rabbitmqctl status`.

4 Führen Sie die Schritte 2 und 3 aus, um die anderen RabbitMQ-Knoten im Cluster in der richtigen Reihenfolge zu starten.

5 Vergewissern Sie sich, ob RabbitMQ vom Cluster getrennt ist.

   Geben Sie Folgendes ein: `rabbitmqctl cluster_status`.

6 Starten Sie den VMware Identity Manager-Dienst erneut.

   Geben Sie Folgendes ein: `service horizon-workspace restart`.

Index